

Числа Хелли–Галлаи для конечных и квазиконечных множеств

И.И. Богданов, В.Л. Дольников, Г.Р. Челноков

1 Вместо введения.

Типичная задача. *В городе работают несколько автобусных маршрутов. Любые два маршрута имеют не более двух общих остановок. Также известно, что для любых десяти маршрутов найдутся такие две остановки A и B , что каждый из этих десяти маршрутов проходит через хотя бы одну из A и B . Докажите, что есть такие две остановки, что каждый из маршрутов проходит через одну из них.*

Докажите, что число 10 нельзя заменить на меньшее. (См. задачу 5.4б).)

Если вам понятно условие этой задачи и нравятся задачи такого типа — вы можете при желании пропустить дальнейший вводный текст и смело переходить к задачам.

В комбинаторике часто встают вопросы, при каких условиях для некоторого набора множеств можно выбрать не очень много элементов так, чтобы каждое множество набора содержало хотя бы один из них (такая система элементов называется *трансверсалью* набора). Такие вопросы появляются, например, при изучении раскрасок (гипер)графов (которые применяются в самых различных областях), а также во многих связанных разделах комбинаторной геометрии. Несмотря на внимание к этой области, многие вопросы, даже выглядящие как вполне школьные, до сих пор являются открытыми проблемами.

В качестве примера приведём до сих пор не доказанную (и не опровергнутую) гипотезу Ловаса–Фабера–Эрдёша.

Гипотеза. *В городе n автобусных остановок, а любые два автобусных маршрута имеют не более одной общей автобусной остановки (каждый маршрут проходит хотя бы через две остановки). Докажите, что автобусные маршруты можно так покрасить в n цветов, что автобусные маршруты одного цвета не имеют общих остановок.*

Естественно, для того, чтобы трансверсаль заданного размера для нашего набора множеств существовала, надо, чтобы она существовала для всех его поднаборов. Оказывается, что при некоторых условиях на семейство бывает достаточно проверить это свойство для поднаборов фиксированного размера. Общеизвестным примером утверждения такого типа является классическая теорема Хелли для выпуклых множеств (см. задачу 2.4).

Первая из основных целей нашего проекта — изучение аналогичных вопросов сначала для множеств из ограниченного числа элементов (раздел 4). Дальнейшие разделы посвящены исследованию близких ситуаций, когда ограничена не мощность множества, а мощность пересечения нескольких различных множеств. Такие вопросы также возникают, например, при исследовании пересечений алгебраических множеств (т.е. множеств, заданных системой алгебраических уравнений).

Многие задачи в этом проекте являются исследовательскими, ибо ответ на них в настоящее время неизвестен (или очень сложен). В таких случаях мы ставим вопрос типа “Насколько хорошую оценку вам удастся получить?” и принимаем любые достаточно хорошие **серийные** (т.е. проходящие для бесконечного числа значений параметров) оценки. Естественно, любые серьёзные улучшения известных оценок в этой области достойны публикации.

Задачи, выданные после промежуточного финиша, отмечены треугольничком[▽].

2 Введение в числа Хелли

2.1. Дан конечный набор отрезков на прямой. Известно, что пересечение всех отрезков набора пусто. Докажите, что в наборе есть два непересекающихся отрезка.

2.2. Дано дерево (т.е. связный граф без циклов) и конечный набор его поддеревьев (т.е. подграфов, каждый из которых — тоже дерево). Известно, что пересечение всех поддеревьев набора пусто. Докажите, что в наборе есть два непересекающихся поддерева.

2.3. Рассмотрим конечный набор дуг фиксированной окружности. Пусть любые 1000 из этих дуг пересекаются. Докажите, что все дуги набора не обязаны пересекаться.

Во всех трёх задачах речь идёт об одном и том же свойстве некоторой системы множеств (например, для задачи 2.1 — это множество отрезков на прямой). Дадим определение этого свойства.

Определение 1. Пусть $\mathcal{F}$ — произвольное (возможно, бесконечное) семейство множеств. Натуральное число k называется числом Хелли семейства $\mathcal{F}$, если верно следующее утверждение:

Пусть $\mathcal{G}$ — конечный набор множеств из $\mathcal{F}$, причём пересечение всех множеств из $\mathcal{G}$ пусто. Тогда найдутся не более, чем k множеств из $\mathcal{G}$ такие, что уже их пересечение пусто.

Иначе говоря, k является числом Хелли семейства $\mathcal{F}$, если выполняется следующее “утверждение типа Хелли”:

Пусть $\mathcal{G}$ — конечный набор множеств из $\mathcal{F}$, такой, что любые k множеств из $\mathcal{G}$ имеют непустое пересечение. Тогда и все множества из $\mathcal{G}$ имеют непустое пересечение.

В терминах этого определения первые две задачи утверждали, что число 2 является числом Хелли для семейств отрезков на прямой и поддеревьев фиксированного дерева. Третья же задача по сути утверждает, что для семейства дуг фиксированной окружности число Хелли не существует.

Определение 2. Пусть $\mathcal{F}$ — семейство множеств. Если для $\mathcal{F}$ существует число Хелли, то минимальное из всех этих чисел мы будем обозначать через $H(\mathcal{F})$. Если же числа Хелли для $\mathcal{F}$ не существует, то мы будем писать $H(\mathcal{F}) = \infty$.

Чтобы лучше понять определение, мы предлагаем порешать следующие задачи.

2.4. (ТЕОРЕМА ХЕЛЛИ ДЛЯ ПЛОСКОСТИ) Пусть $\mathcal{C}$ — семейство всех выпуклых множеств на плоскости. Докажите, что $H(\mathcal{C}) = 3$.

Замечание. В предыдущей задаче условие конечности набора $\mathcal{G}$ из определения можно заменить на условие, что все множества из $\mathcal{C}$ замкнуты и ограничены.

2.5. Докажите, что для семейства бесконечных возрастающих арифметических прогрессий, состоящих из натуральных чисел, число 2 является числом Хелли.

2.6. Найдите $H(\mathcal{O})$, где $\mathcal{O}$ — семейство всех окружностей на плоскости. (**Напоминание.** Окружность — это не круг, а его граница!)

3 Введение в числа Хелли–Галлаи

Следующие определения дают естественное обобщение числа Хелли.

Определение 3. Пусть $\mathcal{F}$ — семейство множеств. Множество X называется трансверсалью семейства $\mathcal{F}$, если $X \cap A \neq \emptyset$ для любого $A \in \mathcal{F}$. Если $|X| = t$, то X называется t -трансверсалью.

Замечание. Семейство имеет 1-трансверсаль тогда и только тогда, когда все его множества пересекаются.

Определение 4. Пусть $\mathcal{F}$ — семейство множеств. Натуральное число k называется t -числом Хелли–Галлаи семейства $\mathcal{F}$, если верно следующее утверждение:

Пусть $\mathcal{G}$ — конечный набор множеств из $\mathcal{F}$, не имеющее t -трансверсали. Тогда найдутся не более, чем k множеств из $\mathcal{G}$, не имеющих t -трансверсали.

Если для $\mathcal{F}$ существует t -число Хелли–Галлаи, то минимальное из всех этих чисел мы будем обозначать через $HG_t(\mathcal{F})$. Если же t -числа Хелли–Галлаи для $\mathcal{F}$ не существует, то мы будем писать $HG_t(\mathcal{F}) = \infty$.

Замечание. Числа Хелли–Галлаи действительно являются обобщениями чисел Хелли, ибо $H(\mathcal{F}) = HG_1(\mathcal{F})$ для любого семейства $\mathcal{F}$.

Следующие задачи опять же дают возможность разобраться с числом Хелли–Галлаи на примерах.

3.1. Пусть $\mathcal{S}$ — множество отрезков на фиксированной прямой.

- а) Докажите, что 3 является 2-числом Хелли–Галлаи для $\mathcal{S}$.
- б) Докажите, что $t + 1$ является t -числом Хелли–Галлаи для $\mathcal{S}$.

3.2. а) Постройте пример семейства множеств $\mathcal{F}$, для которого $H(\mathcal{F}) = 2$, но $HG_2(\mathcal{F}) \geq 1000$.

б) Докажите, что существует такое семейство множеств $\mathcal{F}$, для которого $H(\mathcal{F}) = 2$, но $HG_2(\mathcal{F}) = \infty$.

3.3. Докажите, что $HG_2(\mathcal{C}) = \infty$. (Напомним, что $\mathcal{C}$ — семейство всех выпуклых множеств на плоскости.)

3.4*. Пусть $\mathcal{L}$ — множество всех прямых на плоскости.

- а) Докажите, что $HG_t(\mathcal{L}) \leq t^2 + 1$ при $t \geq 3$.
- б) Насколько можно улучшить эту оценку?

4 Числа Хелли–Галлаи для конечных множеств

В прошлом разделе мы видели, что числа Хелли–Галлаи не зависят напрямую от чисел Хелли. Для того, чтобы такая зависимость имела место, нужны некоторые дополнительные условия на рассматриваемое семейство. Одним из таких условий является ограниченность мощности множеств в семействе. Этому посвящен данный раздел.

Определение 5. Мы обозначаем через $\mathcal{N}_d$ семейство множеств, состоящих из не более, чем d элементов.

4.1. Пусть $\mathcal{G}$ — конечный набор множеств, каждое имеет не более d элементов. Докажите, что если любые $d + 1$ множеств из $\mathcal{G}$ имеют общий элемент, то и все множества из $\mathcal{G}$ имеют общий элемент. Докажите, что число $d + 1$ нельзя заменить на меньшее.

(Упражнение на понимание. Переформулируйте эту задачу, используя терминологию, введенную выше.)

4.2. Докажите, что все числа виде $HG_t(\mathcal{N}_d)$ конечны.

4.3. а) Докажите, что $HG_t(\mathcal{N}_2) \geq C_{t+2}^2$.

б) Докажите, что $HG_t(\mathcal{N}_2) = C_{t+2}^2$.

4.4. Докажите, что $HG_t(\mathcal{N}_d) \geq C_{d+t}^t$.

4.5*. (ОСНОВНАЯ ЗАДАЧА ДЛЯ КОНЕЧНЫХ МНОЖЕСТВ) Докажите, что $HG_t(\mathcal{N}_d) = C_{d+t}^t$.

Предыдущая задача довольно сложна. Желаящие могут использовать следующую задачу в качестве подсказки.

4.6. а) (ЗАДАЧА КАТОНЫ) Пусть множества $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ таковы, что $|A_i| = d$, $|B_i| = t$, множество A_i пересекается со всеми B_j при $j \neq i$, но $A_i \cap B_i = \emptyset$ (при произвольных индексах $1 \leq i, j \leq n$). Докажите, что $n \leq C_{d+t}^t$.

б) Выведите задачу 4.5 из задачи Катоны.

4.7.[▽] Пусть множества $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ удовлетворяют условиям Катоны, т.е. $A_i \cap B_i = \emptyset$ и $A_i \cap B_j \neq \emptyset$ при любых $i \neq j$. Положим $a_i = |A_i|$, $b_i = |B_i|$. Докажите, что

$$\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} \leq 1.$$

Необходимое условие на мощности множеств из предыдущей задачи не является достаточным. Это демонстрирует следующая задача.

4.8. [▽] Докажите, что существуют такие натуральные числа $a_1, \dots, a_n, b_1, \dots, b_n$, что $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} < \frac{1}{10^{100}}$, но множеств $A_1, A_2, \dots, A_n, B_1, \dots, B_n$, удовлетворяющих условиям Катоны и таких, что $|A_i| = a_i, |B_i| = b_i$, не существует.

5 Числа Хелли–Галлаи для квазиконечных множеств

В этом пункте мы ослабим условия конечности, накладываемые на наше семейство $\mathcal{F}$.

Определение 6. Пусть $\mathcal{F}$ — семейство множеств. Будем говорить, что $\mathcal{F}$ есть семейство степени d , если $|A \cap B| \leq d$ для любых различных $A, B \in \mathcal{F}$.

Зафиксируем теперь произвольные натуральные числа d и t . Для каждого семейства $\mathcal{F}$ степени d , рассмотрим его (минимальное) t -число Хелли–Галлаи $HG_t(\mathcal{F})$. Обозначим через $a(d; t)$ наибольшее из всех этих чисел.

Иначе говоря, $a(d; t)$ — это минимальное число, являющееся t -числом Хелли–Галлаи для любого семейства $\mathcal{F}$ степени d .

Этот раздел посвящён оценкам чисел $a(d; t)$.

5.1. Дано семейство множеств $\mathcal{F}$. Пусть $|A \cap B| = 1$ для любых различных $A, B \in \mathcal{F}$ (в частности, $\mathcal{F}$ — семейство степени 1). Пусть, кроме того, среди любых 4 множеств из $\mathcal{F}$ найдутся три, имеющих непустое пересечение. Докажите, что из $\mathcal{F}$ можно выбросить 1 множество так, что все остальные имеют непустое пересечение.

5.2. Дано семейство множеств $\mathcal{F}$. Пусть $|A \cap B| = 1$ для любых различных $A, B \in \mathcal{F}$, причем в $\mathcal{F}$ есть хотя бы 17 множеств. Пусть, кроме того, среди любых 5 множеств из $\mathcal{F}$ найдутся три, имеющих непустое пересечение. Докажите, что $\mathcal{F}$ имеет 2-трансверсаль.

5.3. Докажите, что $a(d; 1) = d + 2$.

5.4. а) Докажите, что $a(1; 2) = 6$.

б) Докажите, что $a(2; 2) = 10$.

в) Докажите, что $a(3; 2) = 15$.

г) Докажите, что $a(4; 2) = 21$.

д)* Для каких значений d вам удастся доказать аналогичные утверждения про $a(d; 2)$?

5.5. а) Докажите, что $a(d; 2) \geq C_{d+3}^2$.

б) Докажите, что $a(d; 2) \leq 2d^2 + 3$ при $d \geq 2$.

в)* Насколько вам удастся улучшить эти оценки?

Замечание. В предыдущей задаче авторы умеют улучшать верхнюю оценку (т.е. оценку из части б)), но разрыв между ней и нижней по-прежнему велик. Интересно было бы получить асимптотически одинаковые верхнюю и нижнюю оценки, то есть оценки, отношение которых стремится к 1 при $d \rightarrow \infty$.

5.6. а) Докажите, что $a(1; 3) = 10$.

б) Докажите, что $a(1; 4) = 15$.

в)* Для каких значений t вам удастся доказать аналогичные утверждения?

5.7. а) Докажите, что $a(1; t) \geq C_{t+2}^2$.

б) Докажите, что $a(1; t) \leq t^2 + 1$ при $t \geq 3$.

в)* Насколько вам удастся улучшить эти оценки?

5.8. а) Докажите, что $a(d; t) \geq C_{d+t+1}^t$.

б)** Существуют ли значения d, t , при которых неравенство в предыдущем пункте строгое?

Замечание. Авторы не знают ответа на вопрос 5.8б).

5.9. а) Докажите, что число $a(d; t)$ конечно при любой паре (d, t) .

б) Насколько хорошую оценку сверху на $a(d; t)$ вам удастся получить?

Вся дальнейшая часть условий была выдана после промежуточного финиша.

Следующее понятие для квазиконечных множеств аналогично условиям Катоны.

Определение 7. Назовём конечное семейство множеств $\mathcal{G}$ $(d; t)$ -исключительным, если (i) $\mathcal{G}$ является семейством степени d , и (ii) для любого $A \in \mathcal{G}$ существует такое t -элементное множество X_A , что $X_A \cap A = \emptyset$, но $X_A \cap B \neq \emptyset$ для любого $B \in \mathcal{G}$, отличного от A .

Обозначим через $b(d; t)$ наибольшую мощность $(d; t)$ -исключительного семейства. Будем говорить, что $b(d; t) = \infty$, если существуют $(d; t)$ -исключительные семейства сколь угодно большой мощности.

5.10.[▽] Докажите, что $b(d; t) \geq a(d; t)$.

5.11.[▽] Докажите, что $b(d; t)$ конечно при всех d и t .

Следующие задачи этого раздела посвящены изучению исключительных множеств.

Зафиксируем на время некоторые числа d , t , а также $(d; t)$ -исключительное семейство $\mathcal{G}$. Напомним, что для каждого $A \in \mathcal{G}$ зафиксировано одно t -элементное множество X_A такое, что $X_A \cap A = \emptyset$, но $X_A \cap B \neq \emptyset$ для любого $B \in \mathcal{G}$, отличного от A .

Определение 8. Пусть x — некоторый элемент. Обозначим через $g(x)$ количество таких множеств $A \in \mathcal{G}$, что $x \in A$. Далее, обозначим через $h(x)$ количество таких множеств $A \in \mathcal{G}$, что $x \in X_A$.

5.12.[▽] а) Пусть $t = 2$. Докажите, что $h(x) \leq d + 2$ для любого x .

б) Пусть t произвольно. Докажите, что $h(x) \leq b(d; t - 1)$.

5.13.[▽] Докажите, что $g(x) \leq b(d - 1; t)$ для любого x .

5.14.[▽] Пусть $t = 2$; предположим, что $h(x) \leq d$. Докажите, что $|\mathcal{G}| \leq g(x) + h(x) + b(d - h(x); 2)$.

6 Числа Хелли–Галлаи для квазиконечных множеств размерности 2

Семейства из предыдущего раздела можно рассматривать как *одномерные*: пересечение любых двух из них конечно. В частности, полагая $t = 1$, мы получаем комбинаторный аналог семейства прямых. В этой связи естественно определить *двумерные* семейства следующим образом.

Определение 9. Пусть $\mathcal{F}$ — семейство множеств. Рассмотрим семейство $\mathcal{F}'$, состоящее из всех попарных пересечений различных множеств из $\mathcal{F}$, то есть

$$\mathcal{F}' = \{A \cap B : A, B \in \mathcal{F}, A \neq B\}.$$

Будем говорить, что $\mathcal{F}$ есть *двумерное* семейство степени d , если $\mathcal{F}'$ — (одномерное) семейство степени d .

Зафиксируем теперь произвольные натуральные числа d и t . Для каждого двумерного семейства $\mathcal{F}$ степени d , рассмотрим его (минимальное) t -число Хелли–Галлаи $HG_t(\mathcal{F})$. Обозначим через $a_2(d; t)$ наибольшее из всех этих чисел.

Мы не предлагаем настолько же развёрнутую программу, как для одномерных множеств. Вместо этого мы предлагаем всем желающим исследовать значения $a_2(d; t)$ самостоятельно. Мы готовы принимать любые результаты об этих числах. Задачи ниже лишь намечают возможные естественные направления исследования.

6.1.[▽] Докажите, что все числа $a_2(d; t)$ конечны.

6.2.[▽] Пусть $d = 0$. Дайте самостоятельно требуемые определения и докажите, что $g(x) \leq t + 1$.

6.3.[▽] (ИССЛЕДОВАТЕЛЬСКАЯ, «БЕЗ ВТОРИЧНЫХ ПЕРЕСЕЧЕНИЙ») Выясните как можно больше о числах $a_2(0; t)$ при различных значениях t .

6.4.[▽] (ИССЛЕДОВАТЕЛЬСКАЯ, «СЛУЧАЙ ПЛОСКОСТЕЙ») Выясните как можно больше о числах $a_2(1; t)$ при различных значениях t .

6.5.[▽] (ИССЛЕДОВАТЕЛЬСКАЯ, ОБЩИЙ СЛУЧАЙ) Выясните как можно больше о числах $a_2(d; t)$ при различных значениях параметров d и t .

Замечание. В последних трёх задачах предпочтение отдаётся серийным оценкам (т.е. оценкам, справедливым для бесконечного множества значений параметра t). Тем не менее, мы настоятельно рекомендуем вам начать с рассмотрения достаточного количества частных случаев.

Числа Хелли–Галлаи для конечных и квазиконечных множеств

И.И. Богданов, В.Л. Дольников, Г.Р. Челноков

Решения.

2.1. Дан конечный набор отрезков на прямой. Известно, что пересечение всех отрезков набора пусто. Докажите, что в наборе есть два непересекающихся отрезка.

Обозначим данные отрезки $[a_1, b_1], \dots, [a_n, b_n]$. Пусть a_s — максимальное из всех a_i , а b_t — минимальное из всех b_i (заметьте, мы не утверждаем, что $s \neq t$). Если $a_s \leq b_t$, то любой отрезок содержит a_s , что противоречит условию. Значит, $a_s > b_t$, поэтому $t \neq s$, и s -й отрезок не пересекается с t -м.

2.2. Дано дерево (т.е. связный граф без циклов) и конечный набор его поддеревьев (т.е. подграфов, каждый из которых — тоже дерево). Известно, что пересечение всех поддеревьев набора пусто. Докажите, что в наборе есть два непересекающихся поддерева.

Заметим, что удаление из дерева любого ребра разбивает его на две компоненты связности, причём, если ребро не принадлежало некоторому поддереву, то это поддерево целиком окажется в одной компоненте.

Обозначим поддерева $G_1, \dots, G_n$. Пусть k — наибольшее число, такое, что пересечение поддеревьев $G = G_1 \cap G_2 \cap \dots \cap G_k$ непусто (тогда $k < n$ по условию). Пересечение G с поддеревом G_{k+1} пусто. Тогда рассмотрим кратчайший путь между подграфами G и G_{k+1} . Первое ребро этого пути не принадлежит G , а значит, не принадлежит какому-то дереву G_i при $1 \leq i \leq k$. Если выбросить это ребро, то поддерева G_{k+1} и G окажутся в разных компонентах, а значит, G_{k+1} и G_i также окажутся в разных компонентах. Тогда G_{k+1} и G_i не пересекаются.

2.3. Рассмотрим конечный набор дуг фиксированной окружности. Пусть любые 1000 из этих дуг пересекаются. Докажите, что все дуги набора не обязаны пересекаться.

Построим пример набора, в котором это не выполняется. Разобьём окружность на 1001 дугу, эти дуги назовем *маленькими*. Дополнение каждой из маленьких дуг будем называть *большой* дугой. Нетрудно понять, что набор из всех больших дуг — требуемый, ибо пересечение любых 1000 больших дуг непусто, а пересечение всех больших дуг пусто.

Замечание. Мы считаем, что большие дуги в нашем примере открыты, т.е. не содержат своих концов. Для получения примера с замкнутыми дугами достаточно чуть-чуть уменьшить большие дуги.

2.4. (ТЕОРЕМА ХЕЛЛИ ДЛЯ ПЛОСКОСТИ) Пусть $\mathcal{C}$ — семейство всех выпуклых множеств на плоскости. Докажите, что $H(\mathcal{C}) = 3$.

Индукция по числу $n \geq 4$ множеств в семействе $\mathcal{G} \subset \mathcal{C}$. Докажем базу при $n = 4$. Рассмотрим выпуклые множества F_1, F_2, F_3, F_4 . Пусть все эти множества, кроме F_i , имеют общую точку x_i ($1 \leq i \leq 4$), и применим к ним следующую лемму.

Лемма 1 (теорема Радона). Любые 4 точки на плоскости можно разбить на два множества так, что выпуклые оболочки множеств имеют общую точку.

Доказательство. Разберите самостоятельно два случая: если точки являются вершинами выпуклого четырёхугольника, и если нет. $\square$

Итак, пусть, например, выпуклые оболочки множеств $\{x_1, x_2\}$ и $\{x_3, x_4\}$ имеют общую точку x . Тогда x принадлежит множествам F_3 и F_4 , поскольку в них лежит отрезок x_1x_2 ; аналогично, x принадлежит множествам F_1 и F_2 . Значит x — общая точка всех четырех множеств. В остальных случаях рассуждение аналогично.

Переход. Пусть утверждение доказано для некоторого $n \geq 4$. Пусть $\mathcal{G} = \{F_1, \dots, F_{n+1}\}$. Построим новое n -элементное семейство из множеств $F'_1 = F_1 \cap F_{n+1}, \dots, F'_n = F_n \cap F_{n+1}$.

По доказанной базе индукции, любые три множества в новом семействе имеют общую точку. Тогда, по предположению индукции, все новые множества имеют общую точку. Эта точка принадлежит всем множествам $F_1, \dots, F_{n+1}$.

2.5. Докажите, что для семейства бесконечных возрастающих арифметических прогрессий, состоящих из натуральных чисел, число 2 является числом Хелли.

Пусть $\mathcal{G}$ — конечное семейство прогрессий из условия, любые две из которых пересекаются. Заметим, что любые две прогрессии из $\mathcal{G}$ пересекаются по бесконечному количеству элементов (а именно, тоже по прогрессии). Значит, можно считать, что i -я прогрессия задаётся условием $x \equiv a_i \pmod{n_i}$ (для этого достаточно «забыть» про некоторый начальный отрезок натурального ряда).

Рассмотрим одну из прогрессий вида $x \equiv a \pmod{n}$. Это условие равносильно системе сравнений вида $x \equiv a \pmod{p_j^{\alpha_j}}$, где $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — разложение числа n на простые множители. Выпишем теперь такую систему для каждой прогрессии из $\mathcal{G}$; нам достаточно показать, что полученная система совместна (т.е. имеет решение).

Заметим, что любые два сравнения из полученной системы совместны (так как они соответствуют или одной прогрессии, или двум). Далее, пусть в системе есть два сравнения по модулю степеней одного и того же простого числа (скажем, $x \equiv a \pmod{p^\alpha}$ и $x \equiv b \pmod{p^\beta}$), причём эти сравнения совместны. Тогда, если $\alpha \geq \beta$, то второе сравнение следует из первого, поэтому второе можно выкинуть.

Проделав такие выкидывания, пока это возможно, в конце получим систему сравнений по модулю степеней различных простых чисел. Она совместна по китайской теореме об остатках. Это и требовалось доказать.

Замечание. Все t -числа Хелли–Галлаи для целочисленных арифметических прогрессий при $t \geq 2$ бесконечны.

2.6. Найдите $H(\mathcal{O})$, где $\mathcal{O}$ — семейство всех окружностей на плоскости.

Ответ. $H(\mathcal{O}) = 4$.

Докажем, что 4 является числом Хелли для семейства $\mathcal{O}$. Рассмотрим конечное семейство окружностей $\mathcal{G}$, такое, что пересечение их всех пусто. Рассмотрим произвольные две окружности $O_1, O_2 \in \mathcal{G}$; они пересекаются в не более чем двух точках; обозначим их A и B (если точек пересечения меньше двух, то рассуждение аналогично). Так как никакая точка не принадлежит всем окружностям, то, в частности, найдется окружность $O_3 \in \mathcal{G}$, не содержащая точку A , и окружность $O_4 \in \mathcal{G}$, не содержащая точку B . Тогда мы нашли 4 окружности O_1, O_2, O_3, O_4 , таких, что их пересечение пусто.

Осталось доказать, что 3 не является числом Хелли для $\mathcal{O}$. Возьмем 4 точки, являющиеся вершинами невырожденного невписанного четырёхугольника. Проведем через каждые три из них окружность. Мы получили 4 окружности, не имеющих в совокупности общих точек, но любые три из которых общую точку имеют.

3.1. Пусть $\mathcal{S}$ — множество отрезков на фиксированной прямой.

а) Докажите, что 3 является 2-числом Хелли–Галлаи для $\mathcal{S}$.

б) Докажите, что $t + 1$ является t -числом Хелли–Галлаи для $\mathcal{S}$.

Пункт а) является частным случаем б). Поэтому мы приводим только решение пункта б).

Обозначим рассматриваемые отрезки $[a_1; b_1], \dots, [a_n, b_n]$. Обозначим через c_1 наименьшее из всех b_i . Тогда ни один из отрезков не может лежать строго левее c_1 , то есть каждый отрезок или содержит c_1 , или лежит строго правее неё. Обозначим через c_2 наименьшее из всех b_i , соответствующих отрезкам, лежащим правее c_1 . Из подобных рассуждений получаем теперь, что каждый отрезок или содержит одну из точек c_1, c_2 , или лежит строго правее c_2 .

Аналогично будем определять $c_3, c_4, \dots$, пока справа от них остаются отрезки. Пусть процесс оборвался после k -го шага. Если $k \leq t$, то мы нашли такие k точек, что каждый отрезок содержит хотя бы одну из них. Пусть теперь $k \geq t + 1$. Тогда мы нашли $t + 1$ попарно непересекающийся отрезок (а именно — те отрезки, правыми концами которых являются точки $c_1, c_2, \dots, c_{t+1}$). Эти $t + 1$ отрезок, очевидно, не имеют t -трансверсали.

Итак, либо все семейство имеет t -трансверсаль, либо найдутся $t + 1$ отрезок, не имеющие t -трансверсали. Это и означает, что $t + 1$ является числом Хелли–Галлаи для отрезков на прямой,

т.е. $HG_t(\mathcal{S}) \leq t + 1$. Пример, показывающий, что $HG_t(\mathcal{S}) > t$, очевиден: достаточно взять $t + 1$ непересекающийся отрезок.

3.2. а) Постройте пример семейства множеств $\mathcal{F}$, для которого $H(\mathcal{F}) = 2$, но $HG_2(\mathcal{F}) \geq 1000$.

б) Докажите, что существует такое семейство множеств $\mathcal{F}$, для которого $H(\mathcal{F}) = 2$, но $HG_2(\mathcal{F}) = \infty$.

а) Положим $k = 500$. Наше семейство будет состоять из $2k + 1$ множеств $A_1, A_2, \dots, A_{2k+1}$ (все индексы рассматриваются по модулю $2k + 1$, т.е. $A_{i+2k+1} = A_i$), которые строятся следующим образом. Сначала каждому подмножеству индексов $S \subset \{1, 2, \dots, 2k + 1\}$, не содержащего двух индексов с разностью 1 (в частности, не содержащему одновременно 1 и $2k + 1$), сопоставим элемент x_S (элементы, сопоставленные разным подмножествам, должны быть различными). Теперь включим в A_k все элементы x_S , для которых $k \in S$.

Полученное семейство $\mathcal{F}$ имеет число Хелли 2. В самом деле, пусть подсемейство $\mathcal{G} \subset \mathcal{F}$ имеет пустое пересечение. Пусть $\mathcal{G} = \{A_i : i \in I\}$; тогда в I есть соседние индексы, ибо иначе x_I лежит во всех множествах из $\mathcal{G}$. Значит, при некотором i в $\mathcal{G}$ нашлись множества A_i и A_{i+1} , но они сами имеют пустое пересечение.

Наконец, покажем, что любые $2k$ множеств из $\mathcal{F}$ имеют 2-трансверсаль, а всё семейство $\mathcal{F}$ не имеет. Если бы $\mathcal{F}$ имело 2-трансверсаль $\{x_S, x_T\}$, то одно из множеств S, T имело бы хотя бы $k + 1$ элемент и потому содержало бы два соседних индекса, что невозможно. С другой стороны, если из $\mathcal{F}$ выкинуть, скажем, A_{2k+1} , то можно положить $S = \{1, 3, \dots, 2k - 1\}$ и $T = \{2, 4, \dots, 2k\}$; тогда $\{x_S, x_T\}$ — трансверсаль всех оставшихся множеств.

Итак, $HG_2(\mathcal{F}) = 2k + 1$.

б) Достаточно для каждого натурального k построить семейство $\mathcal{F}_k$ вышеописанным способом (так, чтобы множества из разных семейств не пересекались), а потом взять объединение всех этих семейств.

3.3. Докажите, что $HG_2(\mathcal{C}) = \infty$. (Напомним, что $\mathcal{C}$ — семейство всех выпуклых множеств на плоскости.)

Достаточно доказать, что $HG_2(\mathcal{C}) \geq 2k + 1$ при любом k . Рассмотрим окружность с центром O и впишем в неё правильный $(2k + 1)$ -угольник с вершинами $x_1, x_2, \dots, x_{2k+1}$ (индексы опять рассматриваются по модулю $2k + 1$). Обозначим через A_i выпуклую оболочку точек $x_i, x_{i+1}, \dots, x_{i+k-1}$. Тогда, очевидно, все множества без любого имеют 2-трансверсаль (например, для множеств $A_1, A_2, \dots, A_{2k}$ трансверсалью является множество $\{x_k, x_{2k}\}$).

Покажем, что каждая точка плоскости T принадлежит не более, чем k множествам. Действительно, если луч OT пересекает отрезок $x_{i-1}x_i$ (не в точке x_{i-1}), то T может принадлежать лишь множествам $A_{i-k+1}, \dots, A_i$. Значит, у нашего $(2k + 1)$ -элементного множества нет 2-трансверсали. Это и требовалось доказать.

3.4*. Пусть $\mathcal{L}$ — множество всех прямых на плоскости.

а) Докажите, что $HG_t(\mathcal{L}) \leq t^2 + 1$ при $t \geq 3$.

б) Насколько можно улучшить эту оценку?

а) Индукция по t . База при $t = 3$ будет разобрана в конце; сначала мы докажем переход.

Пусть $\mathcal{G}$ — конечное семейство прямых, в котором каждые $t^2 + 1$ (или меньше) прямые имеют t -трансверсаль. Выберем произвольные $t^2 + 1$ прямые из $\mathcal{G}$; одна из точек их t -трансверсали принадлежит хотя бы $t + 1$ выбранной прямой. Обозначим эту точку A , а эти прямые $\ell_1, \dots, \ell_{t+1}$.

Пусть $\mathcal{G}'$ — подсемейство в $\mathcal{G}$, состоящее из всех прямых, не проходящих через A . Докажем, что в нём любой поднабор D из $t^2 - t$ (или меньше) прямых имеет $(t - 1)$ -трансверсаль. Действительно, набор $D \cup \{\ell_1, \dots, \ell_{t+1}\}$ имеет t -трансверсаль X . Две прямые из $\ell_1, \dots, \ell_{t+1}$ должны проходить через одну и ту же точку множества X ; значит, эта точка — A , то есть $A \in X$. Тогда $X \setminus \{A\}$ — требуемая трансверсаль для D , ибо прямые из D не проходят через A .

Заметим, что $t^2 - t \geq (t - 1)^2 + 1 \geq HG_{t-1}(\mathcal{L})$. Из доказанного теперь получаем, что $\mathcal{G}'$ имеет $(t - 1)$ -трансверсаль X . Но тогда $X \cup \{A\}$ — требуемая трансверсаль для $\mathcal{G}$.

Доказательство базы при $t = 3$ дословно повторяет переход, кроме единственного места, в котором используется предположение индукции. Именно, нам осталось проверить, что $t^2 - t = 6 \geq HG_2(\mathcal{L})$.

Заметим сначала, что $HG_1(\mathcal{L}) \leq 3$. Действительно, если любые три прямые из $\mathcal{G}$ имеют общую точку, то точка пересечения двух из них обязана принадлежать всем остальным. Теперь неравенство $HG_2(\mathcal{L}) \leq 6$ доказывается дословным повторением перехода (с заменой чисел $t^2 + 1$ и $t^2 - t$ на 6 и 3, соответственно).

б) Мы утверждаем, что $HG_t(\mathcal{L}) = C_{t+2}^2$. Покажем сначала, что $HG_t(\mathcal{L}) \geq C_{t+2}^2$. Выберем некоторые $t + 2$ точки $T_1, \dots, T_{t+2}$ общего положения на плоскости и проведём всевозможные прямые, соединяющие пары этих точек. Нетрудно понять, что исходные точки можно выбрать так, что через каждую точку, отличную от $T_1, \dots, T_{t+2}$, проходит не более двух проведённых прямых. Теперь несложно убедиться в том, что полученное множество прямых не имеет t -трансверсали, а любое его собственное подмножество — имеет.

Осталось доказать, что $HG_t(\mathcal{L}) \leq C_{t+2}^2$. Мы будем использовать следующую лемму.

Лемма 2. Пусть $P_1(x, y), \dots, P_k(x, y)$ — многочлены от двух переменных степени $\leq t$, причём $k > C_{t+2}^2$. Тогда существуют такие числа $s_1, \dots, s_k$, не равные нулю одновременно, что $s_1 P_1(x, y) + \dots + s_k P_k(x, y) = 0$.

Доказательство. Условия на числа s_i — это система из C_{t+2}^2 линейных однородных (т.е. без константных слагаемых) уравнений (количество уравнений — это количество всевозможных мономов от двух переменных степени $\leq t$). Поскольку количество переменных больше количества уравнений, эта система имеет нетривиальное решение. $\square$

Перейдём собственно к решению. Очевидно, достаточно доказать следующее утверждение: если $n \geq C_{t+2}^2$ и любые n прямых из семейства $\mathcal{G}$ имеют t -трансверсаль, то и любая $n + 1$ прямая также имеет t -трансверсаль.

Предположим противное и рассмотрим $n + 1$ прямую, для которых утверждение неверно. Введём систему координат на плоскости так, чтобы прямые не проходили через начало координат. Для любого индекса j , уравнение j -й прямой ℓ_j можно записать в виде $a_j x + b_j y + 1 = 0$.

Зафиксируем теперь некоторый индекс i . Если выкинуть прямую ℓ_i , то найдутся t точек $(x_1, y_1), \dots, (x_t, y_t)$ такие, что каждая из оставшихся прямых проходит хотя бы через одну из них (а ℓ_i , естественно, не проходит). Это означает, что $\prod_{k=1}^t (a_j x_k + b_j y_k + 1) = 0$ при всех $j \neq i$, но не при $j = i$. Обозначая $P_i(a, b) = \prod_{k=1}^t (a x_k + b y_k + 1)$, получаем, что $P_i(a_j, b_j) = 0$ при всех $j \neq i$, но $P_i(a_i, b_i) \neq 0$.

Очевидно, все полученные многочлены имеют степень t . По лемме, найдутся числа $s_1, \dots, s_n$ такие, что $\sum_{i=1}^n s_i P_i(a, b) = 0$. При этом можно считать, что $s_1 \neq 0$. Но тогда $\sum_{i=1}^n s_i P_i(a_1, b_1) = s_1 P_1(a_1, b_1) \neq 0$. Противоречие.

4.1. Пусть $\mathcal{G}$ — конечный набор множеств, каждое имеет не более d элементов. Докажите, что если любые $d + 1$ множеств из $\mathcal{G}$ имеют общий элемент, то и все множества из $\mathcal{G}$ имеют общий элемент. Докажите, что число $d + 1$ нельзя заменить на меньшее.

(Упражнение на понимание. Переформулируйте эту задачу, используя терминологию, введённую выше.)

Условие можно переписать одной формулой $H(\mathcal{N}_d) = d + 1$.

Взяв в качестве $\mathcal{G}$ семейство всех d -элементных подмножеств $(d + 1)$ -элементного множества, мы получаем, что любые d множеств в $\mathcal{G}$ имеют общий элемент, а все $d + 1$ — не имеют. Значит, $H(\mathcal{N}_d) \geq d + 1$.

Пусть теперь $\mathcal{G} \subset \mathcal{N}_d$ — семейство, в котором любые $d + 1$ множеств имеют общий элемент. При всех $i = 1, \dots, d + 1$ обозначим через s_i минимальное возможное количество общих элементов у некоторых i множеств из $\mathcal{G}$. Очевидно, $1 \leq s_{d+1} \leq s_d \leq \dots \leq s_1 = d$. Значит, $s_{j+1} = s_j$ при некотором $j \in [1, d]$.

Пусть $A_1, \dots, A_j \in \mathcal{G}$ таковы, что $|Q| = s_j$, где $Q = A_1 \cap \dots \cap A_j$. Если $Q \not\subseteq A$ для какого-то $A \in \mathcal{G}$, то $s_{j+1} = s_j > |Q \cap A| = |A_1 \cap \dots \cap A_j \cap A|$, что противоречит определению s_{j+1} . Значит, все множества из $\mathcal{G}$ содержат непустое множество Q , что и требовалось доказать.

4.2. Докажите, что все числа виде $HG_t(\mathcal{N}_d)$ конечны.

Естественно, утверждение следует из задачи 4.5. Мы приведём здесь более лёгкое доказательство.

Индукция по t . База при $t = 1$ доказана в предыдущей задаче. Пусть теперь существует число $HG_{t-1}(\mathcal{N}_d) = S$. Покажем, что $HG_t(\mathcal{N}_d) \leq T = S + C_{Sd}^t$.

Рассмотрим произвольное конечное $\mathcal{G} \subset \mathcal{N}_d$, в котором любые T множеств имеют t -трансверсаль. Если любые S множеств из $\mathcal{G}$ имеют $(t-1)$ -трансверсаль, то по предположению индукции $\mathcal{G}$ имеет даже $(t-1)$ -трансверсаль. В противном случае существует набор $\mathcal{K} = \{A_1, \dots, A_S\} \subset \mathcal{G}$, не имеющий $(t-1)$ -трансверсали. Значит, любая t -трансверсаль набора $\mathcal{K}$ должна целиком содержаться в множестве $Q = A_1 \cup \dots \cup A_S$. Заметим, что $|Q| \leq Sd$.

Предположим теперь, что $\mathcal{G}$ не имеет t -трансверсали. Значит, для любого t -элементного подмножества $X \subset Q$ найдётся $A_X \in \mathcal{G}$, не пересекающееся с X . Рассмотрим, наконец, набор

$$\mathcal{K}' = \mathcal{K} \cup \{A_X : X \subset Q, |X| = t\}.$$

Имеем $|\mathcal{K}'| \leq S + C_{Sd}^t = T$, так что $\mathcal{K}'$ должно иметь t -трансверсаль Y . Поскольку $\mathcal{K} \subset \mathcal{K}'$, множество Y должно лежать в Q . Но тогда в $\mathcal{K}'$ есть множество A_Y , не пересекающееся с Y . Это противоречие завершает доказательство.

4.3. а) Докажите, что $HG_t(\mathcal{N}_2) \geq C_{t+2}^2$.

б) Докажите, что $HG_t(\mathcal{N}_2) = C_{t+2}^2$.

а) См. задачу 4.4.

б) Следует из следующей задачи.

4.4. Докажите, что $HG_t(\mathcal{N}_d) \geq C_{d+t}^t$.

Достаточно рассмотреть семейство $\mathcal{G}$ всех d -элементных подмножеств $(d+t)$ -элементного множества X . Тогда любое t -элементное подмножество в X пересекается со всеми множествами из $\mathcal{G}$, кроме одного.

4.5*. (ОСНОВНАЯ ЗАДАЧА ДЛЯ КОНЕЧНЫХ МНОЖЕСТВ) Докажите, что $HG_t(\mathcal{N}_d) = C_{d+t}^t$.

См. следующую задачу.

4.6. а) (ЗАДАЧА КАТОНЫ) Пусть множества $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ таковы, что $|A_i| = d$, $|B_i| = t$, множество A_i пересекается со всеми B_j при $j \neq i$, но $A_i \cap B_i = \emptyset$ (при произвольных индексах $1 \leq i, j \leq n$). Докажите, что $n \leq C_{d+t}^t$.

б) Выведите задачу 4.5 из задачи Катоны.

а) Непосредственно следует из задачи 4.7.

б) Предположим противное. Пусть $\mathcal{G} \subset \mathcal{N}_d$ — семейство минимальной мощности, такое, что любые $\leq C_{d+t}^t$ его подмножеств имеют t -трансверсаль, а само оно t -трансверсали не имеет (тогда, конечно же, $|\mathcal{G}| > C_{d+t}^t$).

Пусть $\mathcal{G} = \{A_1, \dots, A_n\}$. Для каждого $i = 1, \dots, n$, семейство $\mathcal{G} \setminus \{A_i\}$ имеет t -трансверсаль согласно выбору $\mathcal{G}$; обозначим эту трансверсаль B_i . Ясно, что $A_i \cap B_i = \emptyset$. Тогда система множеств $A_1, \dots, A_n, B_1, \dots, B_n$ удовлетворяет условиям задачи Катоны, следовательно, $|\mathcal{G}| = n \leq C_{d+t}^t$. Противоречие.

4.7. Пусть множества $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ удовлетворяют условиям Катоны, т.е. $A_i \cap B_i = \emptyset$ и $A_i \cap B_j \neq \emptyset$ при любых $i \neq j$. Положим $a_i = |A_i|$, $b_i = |B_i|$. Докажите, что

$$\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} \leq 1.$$

Пусть объединение всех множеств содержит m элементов. Рассмотрим $m!$ способов пронумеровать эти элементы числами от 1 до m . Для $i \in [1; m]$ будем говорить, что некоторая нумерация имеет i -й тип, если номер любого элемента множества A_i меньше, чем номер любого элемента множества B_i .

Заметим, что нумерация не может иметь больше одного типа. В самом деле, пусть нумерация имеет типы i -й и j -й типы при $i \neq j$. Пусть a_i и a_j — максимальные номера элемента из A_i и элемента из A_j , соответственно. Можно считать, что $a_i \leq a_j$. Тогда все элементы в B_j имеют номера, большие, чем a_j ; значит, среди элементов множества B_j нет элементов множества A_i , что противоречит условию.

Далее, посчитаем количество нумераций i -го типа. Заметим, что элементы множества $A_i \cup B_i$ могут располагаться $(a_i + b_i)!$ способами, из которых подходят $a_i!b_i!$; при этом, очевидно, для каждого такого способа существует одно и то же количество перестановок всего множества, реализующих этот способ. Итак, искомое количество равно $m! \cdot \frac{a_i!b_i!}{(a_i + b_i)!} = m! \cdot \frac{1}{C_{a_i+b_i}^{a_i}}$.

Наконец, поскольку нумераций, имеющих хоть какой-то тип, не больше, чем всех нумераций вообще, имеем

$$\sum_{i=1}^n \frac{m!}{C_{a_i+b_i}^{a_i}} \leq m!,$$

что и требовалось доказать.

4.8. Докажите, что существуют такие натуральные числа $a_1, \dots, a_n, b_1, \dots, b_n$, что $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} < \frac{1}{10^{100}}$, но множеств $A_1, A_2, \dots, A_n, B_1, \dots, B_n$, удовлетворяющих условиям Катоны и таких, что $|A_i| = a_i$, $|B_i| = b_i$, не существует.

Пусть $a_1 = 1$, $a_2 = 10^{101}$, $a_3 = 10^{101}$ и $b_1 = 10^{101}$, $b_2 = 1$, $b_3 = 1$. Тогда множества B_2 и B_3 должны пересекаться с A_1 . Поскольку все три этих множества одноэлементны, они должны совпадать; но B_2 не может совпадать с B_3 .

5.1. Дано семейство множеств $\mathcal{F}$. Пусть $|A \cap B| = 1$ для любых различных $A, B \in \mathcal{F}$ (в частности, $\mathcal{F}$ — семейство степени 1). Пусть, кроме того, среди любых 4 множеств из $\mathcal{F}$ найдутся три, имеющих непустое пересечение. Докажите, что из $\mathcal{F}$ можно выбросить 1 множество так, что все остальные имеют непустое пересечение.

Рассмотрим любые три множества $A, B, C \in \mathcal{F}$, имеющие общий элемент x . Предположим, что найдутся два различных множества $D, E \in \mathcal{F}$, не содержащие x . Рассмотрим четыре множества A, B, D, E . У трёх из них есть общий элемент y ; ясно, что тогда $y \neq x$. Далее, y принадлежит хотя бы одному из множеств A и B , без ограничения общности множеству A . Тогда y не лежит ни в B , ни в C , так как они уже имеют общий элемент x с множеством A . Тогда y обязан принадлежать обоим множествам D и E .

Рассмотрим теперь четверку B, C, D, E . Любая тройка множеств из нее содержит или пару B, C , или пару D, E . Но единственный общий элемент пары B, C — это x , и он не принадлежит ни D , ни E . Аналогично, единственный общий элемент пары D, E — это y , и он не принадлежит ни B , ни C . Итак, для четверки B, C, D, E нет элемента, покрытого тремя множествами — противоречие.

Значит, наше исходное предположение неверно, и не более чем одно множество в $\mathcal{F}$ не содержит x .

5.2. Дано семейство множеств $\mathcal{F}$. Пусть $|A \cap B| = 1$ для любых различных $A, B \in \mathcal{F}$, причем в $\mathcal{F}$ есть хотя бы 17 множеств. Пусть, кроме того, среди любых 5 множеств из $\mathcal{F}$ найдутся три, имеющих непустое пересечение. Докажите, что $\mathcal{F}$ имеет 2-трансверсаль.

Если среди любых четырех множеств из $\mathcal{F}$ есть три, имеющих общий элемент, то по предыдущей задаче все множества, кроме одного, имеют общий элемент x . Выбрав из оставшегося множества любой его элемент y , мы получим требуемую 2-трансверсаль $\{x, y\}$.

Осталось рассмотреть случай, когда нашлись 4 множества $A, B, C, D \in \mathcal{F}$, пересечение любых трёх из которых пусто. Если к ним добавить любое другое множество $E \in \mathcal{F}$, то три пересекающихся множества появятся; значит, E содержит (единственный!) общий элемент каких-то двух из исходных четырёх множеств. Поскольку у нас есть 13 вариантов для выбора E и 6 возможных пар множеств A, B, C, D , какая-то из пар появится хотя бы трижды; значит, общий элемент x этой пары лежит в пяти множествах из $\mathcal{F}$; обозначим их X_1, X_2, X_3, X_4, X_5 .

Рассмотрим теперь множества в $\mathcal{F}$, не содержащие элемент x . Если их не больше двух, то у них есть общий элемент y , и $\{x, y\}$ — требуемая трансверсаль. Пусть их хотя бы три. Пусть любые три из них имеют общий элемент; тогда легко видеть, что этот элемент y — общий для всех, и мы нашли 2-трансверсаль $\{x, y\}$.

Осталось рассмотреть случай, когда найдутся множества Y, Z, T , не содержащие x и не имеющие общего элемента. Обозначим их попарные пересечения через a_1, a_2, a_3 . Каждое a_i принадлежит не более чем одному из множеств X_1, X_2, X_3, X_4, X_5 . В самом деле, пусть a_1 принадлежит множествам X_1 и X_2 . Тогда X_1 и X_2 пересекаются по двум элементам x и a_1 , что невозможно.

Итак, из 5 множеств X_1, X_2, X_3, X_4, X_5 найдутся два, не содержащие ни одного элемента из a_1, a_2, a_3 . Пусть это X_4 и X_5 . Тогда у пятерки множеств X_4, X_5, Y, Z, T нет тройного пересечения. Противоречие.

Далее мы сначала приведём доказательства ключевых фактов про исключительные множества, а именно задач 5.10, 5.12–5.14. Мы будем затем использовать их в решениях оставшихся задач.

Во всём последующем тексте мы предполагаем, что $\mathcal{G} = (d; t)$ -исключительное семейство.

Заметим сразу, что все множества X_A при $A \in \mathcal{G}$ различны, ибо при $A \neq B$ множество X_A пересекает B , но не A , а множество X_B — наоборот. Более того, отсюда же следует, что $X_A \not\subseteq X_B$.

Для решения дальнейших задач будут полезны следующие простые леммы.

Лемма 3. Пусть $\mathcal{G} = (d; t)$ -исключительное семейство, а S — некоторое множество мощности s . Рассмотрим все такие множества $A \in \mathcal{G}$, что $S \subseteq X_A$; составим из них семейство $\mathcal{F}$ (то есть $\mathcal{F} = \{A \in \mathcal{G} : S \subseteq X_A\}$). Тогда $\mathcal{F}$ является $(d, t - s)$ -исключительным.

Доказательство. Если $S \subseteq X_A$, то $S \cap A = \emptyset$. Значит, для любых различных $A, B \in \mathcal{F}$ мы имеем $B \cap (X_A \setminus S) = B \cap X_A \neq \emptyset$. Таким образом, для семейства $\mathcal{F}$ можно все множества X_A заменить на $X_A \setminus S$, причём $|X_A \setminus S| \leq t - s$. Тогда ясно, что $\mathcal{F} = (d, t - s)$ -исключительное. $\square$

Лемма 4. Пусть $\mathcal{G} = (d; t)$ -исключительное семейство, а S — некоторое множество мощности s . Рассмотрим все множества $A \in \mathcal{G}$, содержащие S , и составим семейство $\mathcal{F}$ из всех таких множеств с выкинутым множеством S (то есть $\mathcal{F} = \{A \setminus S : S \subseteq A \in \mathcal{G}\}$). Тогда $\mathcal{F}$ является $(d - s, t)$ -исключительным.

Доказательство. Ясно, что для любых двух различных множеств $A, B \in \mathcal{G}$, содержащих S , выполняется условие $|(A \setminus S) \cap (B \setminus S)| = |A \cap B| - s \leq d - s$. Кроме того, мы имеем $X_A \cap S = \emptyset$; значит, $(B \setminus S) \cap X_A = B \cap X_A \neq \emptyset$, что и значит, что $\mathcal{F} = (d - s, t)$ -исключительное. $\square$

5.10. Докажите, что $b(d; t) \geq a(d; t)$.

Достаточно доказать, что если $a(d; t) > n$ при некотором n , то и $b(d; t) > n$.

Если $a(d; t) > n$, то существует такое семейство $\mathcal{G}$ степени d , что любые n множеств из $\mathcal{G}$ имеют t -трансверсаль, а всё семейство — не имеет. Из всех подсемейств семейства $\mathcal{G}$, не обладающих t -трансверсалью, выберем минимальное по количеству множеств и назовём его $\mathcal{F}$. Пусть $k = |\mathcal{F}|$; ясно, что $k > n$. Тогда по выбору $\mathcal{F}$, любые $k - 1$ множеств из $\mathcal{F}$ (скажем, все без некоторого A) имеют t -трансверсаль X . Заметим, что X не должна пересекать A , иначе X является t -трансверсалью для $\mathcal{F}$. Значит, X удовлетворяет всем условиям на множество X_A .

Итак, $\mathcal{F} = (d; t)$ -исключительное семейство, поэтому $b(d; t) \geq k > n$, что и требовалось доказать.

Замечание. В дальнейшем почти все верхние оценки, получаемые на $a(d; t)$, на самом деле будут оценками на $b(d; t)$. В этих случаях мы будем опускать ссылку на предыдущую задачу, завершающую доказательство.

5.12. а) Пусть $t = 2$. Докажите, что $h(x) \leq d + 2$ для любого x .

б) Пусть t произвольно. Докажите, что $h(x) \leq b(d; t - 1)$.

Пункт а) является частным случаем б) ввиду задачи 5.3. Тем не менее, мы приведём самостоятельное решение пункта а), а уже в решении б) сошлёмся на нужную лемму.

а) Предположим, что $h(x) \geq d + 3$, то есть существуют такие $A_1, \dots, A_{d+3} \in \mathcal{G}$, что $X_{A_i} = \{x, x_i\}$ при некоторых элементах x_i (эти элементы различны, ибо множества X_{A_i} различны). Но тогда $(d+1)$ -элементное множество $\{x_1, x_2, \dots, x_{d+1}\}$ лежит и в A_{d+2} , и в A_{d+3} . Это невозможно, ибо $|A_{d+2} \cap A_{d+3}| \leq d$.

б) Применив лемму 3 для множества $S = \{x\}$, получаем, что семейство $\mathcal{F} = \{A \in \mathcal{G} : x \in X_A\}$ является $(d, t - 1)$ -исключительным, т.е. $h(x) = |\mathcal{F}| \leq b(d; t - 1)$.

5.13. Докажите, что $g(x) \leq b(d - 1; t)$ для любого x .

Применив лемму 4 для множества $S = \{x\}$, получаем, что семейство $\mathcal{F} = \{A \setminus \{x\} : A \in \mathcal{G}, x \in A\}$ является $(d - 1, t)$ -исключительным, т.е. $g(x) = |\mathcal{F}| \leq b(d - 1; t)$.

5.14. Пусть $t = 2$; предположим, что $h(x) \leq d$. Докажите, что $|\mathcal{G}| \leq g(x) + h(x) + b(d - h(x); 2)$.

Пусть $B_1, \dots, B_h$ — все такие множества в $\mathcal{G}$, что $x \in X_{B_i}$ (тогда $h = h(x)$). Положим $X_{B_i} = \{x, x_i\}$; как обычно, все элементы x_i различны.

Пусть $A_1, \dots, A_k$ — все такие множества в $\mathcal{G}$, что x не лежит ни в A_i , ни в X_{A_i} . Поскольку $k = |\mathcal{G}| - g(x) - h(x)$, достаточно доказать, что $k \leq b(d - h(x); 2)$.

Поскольку $A_i \neq B_j$ при всех i, j , мы получаем $\{x, x_j\} \cap A_i \neq \emptyset$, а значит, $x_j \in A_i$, поскольку $x \notin A_i$. Итак, всё множество $Y = \{x_1, \dots, x_h\}$ лежит во всех множествах A_i . Применяя теперь лемму 4 к множеству $S = Y$, получаем $k \leq b(d - h; 2)$, что и требовалось доказать.

Замечание. Утверждение и решение остаются верными и при $h(x) > d$; в этом случае надо отметить, что $b(d - h; t) = 1$ при $d < h$.

Сначала мы соберём серийные (но не обязательно точные) оценки. Правда, иногда мы будем пользоваться точными оценками из частных случаев ниже.

Согласно задаче 5.10, для получения верхних оценок на $a(d; t)$ достаточно получить такие же оценки на $b(d; t)$. Поэтому в каждом случае ниже мы с самого начала предполагаем, что выбрано $(d; t)$ -исключительное семейство $\mathcal{G}$, и оцениваем его мощность.

5.8. а) Докажите, что $a(d; t) \geq C_{d+t+1}^t$.

б)** Существуют ли значения d, t , при которых неравенство в предыдущем пункте строгое?

а) Пусть $\mathcal{G}$ — семейство всех $(d+1)$ -элементных подмножеств некоторого $(d+t+1)$ -элементного множества B . Тогда любые два различных множества из $\mathcal{G}$ пересекаются не более, чем по d элементам. С другой стороны, любое t -элементное подмножество $X \subset B$ пересекается со всеми множествами из $\mathcal{G}$, кроме одного.

б) Жюри до сих пор не знает ответа на этот вопрос.

5.3. Докажите, что $a(d; 1) = d + 2$.

Согласно задачам 5.8а) и 5.10, нам достаточно доказать, что $b(d; 1) \leq d + 2$. Пусть существует $(d; 1)$ -исключительное семейство $\mathcal{F} = \{A_1, A_2, \dots, A_{d+3}, \dots\}$ из не менее чем $d + 3$ множеств. По определению $(d; 1)$ -исключительного семейства все X_{A_i} одноэлементные (пусть $X_{A_i} = \{x_i\}$); значит, $x_i \in A_j$ при $i \neq j$. Очевидно, $x_i \neq x_j$ при $i \neq j$. Значит, множества A_1 и A_2 содержат $d + 1$ общий элемент $x_3, \dots, x_{d+3}$, что невозможно.

Замечание. В дальнейшем нам ещё потребуется очевидное равенство $a(0; t) = b(0; t) = t + 1$. Его доказательство мы оставляем читателю.

Для удобства введём некоторые обозначения.

Определение 1. Для любого элемента x , обозначим $G_x = \{A \in \mathcal{G} : x \in A\}$ и $H_x = \{A \in \mathcal{G} : x \in X_A\}$.

Для индукционного перехода в следующей задаче будет полезно такое уточнение задачи 5.12а).

Лемма 5. Пусть $t = 2$, и пусть $|\mathcal{G}| > b(d - 1; 2) + d + 3$. Тогда $h(x) \leq d$ для любого элемента x .

Доказательство. От противного. Пусть существуют такие $d + 1$ множеств $A_1, \dots, A_{d+1}$, что $X_{A_i} = \{x, x_i\}$ (при различных элементах x_i). По задаче 5.13, мы имеем $g(x) \leq b(d - 1; 2)$. Значит, в $\mathcal{G}$ существуют хотя бы $d + 3$ множества, не содержащие x , и два из них не совпадают с A_i . Пусть это множества B, C . Поскольку $x \notin B$, но $X_{A_i} \cap B \neq \emptyset$, получаем $\{x_1, \dots, x_{d+1}\} \subseteq B$. Аналогично, $\{x_1, \dots, x_{d+1}\} \subseteq C$. Значит, $|B \cap C| \geq d + 1$, что невозможно. $\square$

Замечание. Это доказательство по сути повторяет доказательство задачи 5.14 (точнее, её версии при $h > d$).

5.5. а) Докажите, что $a(d; 2) \geq C_{d+3}^2$.

б) Докажите, что $a(d; 2) \leq 2d^2 + 3$ при $d \geq 2$.

а) Следует из общего примера из задачи 5.8а).

б) Мы докажем индукцией по $d \geq 2$, что $b(d; 2) \leq 2d^2 + 3$. База будет включена в переход.

Предположим, что $b(d; 2) \geq b(d - 1; 2) + d + 3$. Тогда $h(x) \leq d$ при всех x по лемме 5. Обозначим $b = |\mathcal{G}|$.

Для каждого элемента x обозначим через $n(x)$ количество упорядоченных троек различных множеств (A, B, C) из семейства $\mathcal{G}$, таких, что $x \in A$, $x \in B$, и $x \in X_C$. Мы оценим сумму σ всех чисел $n(x)$ двумя способами.

С одной стороны, существует $b(b-1)$ пар различных множеств (A, B) . Для каждой такой пары есть не более d вариантов выбрать подходящий элемент x (ибо $|A \cap B| \leq d$), и для каждого такого x существует $h(x) \leq d$ вариантов множества C . Итого, $\sigma = \sum_x n(x) \leq b(b-1) \cdot d^2$.

С другой стороны, рассмотрим произвольное множество C и положим $X_C = \{x, y\}$. Каждое из остальных $b-1$ множеств в $\mathcal{G}$ содержит либо x , либо y ; пусть, скажем, s_x множеств содержат x и s_y множеств содержат y ($s_x + s_y \geq b-1$). Тогда существует $s_x(s_x-1)$ пар множеств, пересекающихся по x , и $s_y(s_y-1)$ пар, пересекающихся по y . Итого, тройки с нашим множеством C учитываются как минимум $s(C) = s_x(s_x-1) + s_y(s_y-1)$ раз. Из равенства $s_x + s_y \geq b-1$ нетрудно получить, что $s(C) \geq \frac{(b-1)(b-3)}{2}$ (оценка становится точной, если $s_x = s_y = \frac{b-1}{2}$). Итак, $\sigma \geq b \frac{(b-1)(b-3)}{2}$.

В итоге мы получаем $d^2 b(b-1) \geq \sigma \geq \frac{1}{2} b(b-1)(b-3)$, откуда $2d^2 \leq b-3$, что и требовалось доказать.

Осталось рассмотреть случай, когда $b(d; 2) \leq b(d-1; 2) + d + 2$. Если $d \geq 3$, то по предположению индукции мы имеем $b(d; 2) \leq (2(d-1)^2 + 3) + d + 2 = 2d^2 - 3d + 5 \leq 2d^2 + 3$, что и требовалось. Если же $d = 2$, то по задаче 5.4а) мы имеем $b(1; 2) = 6$, поэтому $b(2; 2) \leq 6 + 2 + 2 = 10$, что и требовалось.

Замечание. Заметим, что оценка в основной части решения допускает улучшения. Так, верхняя оценка на σ точна только тогда, когда $h(x) = d$ при всех x . В то же время, из задачи 5.14 можно увидеть, что при этом условии $g(x)$ не может равняться $\frac{b-1}{2}$, то есть нижняя оценка неточна. Метод получения более точных оценок показан в лемме 7 перед вычислением $b(1; 4)$ и применён далее.

5.7. а) Докажите, что $a(1; t) \geq C_{t+2}^2$.

б) Докажите, что $a(1; t) \leq t^2 + 1$ при $t \geq 3$.

а) Следует из общего примера из задачи 5.8а).

б) Решение дословно повторяет решение задачи 3.4а): единственное свойство прямых на плоскости, которое использовалось в нём (в отличие от 3.4б)!) — то, что они образуют семейство степени 1 (проверьте это!).

5.11. Докажите, что $b(d; t)$ конечно при всех d и t .

Мы докажем оценку $b(d; t) \leq t^{d+1} + (t^{d-1} + t^{d-2} + \dots + t^0)$ индукцией по $d \geq 1$. База при $d = 1$ доказана в задаче 5.7б).

Для перехода допустим, что $d \geq 2$. Рассмотрим произвольное множество $A \in \mathcal{G}$; пусть $X_A = \{x_1, \dots, x_t\}$. Тогда все остальные множества в $\mathcal{G}$ содержат хотя бы один из элементов $x_1, \dots, x_t$. При этом количество множеств, содержащих x_i , не превосходит $b(d-1; t)$ по лемме 4. Значит, $|\mathcal{G}| \leq 1 + tb(d-1; t) = 1 + t^{d+2} + (t^d + t^{d-1} + \dots + t)$, что и требовалось доказать.

Замечание. Вместо задачи 5.7б) можно использовать в качестве базы тривиальную оценку $b(0; t) \leq t + 1$. В этом случае получается немного худшая оценка $b(d; t) \leq t^{d+1} + t^d + \dots + 1$.

5.9. а) Докажите, что число $a(d; t)$ конечно при любой паре (d, t) .

б) Насколько хорошую оценку сверху на $a(d; t)$ вам удастся получить?

Решение пункта а) получается из задач 5.10–5.11. Оттуда же получается оценка $a(d; t) \leq t^{d+1} + (t^{d-1} + t^{d-2} + \dots + t^0)$ при всех $d \geq 1$.

Наконец, мы переходим к точным, хотя и частным, результатам из задач 5.4 и 5.6. Здесь мы не ссылаемся на пункты этих задач, а просто выписываем доказанное равенство.

Нижние оценки во всех случаях непосредственно следуют из задачи 5.8а). Для верхних оценок мы опять предполагаем, что выбрано $(d; t)$ -исключительное семейство $\mathcal{G}$, и оцениваем его мощность.

$b(1; 2) = 6$. Предположим, что $|\mathcal{G}| \geq 7$. Рассмотрим произвольное $C \in \mathcal{G}$; пусть $X_C = \{x, y\}$. Тогда каждое из остальных множеств в $\mathcal{G}$ содержит x или y ; следовательно, хотя бы три из них содержат один и тот же элемент из X_C , скажем, $x \in A_1, A_2, A_3$. Заметим, что $g(x) \leq 3$ по задаче 5.13; значит, остальные множества в $\mathcal{G}$ не содержат x . По нашему предположению, в $\mathcal{G}$, кроме A_i , есть ещё хотя бы 4 множества C_1, C_2, C_3, C_4 .

Рассмотрим произвольный индекс $k = 1, 2, 3, 4$. Пусть $X_{C_k} = \{x_1, x_2\}$. Два из множеств A_i должны содержать один и тот же элемент x_j . Поскольку они пересекаются только по x (ведь

$\mathcal{G}$ — семейство степени 1!), мы получаем, что $x = x_j \in X_{C_k}$. Итак, $x \in C_k$ при всех $k = 1, 2, 3, 4$. Значит, по лемме 3, применённой к $S = \{x\}$, семейство $\{C_1, C_2, C_3, C_4\}$ — $(1; 1)$ -исключительное. Но тогда по задаче 5.3 оно имеет не более 3 элементов. Противоречие.

Замечание. Проанализировав это решение, мы можем выделить следующую лемму, полезную и в дальнейшем.

Лемма 6. Пусть $\mathcal{G}$ — исключительное $(1, t)$ -семейство, причём $g(x) \geq t + 1$ при некотором x . Тогда для любого $B \in \mathcal{G}$, мы имеем $x \in B$ или $x \in X_B$. Кроме того, $g(x) = t + 1$, и семейство $\mathcal{F} = \mathcal{G} \setminus G_x$ является $(1, t - 1)$ -исключительным.

Доказательство. Пусть $g(x) \geq t + 1$, и $G_x \supseteq \{A_1, \dots, A_{t+1}\}$.

Предположим, что $x \notin B$ и $x \notin X_B$ при некотором $B \in \mathcal{G}$. Каждое из множеств $A_1, \dots, A_{t+1}$ содержит хотя бы один элемент из X_B ; поскольку $|X_B| = t$, два из них должны содержать один и тот же элемент (скажем, $y \in A_1 \cap A_2 \cap X_B$). Но тогда $A_1 \cap A_2$ содержит (различные!) элементы x и y , что невозможно. Значит, такого множества B не существует.

Далее, $g(x) \leq t + 1$ по задаче 5.13, так что $g(x) = t + 1$. Второе утверждение следует теперь из леммы 3. $\square$

$b(1; 3) = 10$. Предположим, что $|\mathcal{G}| \geq 11$. Рассмотрим произвольное $C \in \mathcal{G}$; пусть $X_C = \{x, y, z\}$. Тогда каждое из остальных множеств в $\mathcal{G}$ содержит хотя бы один из элементов x, y или z , то есть $g(x) + g(y) + g(z) \geq 10$. Значит, одно из слагаемых больше трёх, скажем, $g(x) \geq 4$. Тогда по лемме 6 мы получаем, что $\mathcal{F} = \mathcal{G} \setminus G_x$ является $(1; 2)$ -исключительным, причём $|\mathcal{F}| \geq 7$. Это противоречит тому, что $b(1; 2) = 6$.

Замечание. Предыдущие два пункта по сути повторяют решение задачи 3.4а). Мы приводим их здесь для удобства восприятия следующего пункта.

Для дальнейшего продвижения мы несколько улучшим главный метод из задачи 5.5. Именно, мы немного изменим определение суммы σ , так, что она будет допускать несколько лучшие оценки. Смысл следующего определения будет ясен из дальнейшей леммы.

Определение 2. Для каждого элемента x , лежащего хотя бы в одном множестве вида X_A , назовём его ценой величину $p(x) = \frac{g(x)(g(x) - 1)}{h(x)}$. Для каждого $C \in \mathcal{G}$ назовём его ценой величину $P(C) = \sum_{x \in X_C} p(x)$.

Лемма 7. Пусть $\mathcal{G}$ — $(d; t)$ -исключительное семейство мощности b . Тогда существует множество $C \in \mathcal{G}$ такое, что $P(C) \leq d(b - 1)$.

Доказательство. Опять же, для каждого элемента x обозначим через $n(x)$ количество упорядоченных троек различных множеств (A, B, C) из семейства $\mathcal{G}$, таких, что $x \in A$, $x \in B$, и $x \in X_C$. Однако теперь мы будем оценивать чуть другую сумму, а именно

$$\Sigma = \sum_x \frac{n(x)}{h(x)}$$

(естественно, сумма берётся по всем элементам, участвующим в множествах вида X_A).

С одной стороны, существует $b(b - 1)$ пар различных множеств (A, B) . Для каждой такой пары есть не более d вариантов выбрать подходящий элемент x (ибо $|A \cap B| \leq d$). Далее, любой элемент $x \in A \cap B$ добавляет ровно единицу к Σ ; действительно, существует $h(x)$ вариантов множества C , и каждый из этих вариантов будет считаться с «весом» $1/h(x)$. Итого, получаем

$$\Sigma = \sum_{(A, B): A \neq B} |A \cap B| \leq d \cdot b(b - 1).$$

С другой стороны, рассмотрим произвольное множество C . Покажем, что тройки вида (A, B, C) вносят в Σ вклад, равный как раз $P(C)$. Действительно, для каждого $x \in X_C$, в числе $n(x)$ посчитаны $g(x)(g(x) - 1)$ пар. Учитывая «вес» $1/h(x)$, мы получаем, что «вклад пары x, C » равен $p(x)$, а тогда «вклад» множества C равен $P(C)$, что и требовалось.

Итак, $db(b - 1) \geq \Sigma = \sum_{C \in \mathcal{G}} P(C)$. По принципу Дирихле, одно из b слагаемых справа не превосходит $d(b - 1)$. $\square$

$b(1; 4) = 15$. Предположим, что $|\mathcal{G}| \geq 16$; выкинув несколько множеств из $\mathcal{G}$, можно считать, что $b = |\mathcal{G}| = 16$. Рассмотрим произвольное $C \in \mathcal{G}$; пусть $X_C = \{x_1, x_2, x_3, x_4\}$. Аналогично предыдущему пункту, получаем, что $\sum_i g(x_i) \geq 15$, причём $g(x_i) \leq 4$ (иначе, используя лемму 6, мы приходим к противоречию с $b(1; 3) = 10$).

Итак, $\sum_i g(x_i) = \sum_i |G_{x_i}| \leq 16$, но каждое $A \in \mathcal{G}$, отличное от C , должно лежать в одном из G_{x_i} . Это означает, что либо все семейства G_{x_i} не пересекаются, либо пересекаются лишь два из них, причём по одному элементу. В любом случае, можно считать, что G_{x_1} , G_{x_2} и G_{x_3} не пересекаются и содержат по 4 множества.

Утверждение. Для любого $A \in \mathcal{G}$, отличного от C , множество X_A не содержит ни одного из элементов x_1, x_2, x_3 .

Доказательство. Пусть $x_1 \in X_A$; тогда, очевидно, $x_1 \notin A$. Заметим, что один из двух элементов x_2, x_3 также не лежит в A , ибо $G_{x_2} \cap G_{x_3} = \emptyset$; пусть для определённости $x_2 \notin A$. Предположим, что $x_2 \notin X_A$. Обозначим четыре множества, содержащие x_2 , через B_1, B_2, B_3, B_4 ; все они не содержат x_1 . Пересечение любых двух из них есть $\{x_2\}$; значит, все множества $B_i \cap X_A$ не пересекаются. Таким образом, X_A и состоит из этих четырёх пересечений (ибо $|X_A| = 4$), а они не содержат x_1 . Это противоречит тому, что $x_1 \in X_A$.

Итак, мы получили, что $x_1, x_2 \in X_A$. Предположим теперь, что $x_3 \notin X_A$. В семействе G_{x_3} есть хотя бы три множества, отличных от A . Тогда они должны пересекаться с X_A по различным элементам, отличным от x_1, x_2 . Это опять же невозможно, ибо $|X_A| = 4$.

Итак, $X_A = \{x_1, x_2, x_3, y\}$ при некотором $y \neq x_4$. Рассмотрим теперь два множества $B, B' \in \mathcal{G}$, не лежащее в G_{x_i} при $i = 1, 2, 3$ и не совпадающие с A, C (такие множества найдутся, ибо $|G_{x_1}| + |G_{x_2}| + |G_{x_3}| + 2 = 14 = |\mathcal{G}| - 2$). Тогда $\emptyset \neq B \cap X_C$, поэтому $x_4 \in B$. Аналогично, $y \in B$, а также $x_4, y \in B'$. Значит, $|B \cap B'| \geq 2$, что невозможно. $\square$

Итак, мы знаем, что $h(x_1) = h(x_2) = h(x_3) = 1$ и $g(x_1) = g(x_2) = g(x_3) = 4$. Значит, $P(C) \geq 3 \cdot \frac{12}{1} + p(x_4) > 36$. С другой стороны, по лемме 7 существует $C \in \mathcal{G}$ такое, что $P(C) \leq db = 30 < 36$. Это противоречие завершает доказательство.

$b(2; 2) = 10$. Предположим, что $|\mathcal{G}| = 11$; тогда из леммы 5 следует, что $h(x) \leq 2$ при всех x , а из задачи 5.13 — что $g(x) \leq 6$. Тогда из задачи 5.14 следует, что при $h(x) = 2$ мы имеем $g(x) = 6$. Значит, если $g(x)$ принимает значение 4, 5 или 6, то величина $p(x)$ не может быть меньше, чем 12, 20 или $\frac{30}{2} = 15$, соответственно.

По лемме 7, существует $C \in \mathcal{G}$, для которого $P(C) \leq 2 \cdot 10 = 20$. Пусть $X_C = \{x, y\}$, причём $g(x) \geq g(y)$. Заметим, что $g(x) + g(y) \geq |G_x \cup G_y| = 10$, так что $g(x) \geq 5$, $g(y) \geq 4$. Тогда $P(C) \geq 15 + 12 = 27$. Противоречие.

$b(3; 2) = 15$. Пусть $|\mathcal{G}| = 16$. Действуя аналогично предыдущему решению, мы получаем $h(x) \leq 3$, $g(x) \leq 10$, причём при $h(x) = 1, 2, 3$ мы имеем соответственно $g(x) \geq 5, 8, 10$.

Далее, из леммы 7 мы находим $C \in \mathcal{G}$ такое, что $P(C) \leq 3 \cdot 15 = 45$. Пусть $X_C = \{x, y\}$ и $g(x) \geq g(y)$. Тогда $g(x) \geq 8$, поэтому $p(x) \geq 28$; также $p(y) \geq 20$, ибо $g(y) \geq 5$. Значит, $P(C) \geq 48$. Противоречие.

$b(4; 2) = 21$. Действуя аналогично предыдущим пунктам, находим $C \in \mathcal{G}$ такое, что $P(C) \leq 84$. Если $X_C = \{x, y\}$ и $g(x) \geq g(y)$, то аналогичное противоречие получается всегда, кроме случая $g(y) = 6$; но тогда должно получиться $g(x) = 15$ и $h(x) = 4$ (иначе опять $P(C) > 84$).

Рассмотрим этот случай отдельно. Поскольку $h(x) = 4$, должны существовать множества C_1, C_2, C_3, C_4 такие, что $h(C_i) = \{x, y_i\}$. Тогда есть $22 - g(x) - h(x) = 3$ множества B_1, B_2, B_3 такие, что $x \notin B_i$ и $x \notin X_{B_i}$. Из свойств множеств X_{C_j} следует, что $\{y_1, y_2, y_3, y_4\} \subseteq B_i$. Значит, любые два из множеств B_i должны пересекаться ровно по элементам y_1, y_2, y_3, y_4 .

Наконец, для любого $C \in \mathcal{G}$, отличного от B_i , множество X_C пересекает все B_i ; значит, один его элемент содержится в двух множествах из B_i . Значит, в X_C содержится один из y_1, y_2, y_3, y_4 . Отсюда следует, что $\sum_i h(y_i) \geq 22 - 3 = 19$; но тогда $h(y_i) \geq 5$ при некотором i . Как мы уже отмечали выше, это невозможно.

Замечание. Развивая эти методы, авторы смогли доказать равенство $a(d; 2) = b(d; 2) = C_{d+2}^2$ для всех $d \leq 7$.

The Helly–Gallai numbers for the families of finite and quasi-finite sets

I.I. Bogdanov, G.R. Chelnokov, V.L. Dolnikov

1 Introduction

Typical problem. *In a city there are some bus routes. Every two routes have at most two common bus stops. Moreover, for each 10 routes there exist two stops A and B such that each among out ten routes passes through at least one of the stops A and B . Prove that there exist two stops such that each route in the city passes through at least one of them.*

Also show that the problem statement does not remain valid after replacing the number 10 by a smaller number. (See problem 5.4b).)

If you are familiar with this type of problems (and you like them) you may skip the preliminary text and just start working on the problems.

One of the widespread types of questions in combinatorics is the following one. Given a family $\mathcal{F}$ of sets, we need to determine whether it is possible to select few elements (usually a prescribed number of them) so that each set in $\mathcal{F}$ contains at least one selected element. (Such selection is called a *transversal* for $\mathcal{F}$.) Such questions are important, for instance, in investigating the colorings of (hyper)graphs (and thus have applications in many areas of mathematics); also such questions are very popular in convex geometry. Despite the popularity of this type of questions, many of them are still unsolved, sometimes even those looking quite innocent.

As an example, we present a known Erdős–Faber–Lovasz conjecture which is neither proved nor disproved at the present moment.

Conjecture. *In a city there are some bus routes and n bus stops. Suppose that each route passes through at least two stops, and each two routes have at most one stop in common. Then all the routes can be colored in colors so that no two routes of the same color have a common station.*

Obviously, the necessary condition for the certain family of set to have a transversal of fixed size is that each its subfamily also has such a transversal. For some special kinds of families, it is sufficient to verify this condition for all the subfamilies of a certain size. The famous result of this type is Helly’s theorem for planar convex sets (see problem 2.4); it deals with the 1-transversals.

The first our principal goal is to investigate this type of questions for the families of sets of bounded finite cardinality (section 4). The next goal is to generalize these results for the case of families of sets with some finiteness conditions for their intersections. This type of families is important, e.g., since the conditions of such kind hold for the *algebraic* sets (i.e. the sets of solutions of certain systems of algebraic equations).

The solution of some problems in this project is not known at the present moment. In this case we ask the question of the type “How far can you improve the estimate?”. For such type of problems, we accept any **serial** bound (that is, a bound that works for infinite number of values of parameters). Please keep in mind that serious improvement of known results in this area is worth being published.

The problems marked by the triangle sign[▽] were given at the semifinal.

2 Introduction to the Helly numbers

2.1. Consider a family of segments in a line. Suppose that the intersection of all segments of this family is empty. Prove that there exist two segments in this family, such that their intersection is empty.

2.2. Consider a tree G (i.e. a connected graph without cycles). Consider the finite family of connected subgraphs of G such that the intersection of all these subgraphs is empty. Prove that there exist two subgraphs in this family, such that their intersection is empty.

2.3. Consider a finite family of arcs of some fixed circle. Suppose that every 1000 arcs of this family have a nonempty intersection. Show that all the arcs of the family do not necessarily have a nonempty intersection.

All the three problems above deal with the same property of some family of sets; for instance, in problem 2.1 we work with the family of all segments in the line. Now we define the property.

Definition 1. Let $\mathcal{F}$ be some (not necessarily finite) family of sets. A positive integer k is called a Helly number for the family $\mathcal{F}$ if the following statement holds:

Let $\mathcal{G}$ be an arbitrary finite subfamily of $\mathcal{F}$. Suppose that the intersection of all sets in $\mathcal{G}$ is empty. Then there exist at most k sets in $\mathcal{G}$ such that their intersection is empty.

In other words, k is a Helly number of the set $\mathcal{F}$ if the following “Helly type statement” takes place:

Let $\mathcal{G}$ be an arbitrary finite subfamily of $\mathcal{F}$. Assume that for every k sets in $\mathcal{G}$, their intersection is nonempty. Then the intersection of all the sets in $\mathcal{G}$ is also nonempty.

Using the introduced notation, one can reformulate the problems 1.1–1.2 as follows: number 2 is a Helly number for both the family of the segments in a line and the family of all subtrees of some fixed tree. The statement of problem 1.3, after a similar reformulation, claims that there is no Helly number for the family of all the arcs of a fixed circle.

Definition 2. Let $\mathcal{F}$ be a family of sets. We write $H(\mathcal{F}) = k$ if k is the minimal Helly number for the family $\mathcal{F}$ (provided that there exists some Helly number for $\mathcal{F}$). If there is no Helly number for $\mathcal{F}$, then we write $H(\mathcal{F}) = \infty$.

The next problems will help you to get acquainted with the Helly numbers.

2.4. (HELLEY’S THEOREM FOR THE CONVEX SETS IN THE PLANE.) Let $\mathcal{C}$ be the family of all convex sets in the plane. Prove that $H(\mathcal{C}) = 3$.

Remark. For the problem above, the condition that the family $\mathcal{G} \subset \mathcal{C}$ is finite (in Definition 1) may be replaced with the condition that all sets of $\mathcal{C}$ are closed and bounded.

2.5. Let $\mathcal{P}$ be the family of all infinite increasing arithmetic progressions consisting of positive integers. Prove that $H(\mathcal{P}) = 2$.

2.6. Let $\mathcal{O}$ be the set of all the circumferences in the plane. Find $H(\mathcal{O})$. (**Reminder.** A circumference is a boundary of a disk in the plane.)

3 Introduction to the Helly–Gallai numbers

We need a bit more general concept than the Helly numbers.

Definition 3. Let $\mathcal{F}$ be a family of sets. A set X is a transversal for the family $\mathcal{F}$ if $X \cap A \neq \emptyset$ for all $A \in \mathcal{F}$. A transversal X is called a t -transversal if $|X| = t$.

Remark. For any family $\mathcal{F}$, the existence of a 1-transversal is equivalent to the condition that the intersection of all sets of $\mathcal{F}$ is nonempty.

Definition 4. Let $\mathcal{F}$ be a family of sets. A positive integer k is called a t -Helly–Gallai number for $\mathcal{F}$ if the following statement holds:

Let $\mathcal{G}$ be an arbitrary finite subfamily of $\mathcal{F}$. Suppose that there is no t -transversal for $\mathcal{G}$. Then there exists a subfamily of at most k sets in $\mathcal{G}$ also admitting no t -transversal.

Next, if there exists a t -Helly–Gallai number for a family $\mathcal{F}$, then we will denote by $HG_t(\mathcal{F})$ the minimal such number. Otherwise we write $HG_t(\mathcal{F}) = \infty$.

Remark. Note that by definition we have $H(\mathcal{F}) = HG_1(\mathcal{F})$, so the new concept is a generalization of the Helly numbers introduced above..

Again, the next problems aim to help to get acquainted with a new notion.

3.1. Let $\mathcal{S}$ be the family of segments in the line.

- a) Prove that $HG_2(\mathcal{S}) = 3$
- b) Prove that $HG_t(\mathcal{S}) = t + 1$.

3.2. a) Construct a family $\mathcal{F}$ such that $H(\mathcal{F}) = 2$ but $HG_2(\mathcal{F}) \geq 1000$.

- b) Prove that there exists a family $\mathcal{F}$ such that $H(\mathcal{F}) = 2$ but $HG_2(\mathcal{F}) = \infty$.

3.3. Prove that $HG_2(\mathcal{C}) = \infty$. (Recall that $\mathcal{C}$ is the family of all convex sets in the plane.)

3.4*. Denote by $\mathcal{L}$ the family of all the lines in the plane.

- a) Prove that $HG_t(\mathcal{L}) \leq t^2 + 1$ for all $t \geq 3$.
- b) How far can you improve this bound?

4 Families of sets of bounded cardinality and their Helly–Gallai numbers

One can see from the previous section that the existence of a finite Helly number for some family $\mathcal{F}$ does not necessarily imply that the Helly–Gallai numbers of this family are finite. Thus, one needs some additional conditions on the family $\mathcal{F}$. One of such natural conditions is the boundedness of all the cardinalities of the sets in $\mathcal{F}$.

Definition 5. Denote by $\mathcal{N}_d$ the family of all sets having at most d elements each.

4.1. Let $\mathcal{G}$ be some finite family of sets having at most d elements each. Suppose that every $d + 1$ sets of $\mathcal{G}$ have a nonempty intersection. Prove that the intersection of all the sets of $\mathcal{G}$ is nonempty.

Moreover, show that in the previous statement, the number $d + 1$ can not be replaced with d .

Comprehension exercise. Reformulate this problem with the use of terminology introduced above.

4.2. Prove that all the numbers of the form $HG_t(\mathcal{N}_d)$ are finite.

4.3. a) Prove that $HG_t(\mathcal{N}_2) \geq C_{t+2}^2$.

- b) Prove that $HG_t(\mathcal{N}_2) = C_{t+2}^2$.

4.4. Prove that $HG_t(\mathcal{N}_d) \geq C_{d+t}^t$.

4.5*. (THE PRINCIPAL RESULT OF THIS SECTION) Prove that $HG_t(\mathcal{N}_d) = C_{d+t}^t$.

The problem above is tough. The next problem may be used as a hint.

4.6. a) (Katona’s problem) Assume that the sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ are chosen so that $|A_i| = d$, $|B_i| = t$, for $i \neq j$ the set A_i has at least one common element with the set B_j , but $A_i \cap B_i = \emptyset$. Prove that $n \leq C_{d+t}^t$.

- b) Assuming that Katona’s problem is solved, prove the problem 4.5.

4.7.[∇] Assume that the sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ satisfy *Katona’s conditions*, i.e. $A_i \cap B_i = \emptyset$ and $A_i \cap B_j \neq \emptyset$ for all $i \neq j$. Let $a_i = |A_i|$, $b_i = |B_i|$. Prove that $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} \leq 1$.

The previous problem presents the constraints for the cardinalities of the sets satisfying Katona’s conditions. The next problem shows that this constraint is far from being sufficient.

4.8.[∇] Prove that there exist positive integers $a_1, \dots, a_n, b_1, \dots, b_n$ such that (i) $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} < \frac{1}{10^{100}}$, but (ii) there are no sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ satisfying Katona’s conditions such that $|A_i| = a_i$, $|B_i| = b_i$.

5 The Helly–Gallai numbers for the quasi-finite sets

In this section we weaken the conditions for the families considered.

Definition 6. Let $\mathcal{F}$ be a family of sets. We say that $\mathcal{F}$ is a family of degree d if for every two distinct sets $A, B \in \mathcal{F}$ we have $|A \cap B| \leq d$.

Now let us fix arbitrary positive integers d and t . Next, for every family $\mathcal{F}$ of degree d let us find its (minimal) t -Helly–Gallai number $HG_t(\mathcal{F})$. Denote by $a(d; t)$ the maximal among these numbers.

In other words, $a(d; t)$ is a minimal number which is a Helly–Gallai number for every family $\mathcal{F}$ of degree d .

This section is devoted to different bounds for the numbers $a(d; t)$;

5.1. Let $\mathcal{F}$ be a family of sets. Suppose that $|A \cap B| = 1$ for every distinct $A, B \in \mathcal{F}$ (in particular, this condition implies that $\mathcal{F}$ is a family of degree 1). Suppose, in addition, that among any four sets in $\mathcal{F}$, there exists three sets having a nonempty intersection. Prove that one can delete one of the sets from $\mathcal{F}$ so that all the remaining sets will have a nonempty intersection.

5.2. Let $\mathcal{F}$ be a family of sets. Suppose that $\mathcal{F}$ contains at least 17 sets, and for every distinct $A, B \in \mathcal{F}$ we have $|A \cap B| = 1$. Moreover, suppose that among any 5 sets in $\mathcal{F}$, there are three sets with a nonempty intersection. Prove that there exists a 2-transversal for $\mathcal{F}$.

5.3. Prove that $a(d; 1) = d + 2$.

5.4. a) Prove that $a(1; 2) = 6$.

b) Prove that $a(2; 2) = 10$.

c) Prove that $a(3; 2) = 15$.

d) Prove that $a(4; 2) = 21$.

e)* Try to prove the analogous statement for some larger values of n .

5.5. a) Prove that $a(d; 2) \geq C_{d+3}^2$.

b) Prove that $a(d; 2) \leq 2d^2 + 3$ for all $d \geq 2$.

c)* How far can you improve these bounds?

Remark. In the problem above, the authors can improve the upper bound (that from part b)), but still there is a substantial gap between the upper and the lower bounds. It would be very interesting to obtain upper and lower bounds which are asymptotically the same; that is, their ratio should tend to 1 as $d \rightarrow \infty$.

5.6. a) Prove that $a(1; 3) = 10$.

b) Prove that $a(1; 4) = 15$.

c)* For which values of t you can prove the analogous statement?

5.7. a) Prove that $a(1; t) \geq C_{t+2}^2$.

b) Prove that $a(1; t) \leq t^2 + 1$ for all $t \geq 3$.

c)* How far can you improve these bounds?

5.8. a) Prove that $a(d; t) \geq C_{d+t+1}^t$.

b)** Do there exist the values of d and t such that the inequality in a) is strict?

Remark. The authors do not know the answer for 5.8b).

5.9. a) Prove that the number $a(d; t)$ is finite for every pair (d, t) .

b) Try to obtain a good¹ bound for the number $a(d; t)$.

The remaining part of the text was given at the semifinal.

The next notion for the quasi-finite sets is analogous to Katona's conditions.

Definition 7. Let $\mathcal{G}$ be a finite family of sets. We say that $\mathcal{G}$ is $(d; t)$ -exceptional if (i) $\mathcal{G}$ is a family of degree d , and (ii) for every $A \in \mathcal{G}$ there exists a set X_A with $|X_A| = t$ such that $X_A \cap A = \emptyset$ but $X_A \cap B \neq \emptyset$ for all $B \in \mathcal{G}$ different from A .

Denote by $b(d; t)$ the maximal cardinality of a $(d; t)$ -exceptional family. (We set $b(d; t) = \infty$ if there exist $(d; t)$ -exceptional families of an arbitrary large cardinality.)

¹as good as possible...

5.10.[▽] Prove that $b(d; t) \geq a(d; t)$.

5.11.[▽] Prove that the number $b(d; t)$ is finite for all d and t .

The next problems in this section are devoted to the investigation of exceptional families.

From now on, we fix positive integers d and t ; we also fix some $(d; t)$ -exceptional family $\mathcal{G}$. Recall that for every $A \in \mathcal{G}$ we fix one set X_A such that $|X_A| = t$, $X_A \cap A = \emptyset$, but $X_A \cap B \neq \emptyset$ for all $B \in \mathcal{G}$ distinct from A .

Definition 8. Let x be some element. Denote by $g(x)$ the number of the sets $A \in \mathcal{G}$ such that $x \in A$. Denote by $h(x)$ the number of the sets $A \in \mathcal{G}$ such that $x \in X_A$.

5.12.[▽] a) Assume that $t = 2$. Prove that $h(x) \leq d + 2$ for every x .

b) Prove that $h(x) \leq b(d; t - 1)$ (for an arbitrary t).

5.13.[▽] Prove that $g(x) \leq b(d - 1; t)$ for every x .

5.14.[▽] Assume that $t = 2$ and $h(x) \leq d$. Prove that $|\mathcal{G}| \leq g(x) + h(x) + b(d - h(x); 2)$.

6 The Helly–Gallai numbers for the two-dimensional quasi-finite sets

The families considered in the previous section may be regarded as *1-dimensional* since the intersection of any two of them is finite. In particular, setting $t = 1$ we get a combinatorial analogue of a family of lines. In the same way, we may define *2-dimensional* families as follows.

Definition 9. Let $\mathcal{F}$ be a family of sets. Let $\mathcal{F}'$ be the family of all the intersections of two distinct elements from $\mathcal{F}$, i.e.

$$\mathcal{F}' = \{A \cap B : A, B \in \mathcal{F}, A \neq B\}.$$

We say that $\mathcal{F}$ is a 2-dimensional family of degree d if $\mathcal{F}'$ is a (1-dimensional) family of degree d .

Now let us fix some positive integers d and t . For every 2-dimensional family $\mathcal{F}$ of degree d , consider its (minimal) t -Helly–Gallai number $HG_t(\mathcal{F})$. Denote by $a_2(d; t)$ the maximal such number.

In this section, we do not propose an explicit investigation agenda. Instead of that, we propose you to investigate the numbers $a_2(d; t)$ by yourself. We will accept all the results about these numbers. The problems below mark only some natural directions of investigation.

6.1.[▽] Prove that all the numbers $a_2(d; t)$ are finite.

6.2.[▽] Assume that $d = 0$. Give the necessary definitions on your own and prove that $g(x) \leq t + 1$.

6.3.[▽] (INVESTIGATORY, “WITH NO DOUBLE INTERSECTIONS”) Find some upper and lower bounds for the numbers $a(0; t)$ for some values of t .

6.4.[▽] (INVESTIGATORY, “THE CASE OF PLANES”) Find some upper and lower bounds for the numbers $a(1; t)$ for some values of t .

6.5.[▽] (INVESTIGATORY, A GENERAL CASE) Find some upper and lower bounds for the numbers $a(d; t)$ for some values of d and t .

Remark. In the last three problems, as usual, serial bounds are more valuable than partial results for fixed values of $(d; t)$. Nevertheless, we insistently recommend you to start with a consideration of a sufficient amount of particular cases.

The Helly–Gallai numbers for the families of finite and quasi-finite sets.

I.I. Bogdanov, G.R. Chelnokov, V.L. Dolnikov

Solutions.

2.1. Consider a family of segments in a line. Suppose that the intersection of all segments of this family is empty. Prove that there exist two segments in this family, such that their intersection is empty.

Denote the given segments as $[a_1, b_1], \dots, [a_n, b_n]$. Let $a_s = \max_{1 \leq i \leq n} a_i$, $b_t = \min_{1 \leq i \leq n} b_i$ (it is possible that $s = t$). If $a_s \leq b_t$ then each given segment contains a_s , which contradicts the condition of the problem. Hence $a_s > b_t$, therefore $t \neq s$, and the s th segment has no common point with the t th one.

2.2. Consider a tree G (i.e. a connected graph without cycles). Consider the finite family of connected subgraphs of G such that the intersection of all these subgraphs is empty. Prove that there exist two subgraphs in this family, such that their intersection is empty.

If we delete any edge e from a tree G , we cut this tree into two components. Moreover, if a subtree G' does not contain e , then it lies in one of these components.

Denote our subtrees by $G_1, \dots, G_n$. Let k be a maximal integer such that the intersection $G = G_1 \cap G_2 \cap \dots \cap G_k$ is nonempty (note that $k < n$). Then the intersection of G and G_{k+1} is empty.

Now consider a shortest path connecting G with G_{k+1} . The first edge e of this path does not belong to G , hence some G_i (with $1 \leq i \leq k$) also does not contain e . Let us delete this edge. The subtrees G_{k+1} and G come to different components of the remaining graph. Therefore G_{k+1} and G_i are also in different components. Hence their intersection is empty.

2.3. Consider a finite family of arcs of some fixed circle. Suppose that every 1000 arcs of this family have a nonempty intersection. Show that all the arcs of the family do not necessarily have a nonempty intersection.

Partition the circle into 1001 arcs (we call them *small* arcs). We call a complement of any small arc a *large* arc. We claim that the family of large arcs is a desired example. Namely, it is easy to check that the intersection of any 1000 large arcs is nonempty, but the intersection of all of them is obviously empty.

Remark. The large arcs in the solution are assumed not to contain their endpoints. One may decrease them slightly to obtain an example consisting of closed arcs.

2.4. (HELLY'S THEOREM FOR THE CONVEX SETS IN THE PLANE.) Let $\mathcal{C}$ be the family of all convex sets in the plane. Prove that $H(\mathcal{C}) = 3$.

Induction on the number $n \geq 4$ of the considered convex sets. The base case is $n = 4$. Consider our convex sets F_1, F_2, F_3, F_4 . Let x_i be a point of intersection of all of them except F_i . We apply the following lemma.

Lemma 1 (Radon's theorem). One can partition any four points in the plane into two sets so that the convex hulls of these sets have a common point.

Proof. Consider two cases: (i) the points are the vertices of some convex quadrilateral, and (ii) one of the points lies inside the triangle formed by the other three. $\square$

So, suppose for example that the convex hulls of the sets $\{x_1, x_2\}$ and $\{x_3, x_4\}$ intersect at point x . Then x lies in F_3 and F_4 , since the whole segment x_1x_2 lies in these sets. Analogously, $x \in F_1 \cap F_2$. All the other cases are completely analogous.

For the induction step, assume that $n \geq 4$ and consider $n + 1$ convex sets $F_1, \dots, F_{n+1}$. Let us construct a new family consisting of n convex sets $F'_1 = F_1 \cap F_{n+1}, \dots, F'_n = F_n \cap F_{n+1}$. By the statement of the base case, each three of the new sets have a nonempty intersection. Then, by the induction hypothesis, all the new sets have a common point, QED.

2.5. Let $\mathcal{P}$ be the family of all infinite increasing arithmetic progressions consisting of positive integers. Prove that $H(\mathcal{P}) = 2$.

Let $\mathcal{G}$ be a finite family of progressions such that every two of them have a common element. Note that the intersection of each two progressions from $\mathcal{G}$ is infinite (in fact, it is an infinite progression as well). So, with no loss of generality we may assume that the i th progression is defined by the condition $x \equiv a_i \pmod{n_i}$ (for that, we need only to “forget” about some initial segment of the row of the positive integers).

Consider one of our progressions; say it is defined by $x \equiv a \pmod{n}$. This condition is equivalent to the system of the relations having the form $x \equiv a \pmod{p_j^{\alpha_j}}$ (here, $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ is the prime decomposition of n). Now, let us write down such a system for each progression. We need to prove that the system of all obtained relations is collocated (i.e. has a solution).

Note that every two relations in our system are collocated, since they correspond either to one or to two progressions. Next, suppose that the system contains two equivalences modulo the powers of the same prime p (say $x \equiv a \pmod{p^\alpha}$ and $x \equiv b \pmod{p^\beta}$). These relations are collocated; we may assume that $\alpha \geq \beta$. Then the latter relation is a consequence of the former one, so we may delete the latter from the system.

Performing such steps, we finally arrive to a system where all moduli are the powers of distinct primes. Such a system has a solution by the Chinese Remainder Theorem.

Remark. One may show that for every $t \geq 2$, there are no t -Helly–Gallai numbers for the set of out progressions,

2.6. Let $\mathcal{O}$ be the set of all the circumferences in the plane. Find $H(\mathcal{O})$.

Answer. $H(\mathcal{O}) = 4$.

Firstly, we prove that 4 is a Helly number for $\mathcal{O}$. Consider a finite family $\mathcal{G}$ of circumferences such that the intersection of all of them is empty. Consider arbitrary different circumferences $O_1, O_2 \in \mathcal{G}$. They have at most two points of intersection. Denote these points by A and B (if some of these points do not exist, the arguments are the same).

Recall that no point belongs to all the circumferences. Therefore there exist $O_3, O_4 \in \mathcal{G}$ such that $A \notin O_3$ and $B \notin O_4$. Hence O_1, O_2, O_3, O_4 have no common points, as desired.

We are left to present an example showing that $H(\mathcal{O}) > 3$. Consider a noncyclic nondegenerate quadrilateral $ABCD$. Consider four circumcircles of the triangles ABC, ABD, ACD, BCD . Each three of them have a nonempty intersection but all four do not.

3.1. Let $\mathcal{S}$ be the family of segments in the line.

a) Prove that $HG_2(\mathcal{S}) = 3$

b) Prove that $HG_t(\mathcal{S}) = t + 1$.

Item a) is a particular case of b); so we present only a solution for the latter one.

Denote the segments under consideration as $[a_1, b_1], \dots, [a_n, b_n]$. Denote by c_1 the minimal number among all b_i 's. Then each our segment either contains c_1 or lies to the right of c_1 . Denote by c_2 the minimal b_i such that the segment $[a_i, b_i]$ lies to the right of c_1 . Analogously, we get that each our segment either contains c_1 or c_2 , or lies to the right of c_2 .

Proceeding in the same way while it is possible, we finally get the sequence $c_1, c_2, \dots, c_k$ such that each segment contains at least one of these k numbers. So, if $k \leq t$ then we have found a desired transversal. Assume now that $k \geq t + 1$. Consider $t + 1$ segments with the right ends $c_1, \dots, c_{t+1}$; by our choice, they are pairwise disjoint, so they do not admit a t -transversal.

Thus, we have proved that either all the segments have a t -transversal, or there are $t + 1$ pairwise disjoint segments. This means that $t + 1$ is a t -Helly–Gallai number for the segments in the line. Finally, an obvious example of $t + 1$ pairwise disjoint segments shows that $HG_t(\mathcal{S}) > t$.

3.2. a) Construct a family $\mathcal{F}$ such that $H(\mathcal{F}) = 2$ but $HG_2(\mathcal{F}) \geq 1000$.

b) Prove that there exists a family $\mathcal{F}$ such that $H(\mathcal{F}) = 2$ but $HG_2(\mathcal{F}) = \infty$.

a) Set $k = 500$. We construct a family $\mathcal{F}$ of $2k + 1$ sets $A_1, \dots, A_{2k+1}$ (all indices are considered modulo $2k + 1$; thus $A_i = A_{2k+1+i}$) as follows. Firstly, consider a set of indices $S \subset \{1, 2, \dots, 2k + 1\}$ which does not contain two indices with difference 1 (in particular, we prohibit the situation $1, 2k + 1 \in S$). For each such set S , we introduce an element x_S (the elements for different sets should be different as well). Next, we define $A_k = \{x_S : k \in S\}$.

The obtained family has a Helly number 2. Indeed, assume that a subfamily $\mathcal{G} \subset \mathcal{F}$ has an empty intersection; let $\mathcal{G} = \{A_i : i \in I\}$. If I contains two indices i and $i + 1$ with difference 1, then $A_i, A_{i+1} \in \mathcal{G}$ and $A_i \cap A_{i+1} = \emptyset$. Otherwise all the sets in $\mathcal{G}$ contain x_I which is impossible.

Finally, we claim that every $2k$ sets from $\mathcal{F}$ have a 2-transversal while all $2k + 1$ sets do not. Assume that $\mathcal{F}$ admits a 2-transversal $\{x_S, x_T\}$ with $|S| \geq |T|$. Then $|S| \geq k + 1$, and hence S contains two neighboring indices which is impossible. On the other hand, let us delete A_{2k+1} from $\mathcal{F}$; all the other sets have a 2-transversal $\{x_S, x_T\}$ where $S = \{1, 3, \dots, 2k - 1\}$ and $T = \{2, 4, \dots, 2k\}$.

Thus, $HG_2(\mathcal{F}) = 2k + 1$.

b) For every positive integer k , let us construct a family $\mathcal{F}_k$ as above. We may assume that the sets from different families have no common elements. Then it is easy to show that the union $\mathcal{F} = \mathcal{F}_1 \cup \mathcal{F}_2 \cup \dots$ satisfies all the requirements.

3.3. Prove that $HG_2(\mathcal{C}) = \infty$. (Recall that $\mathcal{C}$ is the family of all convex sets in the plane.)

It suffices to prove that $HG_2(\mathcal{C}) \geq 2k + 1$ for every positive integer k . Consider a circle with center O ; let $x_1, \dots, x_{2k+1}$ be the vertices of a regular $(2k + 1)$ -gon inscribed into this circle (again, we regard the indices modulo $2k + 1$). Let A_i be a convex hull of the points $x_i, \dots, x_{i+k-1}$. Then all the considered sets except any of them admit a 2-transversal (e.g., $\{x_k, x_{2k}\}$ is a 2-transversal for all the sets except A_{2k+1}).

On the other hand, we claim that each point T belongs to not more than k sets. Actually, let the ray OT intersect the boundary of $(2k + 1)$ -gon on the semiinterval $(x_{i-1}, x_i]$. Then T may belong only to the sets $A_{i-k+1}, \dots, A_i$ as desired.

Hence our family of cardinality $(2k + 1)$ does not admit a 2-transversal, QED.

3.4*. Denote by $\mathcal{L}$ the family of all the lines in the plane.

a) Prove that $HG_t(\mathcal{L}) \leq t^2 + 1$ for all $t \geq 3$.

b) How far can you improve this bound?

a) Induction on $t \geq 3$. We first prove the induction step; the base case $t = 3$ is investigated further.

Let $\mathcal{G}$ be a finite family of lines such that every $\leq t^2 + 1$ lines from $\mathcal{G}$ have a t -transversal. Choose arbitrary $t^2 + 1$ lines from $\mathcal{G}$. One of the points of their t -transversal should belong to at least $t + 1$ chosen lines. Denote this point by A , and let $\ell_1, \dots, \ell_{t+1} \in \mathcal{G}$ be $t + 1$ lines containing A .

Denote by $\mathcal{G}'$ a subfamily of $\mathcal{G}$ consisting of those lines which do not contain A . We claim that each subfamily $D \subseteq \mathcal{G}$ such that $|D| \leq t^2 - t$ has a $(t - 1)$ -transversal. Actually, we know that the family $D \cup \{\ell_1, \dots, \ell_{t+1}\}$ has a t -transversal X . By the pigeonhole principle, two of the lines $\ell_1, \dots, \ell_{t+1}$ should pass through the same point of X ; hence this point is A , i.e. $A \in X$. Finally, since the lines from D do not contain A , the set $X \setminus \{A\}$ is a transversal of D .

Note now that $t^2 - t \geq (t - 1)^2 + 1 \geq HG_{t-1}(\mathcal{L})$. Hence $\mathcal{G}'$ has a $(t - 1)$ -transversal X by the induction hypothesis; therefore $X \cup \{A\}$ is a desired t -transversal for $\mathcal{G}$.

The proof of the base case follows the same lines except for the last paragraph (namely, the only argument where we use the induction hypothesis). To finish this argument, it suffices to show that $t^2 - t = 6 \geq HG_2(\mathcal{L})$.

Note first that $HG_1(\mathcal{L}) \leq 3$. Actually, if every three lines from $\mathcal{G}$ have a common point, then the intersection point of two of these lines should belong to all the other lines. Finally, the inequality $HG_2(\mathcal{L}) \leq 6$ can be obtained again in the same way as the induction step (with the numbers $t^2 + 1$ and $t^2 - t$ replaced by 6 and 3, respectively).

b) We prove that $HG_t(\mathcal{L}) = C_{t+2}^2$.

Firstly, we show that $HG_t(\mathcal{L}) \geq C_{t+2}^2$. Take $t + 2$ points $T_1, \dots, T_{t+2}$ in a general position, and draw all the lines connecting them. One may show that it is possible to choose the points in such a way that no three lines intersect at a point different from T_i 's. For such arrangement of points, our C_{t+2}^2 lines do not admit a t -transversal, but all the lines except an arbitrary one have a t -transversal.

It remains to prove that $HG_t(\mathcal{L}) \leq C_{t+2}^2$. We will use the following lemma.

Lemma 2. *Let $P_1(x, y), \dots, P_k(x, y)$ be the polynomials in two variables of degree $\leq t$. Suppose that $k > C_{t+2}^2$. Then there exist the numbers $s_1, \dots, s_k$ (not all of them are zeroes) such that $s_1 P_1(x, y) + \dots + s_k P_k(x, y) = 0$.*

Proof. Our conditions on the variables s_i can be rewritten as a system of C_{t+2}^2 linear homogeneous (i.e. with zero constant terms) equations (the number of equations is simply the number of monomials of degree $\leq t$ in two variables). Since the number of variables is strictly greater than the number of equations, this system has a nonzero solution. $\square$

Now we return to the solution. Obviously, it suffices to prove the following statement: If $n \geq C_{t+2}^2$, and every n lines in $\mathcal{G}$ have a t -transversal, then every $n + 1$ lines from $\mathcal{G}$ also have a t -transversal.

Assume the contrary and consider a family $\mathcal{F}$ of $n + 1$ lines violating our statement. Introduce a Cartesian system so that the origin does not lie on any considered line. For an arbitrary index j , the equation of the j th line ℓ_j can be written in the form $a_j x + b_j y + 1 = 0$.

Now let us fix an arbitrary index i for a while. All the lines in $\mathcal{F}$ except ℓ_i have a t -transversal consisting of points $(x_1, y_1), \dots, (x_t, y_t)$ (surely, none of these points lie on ℓ_i). This means that $\prod_{k=1}^t (a_j x_k + b_j y_k + 1) = 0$ for all $j \neq i$, but the same relation is false for $j = i$. Denoting now $P_i(a, b) = \prod_{k=1}^t (a x_k + b y_k + 1)$, we obtain that $P_i(a_j, b_j) = 0$ for all $j \neq i$, but $P_i(a_i, b_i) \neq 0$.

All the obtained polynomials have degree t . By the lemma above, there exist the numbers $s_1, \dots, s_n$ such that $\sum_{i=1}^n s_i P_i(a, b) = 0$. We may assume that $s_1 \neq 0$. Hence we get $\sum_{i=1}^n s_i P_i(a_1, b_1) = s_1 P_1(a_1, b_1) \neq 0$. A contradiction.

4.1. *Let $\mathcal{G}$ be some finite family of sets having at most d elements each. Suppose that every $d + 1$ sets of $\mathcal{G}$ have a nonempty intersection. Prove that the intersection of all the sets of $\mathcal{G}$ is nonempty.*

Moreover, show that in the previous statement, the number $d + 1$ can not be replaced with d .

Comprehension exercise. *Reformulate this problem with the use of terminology introduced above.*

The problem statement can be rewritten as $H(\mathcal{N}_d) = d + 1$.

Let $\mathcal{G}$ be a family of all subsets with d elements in some fixed set X of cardinality $d + 1$. Then each d elements have a common element but the whole family does not. Thus, $H(\mathcal{N}_d) \geq d + 1$.

Consider now an arbitrary finite subfamily $\mathcal{G} \subset \mathcal{N}_d$ such that each $d + 1$ sets in $\mathcal{G}$ share a common element. For every $i = 1, \dots, d + 1$, denote by s_i the minimal cardinality of the intersection of some i sets from $\mathcal{G}$. Obviously, $1 \leq s_{d+1} \leq s_d \leq \dots \leq s_1 = d$. It follows that $s_{j+1} = s_j$ for some $j \in [1, d]$.

Consider now the sets $A_1, \dots, A_j \in \mathcal{G}$ such that $|Q| = s_j$, where $Q = A_1 \cap \dots \cap A_j$. Assume that $Q \not\subseteq A$ for some $A \in \mathcal{G}$; then we get $s_{j+1} = s_j > |Q \cap A| = |A_1 \cap \dots \cap A_j \cap A|$ which contradicts to the definition of s_{j+1} . Thus, all the sets in $\mathcal{G}$ contain a nonempty set Q , QED.

4.2. *Prove that all the numbers of the form $HG_t(\mathcal{N}_d)$ are finite.*

Surely, this problem is a corollary of the problem 4.5. Here we present an easier proof.

Induction on t . The base case $t = 1$ follows from the previous problem.

For the induction step, assume that $HG_{t-1}(\mathcal{N}_d) = S < \infty$. We prove that $HG_t(\mathcal{N}_d) \leq T = S + C_{Sd}^t$.

Consider an arbitrary finite subfamily $\mathcal{G} \subset \mathcal{N}_d$ such that every T sets in $\mathcal{G}$ have a t -transversal. If every S sets of $\mathcal{G}$ have $(t - 1)$ -transversal, then the family $\mathcal{G}$ has even a $(t - 1)$ -transversal by the induction hypothesis. Otherwise, there exists a subfamily $\mathcal{K} = \{A_1, \dots, A_S\} \subset \mathcal{G}$ which has no $(t - 1)$ -transversal. Thus each t -transversal of the family $\mathcal{K}$ should be contained in the set $Q = A_1 \cup \dots \cup A_S$. Remark that $|Q| \leq Sd$.

Assume now that the family $\mathcal{G}$ has no t -transversal. Then for each t -element subset $X \subset Q$ there exists a set $A_X \in \mathcal{G}$ such that $A_X \cap X = \emptyset$. Now consider the subfamily

$$\mathcal{K}' = \mathcal{K} \cup \{A_X : X \subset Q, |X| = t\}.$$

We have $|\mathcal{K}'| \leq S + C_{Sd}^t = T$. Therefore $\mathcal{K}'$ must have a t -transversal Y . Since $\mathcal{K} \subset \mathcal{K}'$, we have $Y \subset Q$. Finally, by the choice of $\mathcal{K}'$, there exists the set $A_Y \in \mathcal{K}'$ such that $A_Y \cap Y = \emptyset$. This contradiction concludes the proof.

- 4.3.** a) Prove that $HG_t(\mathcal{N}_2) \geq C_{t+2}^2$.
b) Prove that $HG_t(\mathcal{N}_2) = C_{t+2}^2$.

a) See problem 4.4.

b) Follows from problem 4.5.

- 4.4.** Prove that $HG_t(\mathcal{N}_d) \geq C_{d+t}^t$.

It suffices to take a family $\mathcal{G}$ of all d -element subsets of some fixed $(d+t)$ -element set X . Actually, each t -element subset in X has a common element with each set in $\mathcal{G}$ except one.

- 4.5*.** (THE PRINCIPAL RESULT OF THIS SECTION) Prove that $HG_t(\mathcal{N}_d) = C_{d+t}^t$.

See the next problem.

- 4.6.** a) (Katona's problem) Assume that the sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ are chosen so that $|A_i| = d$, $|B_i| = t$, for $i \neq j$ the set A_i has at least one common element with the set B_j , but $A_i \cap B_i = \emptyset$. Prove that $n \leq C_{d+t}^t$.

b) Assuming that Katona's problem is solved, prove the problem 4.5.

a) Follows immediately from problem 4.7.

b) Assume the contrary. Consider a family $\mathcal{G} \subset \mathcal{N}_d$ of minimal cardinality such that every its subfamily with $\leq C_{d+t}^t$ sets has a t -transversal, but $\mathcal{G}$ does not have a t -transversal. Surely, we have $|\mathcal{G}| > C_{d+t}^t$.

Let $\mathcal{G} = \{A_1, \dots, A_n\}$. By our choice, for every $i = 1, \dots, n$ the family $\mathcal{G} \setminus \{A_i\}$ has a t -transversal B_i . By the choice again, we have $A_i \cap B_i = \emptyset$. Thus, the sets $A_1, \dots, A_n, B_1, \dots, B_n$ satisfy the conditions of Katona's problem and hence $|\mathcal{G}| = n \leq C_{d+t}^t$. A contradiction.

- 4.7.** Assume that the sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ satisfy Katona's conditions, i.e. $A_i \cap B_i = \emptyset$ and $A_i \cap B_j \neq \emptyset$ for all $i \neq j$. Let $a_i = |A_i|$, $b_i = |B_i|$. Prove that $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} \leq 1$.

Let $X = A_1 \cup \dots \cup A_n \cup B_1 \cup \dots \cup B_n$; denote $n = |X|$. Consider all $m!$ ways of numbering the elements of X by $1, \dots, m$ (or, equivalently, all bijections $\sigma : X \rightarrow \{1, 2, \dots, m\}$). Consider any such numbering σ ; we say that it is of i th type (for some $1 \leq i \leq n$) if all the elements of A_i have smaller numbers than all the elements of B_i (i.e. $\sigma(a) < \sigma(b)$ for all $a \in A_i$, $b \in B_i$).

Firstly, we note that each numbering is of at most one type. Assume, to the contrary, that σ is of both i th and j th types for $i \neq j$. Denote $a_i = \max_{a \in A_i} \sigma(a)$, $a_j = \max_{a \in A_j} \sigma(a)$; we may assume that $a_i \leq a_j$. Then for every $b \in B_j$ and $a \in A_i$ we have $\sigma(b) > a_j \geq a_i \geq \sigma(a)$; hence $A_i \cap B_j = \emptyset$. This contradiction shows that our claim is valid.

Next, let us estimate the total number of the numberings of i th type. The elements of $A_i \cup B_i$ can be ordered in $(a_i + b_i)!$ ways, and there are exactly $a_i!b_i!$ appropriate ones. Moreover, for each such order, there exists the same number of the numberings realizing this order. Hence the number of the numberings of i th type is exactly $m! \cdot \frac{a_i!b_i!}{(a_i + b_i)!} = m! \cdot \frac{1}{C_{a_i+b_i}^{a_i}}$.

Finally, the total number of the numberings is at least the sum of all the numbers found above, i.e.

$$\sum_{i=1}^n \frac{m!}{C_{a_i+b_i}^{a_i}} \leq m!,$$

QED.

- 4.8.** Prove that there exist positive integers $a_1, \dots, a_n, b_1, \dots, b_n$ such that (i) $\sum_{i=1}^n \frac{1}{C_{a_i+b_i}^{a_i}} < \frac{1}{10^{100}}$, but (ii) there are no sets $A_1, A_2, \dots, A_n, B_1, \dots, B_n$ satisfying Katona's conditions such that $|A_i| = a_i$, $|B_i| = b_i$.

Define $a_1 = 1$, $a_2 = 10^{101}$, $a_3 = 10^{101}$ and $b_1 = 10^{101}$, $b_2 = 1$, $b_3 = 1$. Then each of the sets B_2 and B_3 should have a common element with A_1 . All these three sets are of cardinality 1, so they should coincide. Hence, since $B_2 \cap A_2 = \emptyset$, we also have $B_3 \cap A_2 = \emptyset$ which is impossible.

5.1. *Let $\mathcal{F}$ be a family of sets. Suppose that $|A \cap B| = 1$ for every distinct $A, B \in \mathcal{F}$ (in particular, this condition implies that $\mathcal{F}$ is a family of degree 1). Suppose, in addition, that among any four sets in $\mathcal{F}$, there exists three sets having a nonempty intersection. Prove that one can delete one of the sets from $\mathcal{F}$ so that all the remaining sets will have a nonempty intersection.*

Consider three sets with a nonempty intersection, say $x \in A \cap B \cap C$. Suppose that there exist two different sets D and E not containing x . Consider the four sets A, B, D, E . Some three of them have a common element y ($y \neq x$ since $x \notin D, E$). Then y belongs to at least one of the sets A and B ; without loss of generality, $y \in A$. Next, A and B may have at most one element in their intersection, and $x \in A \cap B$; therefore $y \notin B$. Analogously, $y \notin C$. Then $y \in D$ and $y \in E$, in other case there is no three sets among A, B, D, E covering y .

Consider the four sets B, C, D, E . Among any three of them there are either both B and C , or both D and E . The unique common element of B and C is x , and it does not belong to D or E . Analogously, the unique common element of D and E is y , and it does not belong to B or C . Thus, the four sets B, C, D, E have no element belonging to three of them. This contradiction proves that there exists at most one set in $\mathcal{F}$ not containing x .

5.2. *Let $\mathcal{F}$ be a family of sets. Suppose that $\mathcal{F}$ contains at least 17 sets, and for every distinct $A, B \in \mathcal{F}$ we have $|A \cap B| = 1$. Moreover, suppose that among any 5 sets in $\mathcal{F}$, there are three sets with a nonempty intersection. Prove that there exists a 2-transversal for $\mathcal{F}$.*

Assume that for every four sets in $\mathcal{F}$, there are three with a nonempty intersection. Then, by the previous problem, some element x belongs to all the sets on $\mathcal{F}$ except one. Taking any element y from this exceptional set, we obtain a 2-transversal $\{x, y\}$ of $\mathcal{F}$.

Otherwise, there exist four sets A, B, C, D such that no three of them share a common element. Adding any other set $E \in \mathcal{F}$, we obtain a 5-tuple of sets three of which have a common element; these sets should be E together with some pair of the original four sets, and their common element is a (unique!) common element for this pair. There are 13 ways to choose $E \in \mathcal{F}$ and 6 ways to choose a pair of the original sets. Hence, some pair appears for three choices of E , and its common element x belongs to five sets in $\mathcal{F}$. Now we denote these five sets by X_1, X_2, X_3, X_4, X_5 .

Consider now all the sets in $\mathcal{F}$ not containing x . If there are at most two of them, then their common element y together with x form a desired 2-transversal for $\mathcal{F}$. Next, if every three of these sets have a common element, then it is easy to see that this element y should be the same for all the triples, and $\{x, y\}$ is a 2-transversal for $\mathcal{F}$ again.

In the only case remaining, there exist three sets Y, Z, T not containing x and with no common element. Denote their pairwise common elements by a_1, a_2, a_3 . Note that a_i cannot belong to two of the sets $X_1, \dots, X_5$ since otherwise these two sets have two common elements: x and a_i . Hence, among these five sets there are two (say X_4 and X_5) containing none of a_i 's. Finally, consider five sets X_4, X_5, Y, Z, T ; no three of them have a common element. A contradiction.

Firstly, we will present the solutions of problems 5.10 and 5.12–5.14. We will use them further as lemmas.

In the sequel, by $\mathcal{G}$ we always denote a (d, t) -exceptional family.

One may easily check that $X_A \not\subseteq X_B$ for arbitrary distinct $A, B \in \mathcal{G}$.

We need the following easy lemmas.

Lemma 3. *Let S be some set, $|S| = s$. Consider the subfamily $\mathcal{F} = \{A : A \in \mathcal{G}, S \subseteq X_A\}$. Then $\mathcal{F}$ is a $(d, t - s)$ -exceptional family.*

Proof. If $S \subseteq X_A$ then $S \cap A = \emptyset$. Thus for all distinct $A, B \in \mathcal{F}$ we have $A \cap (X_B \setminus S) = A \cap X_B \neq \emptyset$. Hence, the set $X_A \setminus S$ has a common element with each set in $\mathcal{F}$ except A . Moreover, we have $|X_A \setminus S| = t - s$. That means exactly that $\mathcal{F}$ is $(d; t - s)$ -exceptional. $\square$

Lemma 4. *Let S be some set, $|S| = s$. Consider the family $\mathcal{F} = \{A \setminus S : A \in \mathcal{G}, S \subset A\} \subset \mathcal{G}$. Then $\mathcal{F}$ is a $(d - s, t)$ -exceptional family.*

Proof. For every distinct $A, B \in \mathcal{G}$, we have $|(A \setminus S) \cap (B \setminus S)| = |A \cap B| - s \leq d - s$. Also, since $X_A \cap S = \emptyset$ we have $(B \setminus S) \cap X_A = B \cap X_A \neq \emptyset$. Finally, $(A \setminus S) \cap X_A \subseteq A \cap X_A = \emptyset$. $\square$

5.10. Prove that $b(d; t) \geq a(d; t)$.

It is sufficient to prove that for any integer n , $a(d; t) > n$ implies $b(d; t) > n$.

If $a(d; t) > n$, then there exist a family $\mathcal{G}$ of degree d such that any n sets in $\mathcal{G}$ have a t -transversal, but the whole family does not. Consider the minimal (with respect of number of sets) subfamily $\mathcal{F} \subset \mathcal{G}$ having no t -transversal. Obviously, $|\mathcal{F}| > n$. Since $\mathcal{F}$ is minimal, any subfamily of $\mathcal{F}$ has a t -transversal, thus $\mathcal{F}$ is (d, t) -exceptional. Then $b(d; t) > n$.

Remark. In the sequel, almost all the upper bounds for $a(d; t)$ are in fact the upper bounds for $b(d; t)$. In this case we just omit mentioning that $b(d; t) \geq a(d; t)$.

5.12. a) Let $t = 2$. Prove that $h(x) \leq d + 2$ for arbitrary x .

b) Prove that $h(x) \leq b(d; t - 1)$ for arbitrary d, t, x .

Although item b) is a generalization of item a), we present a separate proof of item a) to clarify the idea.

a) Suppose $h(x) \geq d + 3$, i.e. there exist $A_1, \dots, A_{d+3} \in \mathcal{G}$ such that $X_{A_i} = \{x, x_i\}$ for some elements x_i (obviously, the elements x_i are distinct). Then $\{x_1, x_2, \dots, x_{d+1}\} \subset A_{d+2}$ and $\{x_1, x_2, \dots, x_{d+1}\} \subset A_{d+3}$ which contradicts the condition $|A_{d+2} \cap A_{d+3}| > d$.

b) Applying Lemma 3 for the case $S = \{x\}$, we obtain that the family $\mathcal{F} = \{A \in \mathcal{G} : x \in X_A\}$ is $(d, t - 1)$ -exceptional, thus $h(x) = |\mathcal{F}| \leq b(d; t - 1)$.

5.13. Prove that $g(x) \leq b(d - 1; t)$ for every x .

Applying Lemma 4 to the set $S = \{x\}$, we obtain that $\mathcal{F} = \{A \setminus \{x\} : A \in \mathcal{G}, x \in A\}$ is $(d - 1, t)$ -exceptional, i.e. $g(x) = |\mathcal{F}| \leq b(d - 1; t)$.

5.14. Assume that $t = 2$ and $h(x) \leq d$. Prove that $|\mathcal{G}| \leq g(x) + h(x) + b(d - h(x); 2)$.

Let $B_1, \dots, B_h \in \mathcal{G}$ be all the sets in $\mathcal{G}$ that contain x (then $h = h(x)$). Let $X_{B_i} = \{x, x_i\}$; again all x_i are distinct.

Let $A_1, \dots, A_k \in \mathcal{G}$ be all the sets such that $x \notin A_i$ and $x \notin X_{A_i}$. Since $k = |\mathcal{G}| - g(x) - h(x)$, it is sufficient to prove that $k \leq b(d - h(x); 2)$.

Since $A_i \neq B_j$ for all i and j , we get $\{x, x_j\} \cap A_i \neq \emptyset$. Keeping in mind that $x \notin A_i$ we get $x_j \in A_i$. Denote $Y = \{x_1, \dots, x_h\}$; we have proved that $Y \subset A_i$ for all $i = 1, \dots, k$. Now, applying Lemma 4 for $S = Y$ we get $k \leq b(d - h; 2)$.

Remark. Both the statement and the proof remain valid for the case $h(x) > d$; note that we have $b(d - h; t) = 1$ for $d < h$.

Now, we firstly prove the serial bounds, although using sometimes the sharp partial bounds obtained further.

Since $a(d; t) \leq b(d; t)$ (see problem 5.10) it is sufficient to prove the required upper bounds for $b(d; t)$ instead of $a(d; t)$. Thus in such cases we always consider some $(d; t)$ -exceptional family $\mathcal{G}$ and prove some upper bounds for $|\mathcal{G}|$.

5.8. a) Prove that $a(d; t) \geq C_{d+t+1}^t$.

b)** Do there exist the values of d and t such that the inequality in a) is strict?

a) Consider a set B , $|B| = d + t + 1$. Let $\mathcal{G}$ be the family of all $(d + 1)$ -element subsets of B . Then for any distinct $A_1, A_2 \in \mathcal{G}$ we have $|A_1 \cap A_2| \leq d$. Also, for any $A \in \mathcal{G}$ we put $X_A = B \setminus A$. Thus $|X_A| = t$ and $A_1 \cap X_A \neq \emptyset$ for any distinct $A, A_1 \in \mathcal{G}$. So, $\mathcal{G}$ is (d, t) -exceptional.

b) The solution of this item is still not known.

5.3. Prove that $a(d; 1) = d + 2$.

Suppose that a $(d; 1)$ -exceptional family $\mathcal{G}$ contains at least $d + 3$ sets, say $\{A_1, A_2, \dots, A_{d+3}\} \subseteq \mathcal{G}$. Let $X_{A_i} = \{x_i\}$, all x_i are distinct for $i = 1, \dots, d + 3$. By the definition of a $(d; t)$ -exceptional family we have $x_i \in A_1$ for $i = 3, \dots, d + 3$. Analogously $x_i \in A_2$ for $i = 3, \dots, d + 3$. Thus $|A_1 \cap A_2| \geq |\{x_3, \dots, x_{d+3}\}| = d + 1$. A contradiction.

Remark. Further we will also use an obvious proposition $a(0; t) = b(0; t) = t + 1$.

For the sake of brevity we introduce the following notation.

Definition 1. Let $G_x = \{A \in \mathcal{G} : x \in A\}$ and $H_x = \{A \in \mathcal{G} : x \in X_A\}$ for arbitrary x .

For the induction step in the next problem, we need the following sharpening of the statement of problem 5.12a).

Lemma 5. Assume that $t = 2$ and $|\mathcal{G}| > b(d-1; 2) + d + 3$. Then $h(x) \leq d$ for all x .

Proof. Assume, to the contrary, that there exist $d+1$ distinct sets $A_1, \dots, A_{d+1}$ such that $x \in X_{A_i}$. Let $X_{A_i} = \{x, x_i\}$ (again all x_i are distinct). Applying problem 5.13 we get $g(x) \leq b(d-1; 2)$, so there are at least $d+3$ sets in $\mathcal{G} \setminus G_x$ and at least two of these sets are distinct from $A_1, \dots, A_{d+1}$. Denote those two sets by B and C . Since $x \notin B$ but $X_{A_i} \cap B \neq \emptyset$ we conclude $\{x_1, \dots, x_{d+1}\} \subseteq B$. Analogously $\{x_1, \dots, x_{d+1}\} \subseteq C$. Thus $|B \cap C| \geq d+1$. A contradiction. $\square$

Remark. In fact, this proof is a repetition of the solution of problem 5.14 (or its version for $h > d$).

5.5. a) Prove that $a(d; 2) \geq C_{d+3}^2$.

b) Prove that $a(d; 2) \leq 2d^2 + 3$ for all $d \geq 2$.

a) Follows from problem 5.8a).

b) We use the induction on $d \geq 2$ to prove that $b(d; 2) \leq 2d^2 + 3$. The base case will follow from the step.

Assume first that $b(d; 2) \geq b(d-1; 2) + d + 3$. Then for all x we have $h(x) \leq d$ by Lemma 5. Let $b = |\mathcal{G}|$.

Now, for every element x denote by $n(x)$ the number of (ordered) triples of distinct sets (A, B, C) from $\mathcal{G}$ such that $x \in A$, $x \in B$, and $x \in X_C$. We will bound the sum σ of all the numbers $n(x)$ in two different ways.

On one hand, there exist $b(b-1)$ pairs of different sets (A, B) . For each such pair, there are not more than d ways to choose an element $x \in A \cap B$, and for every such element there exist $h(x) \leq d$ possibilities for C . Thus, we get $\sigma = \sum_x n(x) \leq b(b-1) \cdot d^2$.

On the other hand, consider an arbitrary set C ; let $X_C = \{x, y\}$. Each of the other $b-1$ sets in $\mathcal{G}$ contains either x or y . Denote by s_x and s_y the number of sets containing x and y , respectively. Then $s_x + s_y \geq b-1$. Furthermore, there exist $s_x(s_x-1)$ pairs of the sets intersecting by x , as well as $s_y(s_y-1)$ pairs intersecting by y . In all, the triples with this fixed C are counted exactly $s(C) = s_x(s_x-1) + s_y(s_y-1)$ times. From $s_x + s_y \geq b-1$ one easily gets $s(C) \geq \frac{(b-1)(b-3)}{2}$ (the estimate is sharp for $s_x = s_y = \frac{b-1}{2}$). Thus, we get $\sigma \geq b \frac{(b-1)(b-3)}{2}$.

Finally we get $d^2b(b-1) \geq \sigma \geq \frac{1}{2}b(b-1)(b-3)$, hence $2d^2 \leq b-3$, QED.

The only remaining case is $b(d; 2) \leq b(d-1; 2) + d + 2$. If $d \geq 3$, then by the induction hypothesis we have $b(d; 2) \leq (2(d-1)^2 + 3) + d + 2 = 2d^2 - 3d + 5 \leq 2d^2 + 3$, as desired. Finally, if $d = 2$, then we use the problem 5.4a) to obtain $b(1; 2) = 6$, therefore $b(2; 2) \leq 6 + 2 + 2 = 10$ which is even stronger than we need.

Remark. Note that the estimates in main part of the solution admit some improvements. Thus, the upper bound for σ is sharp only if $h(x) = d$ for all x . On the other hand, one may see from problem 5.14 that under this restriction $g(x)$ is much greater than $\frac{b-1}{2}$, and the lower bound is far from being sharp. The method of obtaining sharper bounds is shown in the proof of the Lemma 7 before the computation of $b(1; 4)$ and applied after that.

5.7. a) Prove that $a(1; t) \geq C_{t+2}^2$.

b) Prove that $a(1; t) \leq t^2 + 1$ for all $t \geq 3$.

a) Follows from problem 5.8a).

b) The solution is literally the same as that for 3.4a): the only property of the lines which is used there (but not in 3.4b)!) is exactly that they form a family of degree 1.

5.11. Prove that the number $b(d; t)$ is finite for all d and t .

We prove the estimate $b(d; t) \leq t^{d+1} + (t^{d-1} + t^{d-2} + \dots + t^0)$ by the induction on $d \geq 1$. The base case $d = 1$ is proved in 5.76).

For the induction step, let $d \geq 2$. Consider an arbitrary set $A \in \mathcal{G}$; let $X_A = \{x_1, \dots, x_t\}$. Then each of the other sets in $\mathcal{G}$ contains at least one of the elements $x_1, \dots, x_t$. Next, the number

of sets in $\mathcal{G}$ containing x_i is at most $b(d-1; t)$ by Lemma 4. Therefore $|\mathcal{G}| \leq 1 + tb(d-1; t) = 1 + t^{d+2} + (t^d + t^{d-1} + \dots + t)$, as desired.

Remark. Instead of 5.76), one may use a trivial bound $b(0; t) \leq t + 1$ as the base case. This way, one obtains a bit weaker bound, namely $b(d; t) \leq t^{d+1} + t^d + \dots + 1$.

5.9. a) Prove that the number $a(d; t)$ is finite for every pair (d, t) .

b) Try to obtain a good¹ bound for the number $a(d; t)$.

Item a) is an immediate consequence of 5.10 and 5.11. From the solutions of the same problems one can obtain $a(d; t) \leq t^{d+1} + (t^{d-1} + t^{d-2} + \dots + t^0)$ for all $d \geq 1$.

Finally, we proceed to sharp (although particular) results from problems 5.4 and 5.6. Here we do not refer to the numbers of problems but just write down the equalities to be proved.

The lower bounds in all cases follow directly from problem 5.8a). For the upper bounds we assume again that a $(d; t)$ -critical family $\mathcal{G}$ is chosen and we bound the cardinality of the family.

$b(1; 2) = 6$. Assume that $|\mathcal{G}| \geq 7$. Consider an arbitrary $C \in \mathcal{G}$; set $X_C = \{x, y\}$. Then each of the remaining sets in $\mathcal{G}$ contains either x or y ; hence at least three of the sets contain the same element of X_C , say $x \in A_1, A_2, A_3$. Notice that $g(x) \leq 3$ by problem 5.13; so the remaining sets in $\mathcal{G}$ do not contain x . By our assumption, $\mathcal{G}$ contains at least 4 sets C_1, C_2, C_3, C_4 distinct from A_i .

Consider an arbitrary index $k = 1, 2, 3, 4$. Set $X_{C_k} = \{x_1, x_2\}$. There must be two sets among A_i containing the same element x_j . Since their intersection consists of x only (because $\mathcal{G}$ is a family of degree 1!) it follows that $x = x_j \in X_{C_k}$. Thus $x \in C_k$ for each $k = 1, 2, 3, 4$. Then by Lemma 3 applied to $S = \{x\}$ the family $\{C_1, C_2, C_3, C_4\}$ is $(1; 1)$ -exceptional, and by problem 5.3 it has at most 3 elements. A contradiction.

Remark. Analyzing this solution one can capture the following lemma useful for the sequel.

Lemma 6. Let $\mathcal{G}$ be an exceptional $(1, t)$ -family such that $g(x) \geq t + 1$ for some x . Then for each $B \in \mathcal{G}$, we have either $x \in B$ or $x \in X_B$. Moreover, in this case we have that $g(x) = t + 1$ and the family $\mathcal{F} = \mathcal{G} \setminus G_x$ is $(1, t - 1)$ -exceptional.

Proof. Assume that $g(x) \geq t + 1$; we have $G_x \supseteq \{A_1, \dots, A_{t+1}\}$.

Assume that $x \notin B$ and $x \notin X_B$ for some $B \in \mathcal{G}$. Each of the sets $A_1, \dots, A_{t+1}$ contains at least one element of X_B ; since $|X_B| = t$ it follows that two of these sets contain the same element (say, $y \in A_1 \cap A_2 \cap X_B$). But then $A_1 \cap A_2$ contains (distinct!) elements x and y , which is impossible. Thus the required set B does not exist.

Further, $g(x) \leq t + 1$ by problem 5.13, so that $g(x) = t + 1$. The second assertion now follows from Lemma 3. $\square$

$b(1; 3) = 10$. Assume that $|\mathcal{G}| \geq 11$. Consider an arbitrary $C \in \mathcal{G}$; set $X_C = \{x, y, z\}$. Then each of the remaining sets in $\mathcal{G}$ contains at least one of the elements x, y , or z , thus $g(x) + g(y) + g(z) \geq 10$. Hence at least one of the summands is greater than 3, say, $g(x) \geq 4$. Then by Lemma 6 we obtain that $\mathcal{F} = \mathcal{G} \setminus G_x$ is $(1; 2)$ -exceptional, and $|\mathcal{F}| \geq 7$. This contradicts to $b(1; 2) = 6$.

Remark. The previous two statements essentially repeat the solution of problem 3.4a). We present them here to make the appreciation of the next point more convenient.

For the sequel we improve somehow the main approach of problem 5.5. That is, we slightly modify the definition of the sum σ , so that it allows to obtain a bit better estimates. The meaning of the following definition is clear from the lemma afterwards.

Definition 2. For each element x belonging to at least one set of the form X_A , the price of x is $p(x) = \frac{g(x)(g(x) - 1)}{h(x)}$. For each $C \in \mathcal{G}$, define its price by the formula $P(C) = \sum_{x \in X_C} p(x)$.

Lemma 7. Let $\mathcal{G}$ be a $(d; t)$ -critical family of cardinality b . Then there exists a set $C \in \mathcal{G}$ such that $P(C) \leq d(b - 1)$.

¹as good as possible. . .

Proof. Again, for each element x denote by $n(x)$ the number of ordered triples of distinct sets (A, B, C) from the family $\mathcal{G}$ such that $x \in A$, $x \in B$, and $x \in X_C$. But now we are going to estimate a different sum, that is

$$\Sigma = \sum_x \frac{n(x)}{h(x)}$$

(naturally, the sum is over all the elements appearing in the sets of the form X_A).

On one hand, there exist $b(b-1)$ pairs of distinct sets (A, B) . For each such pair there is no more than d possibilities to choose an appropriate element x (because $|A \cap B| \leq d$). Further, any element $x \in A \cap B$ contributes exactly 1 to the sum Σ ; indeed, there exist $h(x)$ possibilities for the set C , and each of these possibilities is counted with the “weight” $1/h(x)$. Thus we get

$$\Sigma = \sum_{(A,B): A \neq B} |A \cap B| \leq d \cdot b(b-1).$$

On the other hand, we consider an arbitrary set C , and we show that its contribution to Σ is equal to $P(C)$. Indeed, for each $x \in X_C$, we count exactly $g(x)(g(x)-1)$ pairs in the number $n(x)$. Taking into account the “weight” $1/h(x)$, we obtain that the “contribution of the pair x, C ” equals $p(x)$. Therefore the contribution of the set C equals $P(C)$, as required.

So $db(b-1) \geq \Sigma = \sum_{C \in \mathcal{G}} P(C)$. By the pigeonhole principle, one of the b summands from the right-hand side is not greater than $d(b-1)$. $\square$

$b(1; 4) = 15$. Assume that $|\mathcal{G}| \geq 16$; removing several sets from $\mathcal{G}$ we may also assume that $b = |\mathcal{G}| = 16$. Consider an arbitrary $C \in \mathcal{G}$; set $X_C = \{x_1, x_2, x_3, x_4\}$. Analogously to the previous case, we get $\sum_i g(x_i) \geq 15$, and $g(x_i) \leq 4$ (otherwise, using Lemma 6, we get a contradiction with $b(1; 3) = 10$).

So $\sum_i g(x_i) = \sum_i |G_{x_i}| \leq 16$, but each set $A \in \mathcal{G}$ distinct from C must be contained in at least one of G_{x_i} . This implies that either all the families G_{x_i} are disjoint or only two of them intersect each other by a single set. In any case we may assume that G_{x_1} , G_{x_2} , and G_{x_3} are disjoint and contain 4 sets each.

Proposition. For each $A \in \mathcal{G}$, which is distinct from C , the set X_A contains neither of the elements x_1, x_2, x_3 .

Proof. Assume that $x_1 \in X_A$; then clearly $x_1 \notin A$. Notice that one of the two elements x_2, x_3 also does not belong to A , because $G_{x_2} \cap G_{x_3} = \emptyset$; we may assume that $x_2 \notin A$. Suppose now that $x_2 \in X_A$. Denote by B_1, B_2, B_3, B_4 the four sets containing x_2 ; none of them contains x_1 . The intersection of any two of them is $\{x_2\}$; hence all the sets $B_i \cap X_A$ are disjoint. Thus X_A consists of these four intersections (because $|X_A| = 4$). But they do not contain x_1 . This contradicts to the assumption that $x_1 \in X_A$.

We have proved that $x_1, x_2 \in X_A$. Now assume that $x_3 \notin X_A$. The family G_{x_3} contains at least three sets distinct from A . They must intersect with X_A by distinct elements, which are also distinct from x_1, x_2 . This is again impossible because $|X_A| = 4$. Thus $X_A = \{x_1, x_2, x_3, y\}$ for some $y \neq x_4$.

Finally, consider two sets $B, B' \in \mathcal{G}$ which do not belong to $G_{x_1} \cup G_{x_2} \cup G_{x_3}$ and are distinct from A and C (such sets exist because $|G_{x_1}| + |G_{x_2}| + |G_{x_3}| + 2 = 14 = |\mathcal{G}| - 2$). Then $\emptyset \neq B \cap X_C$, therefore $x_4 \in B$. Analogously, $y \in B$, and also $x_4, y \in B'$. Thus $|B \cap B'| \geq 2$, which is impossible. $\square$

So we know that $h(x_1) = h(x_2) = h(x_3) = 1$ and $g(x_1) = g(x_2) = g(x_3) = 4$. Hence $P(C) \geq 3 \cdot \frac{12}{1} + p(x_4) > 36$. On the other hand, by Lemma 7 there exists $C \in \mathcal{G}$ such that $P(C) \leq db = 30 < 36$. This contradiction concludes the proof.

$b(2; 2) = 10$. Assume that $|\mathcal{G}| = 11$. It follows from Lemma 5 that $h(x) \leq 2$ for each x , and by problem 5.13 we have $g(x) \leq 6$. Then by problem 5.14, we get that $g(x) = 6$ whenever $h(x) = 2$. Thus if $g(x)$ attains one of the values 4, 5 or 6, then $p(x)$ cannot be less than 12, 20 or $\frac{30}{2} = 15$, respectively.

By Lemma 7 there exist $C \in \mathcal{G}$ such that $P(C) \leq 2 \cdot 10 = 20$. Let $X_C = \{x, y\}$, where $g(x) \geq g(y)$. Notice that $g(x) + g(y) \geq |G_x \cup G_y| = 10$, so that $g(x) \geq 5$, $g(y) \geq 4$. Then $P(C) \geq 15 + 12 = 27$. A contradiction.

$b(3; 2) = 15$. Assume that $|\mathcal{G}| = 16$. Arguing analogously to the previous solution we get $h(x) \leq 3$, $g(x) \leq 10$, and for $h(x) = 1, 2, 3$ we have $g(x) \geq 5, 8, 10$, respectively.

Further, using Lemma 7 we find $C \in \mathcal{G}$ such that $P(C) \leq 3 \cdot 15 = 45$. Set $X_C = \{x, y\}$, where $g(x) \geq g(y)$. Then $g(x) \geq 8$, therefore $p(x) \geq 28$; also $p(y) \geq 20$, because $g(y) \geq 5$. Thus $P(C) \geq 48$. A contradiction.

$b(4; 2) = 21$. Arguing analogously to the previous solutions, we find $C \in \mathcal{G}$ such that $P(C) \leq 84$. If $X_C = \{x, y\}$ and $g(x) \geq g(y)$, then we get an analogous contradiction in every case except $g(y) = 6$; in this remaining case we necessarily have $g(x) = 15$ and $h(x) = 4$ (otherwise $P(C) > 84$ again).

Consider the last case separately. Since $h(x) = 4$, there exist sets C_1, C_2, C_3, C_4 such that $h(C_i) = \{x, y_i\}$. Then there exist $22 - g(x) - h(x) = 3$ sets B_1, B_2, B_3 such that $x \notin B_i$ and $x \notin X_{B_i}$. By the properties of the sets X_{C_j} it follows that $\{y_1, y_2, y_3, y_4\} \subseteq B_i$. Thus any two sets B_i must intersect precisely by the elements y_1, y_2, y_3, y_4 .

Finally, for each $C \in \mathcal{G}$, which is distinct from B_i , the set X_C intersects all B_i ; thus one its element is contained in two sets B_i, B_j . Thus one of the elements y_1, y_2, y_3, y_4 is contained in X_C . This implies that $\sum_i h(y_i) \geq 22 - 3 = 19$; but then $h(y_i) \geq 5$ for some i . As we have noticed above, this is impossible.

Remark. Developing these approaches the authors have proved that $a(d; 2) = b(d; 2) = C_{d+2}^2$ for each $d \leq 7$.

Необычные свойства из необычного условия.

Проект представляют Ф.Ивлев, В.Мокин, А.Заславский, О.Дмитриев и Р.Женодаров

Общая постановка задачи.

Пусть дан треугольник ABC . Обозначим его середины сторон через A_0 , B_0 и C_0 , точки касания вписанной окружности со сторонами через A_1 , B_1 и C_1 соответственно. Обозначим точку пересечения AA_1 , BB_1 и CC_1 через G (в дальнейшем — точка Жергонна). Пусть I — центр вписанной окружности треугольника ABC , O — центр описанной окружности, H — ортоцентр (точка пересечения высот). F — точка Фейербаха треугольника ABC .

Единственное условие, которое мы наложим на треугольник так это то, что точки A , I , G и C лежат на одной окружности.

Квантор $\forall$ в скобках перед условием задачи означает, что данный факт верен для любого треугольника (и без наложенного на него нами условия). Заметим, что отсутствие этого значка не означает обратное!

Часть А.

1. $(\forall)$ Докажите, что угол $\angle AIC = 90^\circ + \frac{\angle B}{2}$.
2. $(\forall)$ Докажите, что $\angle AIC + \angle A_1B_1C_1 = 180^\circ$.
3. $(\forall)$ Докажите, что если через точку A_1 провести прямую параллельную биссектрисе угла C , а через C_1 провести прямую параллельную биссектрисе угла A , то они пересекутся в точке диаметрально противоположной B_1 во вписанной окружности.
4. Докажите, что если точки A , G , I и C лежат на одной окружности, то если построить параллелограмм A_1GC_1F' , его вершина F' будет лежать на вписанной окружности.
5. $(\forall)$ Докажите, что G — точка Лемуана треугольника $A_1B_1C_1$. Точка Лемуана — точка изогонально сопряженная точке пересечения медиан.
6. Докажите, что в случае нашего условия центр тяжести треугольника $A_1B_1C_1$ будет лежать на описанной окружности треугольника A_1IC_1 .
7. Постройте треугольник с наложенным на него нашим условием и заданным углом $\angle B$. Например, по вершине B и вписанной окружности.
8. Покажите, что угол $\angle B$ меньше 60° .

Часть В.

Пусть вторая точка пересечения AA_1 со вписанной окружностью — точка Q , а вторая точка пересечения CC_1 со вписанной окружностью — P . Теперь пусть K — бегающая точка по вписанной окружности. Обозначим точку пересечения KP с BC через P' , а KQ с AB через Q' .

1. Докажите, что если через точки P и Q провести прямые параллельные BC и AB соответственно, то они пересекутся на вписанной окружности. Обозначим эту точку через T .
2. Найдите ГМТ середин M отрезков $P'Q'$.
3. Пусть A_1C_1 пересекает AC в точке R . Через точку R провели прямые параллельные AB и BC до пересечения с BC и AB в точках P_1 и Q_1 соответственно. Докажите, что прямые PP_1 и QQ_1 пересекаются на вписанной окружности.
4. ($\forall$) Докажите, что точки P , Q и R лежат на одной прямой.
5. Пусть точка пересечения B_1C_0 с BC — точка P_2 , а точка пересечения B_1A_0 с AB — точка Q_2 . Докажите, что прямые PP_2 и QQ_2 пересекаются на вписанной окружности.
6. Проведем прямую через середину отрезка AC_1 и точку Q , а также через середину отрезка CA_1 и точку P . Докажите, что они пересекутся на вписанной окружности. С этого момента точка K и есть эта точка пересечения. Она больше не бежит по окружности. Точки P' и Q' теперь тоже фиксированы. Это точки, соответствующие точке K .
7. Докажите, что точки T , K и B лежат на одной прямой.
8. Докажите, что прямые BK и BF' изогонально сопряжены в углу $\angle B$.
9. Докажите, что точки K , G и F' лежат на одной прямой.
10. Пусть E — середина отрезка A_1C_1 . Докажите, что E — центр вписанной окружности треугольника $P'Q'B$.

В дальнейшем точки P , Q , P' , Q' и R нам больше не понадобятся (может быть за исключением последней). Можно расценивать это в виде рекомендации перерисовать рисунок, на котором эти точки уже не отмечать.

Часть С.

Три прямые, проходящие через точку Фейербаха.

Поскольку эта часть очень важна для проекта, но сама по себе является достаточно сложной, то в ней разрешается в доказательствах использовать предыдущие пункты. Так же будет разрешено в дальнейших решениях использовать эту часть без доказательства.

В этой части приведены пункты верные для произвольного неравностороннего треугольника, поэтому здесь опущен квантор $\forall$ перед пунктами.

1. Пусть соответственные стороны треугольников $A_0B_0C_0$ и $A_1B_1C_1$ пересекаются в точках A' , B' и C' . Докажите, что на сторонах треугольника $A'B'C'$ лежат вершины треугольника ABC .
2. Докажите, что треугольник $A'B'C'$ автополярен относительно вписанной окружности. Т.е. каждая его сторона является полярной вершины, через которую эта сторона не проходит.
3. Докажите, что прямые AA' , BB' и CC' параллельны.
4. Докажите, что прямая IG проходит через точки пересечения соответственных сторон треугольников $A_1B_1C_1$ и $A'B'C'$.
5. Пусть M — точка пересечения медиан треугольника ABC . Докажите, что прямая IM проходит через точки пересечения соответственных сторон треугольников $A_0B_0C_0$ и $A'B'C'$.
6. Докажите, что прямые AA' , BB' , CC' параллельны прямой, проходящей через точки пересечения сторон треугольника Жергонна с соответствующими сторонами треугольника ABC . То есть полярю G относительно вписанной окружности.
7. Обозначим точку пересечения прямых CI и C_1A_1 через C_A , а CI с C_1B_1 через C_B . Аналогично определяются точки A_B , A_C , B_A , B_C . Докажите, что точки A , C_1 , C_A , I лежат на одной окружности.
8. Докажите, что C_A лежит на B_0C_0 .
9. Докажите, что центр описанной окружности треугольника $C_AC_BC_1$ — точка C_0 .
10. Докажите, что точки C_A , C_B , A_B , A_C лежат на окружности ортогональной вписанной окружности. То есть, что эта окружность переходит сама в себя при инверсии относительно вписанной окружности. Обозначим ее через ω_B и две аналогичных ей через ω_A и ω_C соответственно.
11. Пусть окружности ω и γ ортогональны, а P и Q их центры соответственно. Докажите, что полярю P относительно γ , полярю Q относительно ω и радикальная ось ω и γ совпадают.
12. Дан вписанный четырехугольник $ABCD$. Пусть N — точка пересечения прямых AB и CD , M — BC и AD , а P — AC и BD . Докажите, что NM — полярю точки P относительно описанной окружности четырехугольника.
13. Обозначим центр окружности ω_B через O_B . Аналогично определим точки O_A и O_C . Докажите, что O_B лежит на $A'C'$.
14. Докажите, что середины сторон исходного треугольника лежат на сторонах треугольника $O_AO_BO_C$.
15. Докажите, что треугольник $A_0B_0C_0$ является ортотреугольником треугольника $O_AO_BO_C$. Ортотреугольник — треугольник вершины которого являются основаниями высот другого.
16. Обозначим через M_B середину стороны O_AO_C . Аналогично определим M_A и M_C . Докажите, что треугольники $A_1B_1C_1$ и $M_AM_BM_C$ гомотетичны.

17. Докажите, что точки B' , M_B и B_1 лежат на одной прямой.
18. Докажите, что прямые A_1A' , B_1B' , C_1C' пересекаются в точке Фейербаха треугольника ABC .
19. Докажите теорему Фейербаха. То есть докажите, что вписанная окружность и окружность Эйлера в разностороннем треугольнике касаются.
20. Докажите, что касательная в точке F к вписанной окружности проходит через точки пересечения соответственных сторон треугольников ABC и $A'B'C'$.
21. Докажите, что точки B_C , C_B , A_1 , A_0 лежат на одной окружности.
22. Докажите, что F лежит на той же окружности.
23. Придумайте другое доказательство того, что прямая A_1A' проходит через F .

Часть D.

1. Через A'' , B'' и C'' обозначим точки пересечения прямых A_1F' , B_1F' и C_1F' со сторонами треугольника $A_1B_1C_1$. Докажите, что треугольник $A''B''C''$ автополярен относительно вписанной окружности и на его сторонах лежат вершины треугольника ABC .
2. Докажите, что если симметрично отразить точки A и C относительно A_1 и C_1 соответственно, то они попадут на прямую $A''C''$.
3. Докажите, что BC_1A_0C'' и BA_1C_0A'' — параллелограммы.
4. Докажите, что $F' = F$. То есть, что F' — точка Фейербаха треугольника ABC .
5. Пусть a , b и c — длины сторон CB , AC и AB соответственно. Докажите, что $(a + c - b)^2 = ac$.
6. Докажите, что следствие предыдущего пункта является достаточным условием для того, чтобы треугольник обладал наложенными нами на него свойствами.
7. Докажите, что F — точка пересечения медиан треугольника $A'B_0C'$.
8. Пусть S — середина $A'C'$. Докажите, что через нее проходит прямая FB_0 .
9. Докажите, что S является серединой отрезка BO_B .
10. Докажите, что SE параллельна BB_1 .
11. Докажите, что OF параллельна BB_1 .
12. Докажите, что F является точкой пересечения медиан треугольника $O_BA_0C_0$.
13. $(\forall)$ Пусть L_B — полюс средней линии A_0C_0 относительно вписанной окружности. Докажите, что L_B является точкой пересечения $A'C'$ с GE .
14. $(\forall)$ Докажите, что ортоцентр треугольника ACL_B — точка I .
15. $(\forall)$ Пусть G' — изогональный образ точки Жергона. Докажите, что G' — центр гомотетии вписанной и описанной окружностей.
16. Докажите, что G' симметрична G относительно биссектрисы угла $\angle B$.
17. $(\forall)$ Докажите, что точки F , G' и M лежат на одной прямой.
18. Докажите, что FM параллельна биссектрисе угла $\angle B$.
19. Докажите, что прямые GM и $A'C'$ параллельны.
20. Докажите, что O_B является серединой BL_B .
21. Докажите, что F — центр масс треугольника $A_1L_BC_1$.
22. Докажите, что точка L_B изогонально сопряжена точке пересечения A_1C_1 и OI .

Часть X.

Эта часть рассказывает о гиперболе Фейербаха и предлагает порешать несколько пунктов, которые связаны с ней.

1. $(\forall)$ Докажите, что образ прямой, не проходящей через вершины треугольника при изогональном сопряжении — коника.
2. $(\forall)$ Покажите, что изогональный образ прямой OI касается этой прямой.
3. $(\forall)$ Покажите, что изогональный образ прямой OI — равносторонняя гипербола. Получившаяся коника называется гиперболой Фейербаха.
4. $(\forall)$ Докажите, что на гиперболе Фейербаха лежат точки A, B, C, I, H, G и N , где N — точка Нагеля треугольника ABC .
5. $(\forall)$ Пусть l — произвольная прямая, проходящая через O . Обозначим через l' конику, полученную из прямой l изогональным сопряжением. Докажите, что центр l' лежит на окружности Эйлера.
6. $(\forall)$ Пусть через вершины треугольника ABC проходит равносторонняя гипербола, а P — произвольная точка на ней. Докажите, что описанная окружность подерного треугольника точки P относительно треугольника ABC проходит через центр гиперболы.
7. $(\forall)$ Докажите, что центр гиперболы Фейербаха — точка Фейербаха.
8. $(\forall)$ Докажите, что L_B лежит на гиперболе Фейербаха.
9. $(\forall)$ Докажите, что прямая FB_1 пересекается с описанной окружностью треугольника A_1C_1I и гиперболой Фейербаха в двух общих точках.
10. Покажите, что ГМТ центров изогональных образов прямых, проходящих через I — эллипс, проходящий через основания биссектрис, середины сторон и точку Фейербаха.
11. Докажите, что прямые B_0L и GM пересекаются на гиперболе Фейербаха.
12. $(\forall)$ Докажите, что точка пересечения прямых FB_0 и A_1C_1 — полюс прямой AC относительно гиперболы Фейербаха.
13. $(\forall)$ Докажите, что полюс прямой $A'C'$ — точка симметричная B_1 относительно E .

Часть F.

1. Пусть Q'' — точка симметричная Q относительно Q' . Аналогично определим P'' . Докажите, что $P''Q'' = AC$.
2. Докажите, что в треугольнике $P''FQ''$
 - FB — медиана.
 - FI — высота.
 - FG' — прямая, соединяющая F с центром описанной окружности этого треугольника.
 - FG — симедиана.
3. Докажите, что прямая KB_1 проходит через точки пересечения $A'E$ с BC и $C'E$ с AB .
4. Докажите, что прямая KB_1 проходит через точку пересечения $A'C'$ и A_0C_0 .
5. Докажите, что GG' и BB' пересекаются на гиперболе Фейербаха.
6. Докажите, что прямые FG' и BB' пересекаются на описанной окружности треугольника ABC . Обозначим эту точку через D .
7. Докажите, что прямая $L_B B_0$ проходит через D .
8. Обозначим точку Фейербаха треугольника $BP'Q'$ через F'' . Докажите, что $F''F \parallel BB_1$.
9. Докажите, что прямые FO_B , EB_0 и BB' пересекаются в одной точке.
10. Докажите, что гипербола Фейербаха треугольника $P''Q''B$ проходит через точку B' .
11. Докажите, что гипербола Фейербаха треугольника $P''Q''B$ проходит через точку L_B .
12. Пусть C'_1 — точка касания вписанной окружности треугольника $BP''Q''$ со стороной QB . Аналогично определяются точки A'_1 и B'_1 . Докажите, что прямая $A'_1C'_1$ в четыре раза ближе к F чем A_1C_1 .
13. ($\forall$) Докажите, что прямые A_0A' , B_0B' , C_0C' пересекаются в одной точке, лежащей на общей касательной окружностей Эйлера и вписанной окружности. Обозначим эту точку через M' .
14. Докажите, что M' лежит на биссектрисе угла $\angle B$.
15. ($\forall$) Через точку F провели прямые параллельные AA_1 , BB_1 , CC_1 до пересечения с AA' , BB' , CC' соответственно. Докажите, что три полученные точки пересечения будут лежать на прямой GM .
16. ($\forall$) Через M' провели прямые параллельные медианам треугольника ABC до пересечения с соответственными прямыми AA' , BB' и CC' . Докажите, что полученные точки пересечения лежат на прямой IM .
17. Докажите, что прямые KB_1 , GM , A_1C_1 пересекаются в одной точке.
18. Докажите, что соответственные асимптоты гипербол Фейербаха треугольников ABC и $BP'Q'$ параллельны.

Часть А.
Решения.

1. Легко следует из счета в углах.
2. Легко следует из предыдущего пункта и счета в углах.
3. Легко следует из того, что угол между биссектрисой угла $\angle A$ и прямой B_1C_1 равен 90° и аналогичного факта про угол $\angle B$.
4. Очевидное следствие двух предыдущих пунктов и свойств вписанного угла.
5. Обозначим середину отрезка A_1C_1 через E . Пересечем B_1E вторично со вписанной окружностью в точке X . Теперь считая степень точки E относительно описанной окружности BA_1IC_1 получаем $BE \cdot EI = EA_1 \cdot EC_1$. Теперь относительно вписанной окружности продолжаем $EA_1 \cdot EC_1 = EB_1 \cdot EX$. Значит по обратному свойству вписанности получаем, что $BXIB_1$ вписанный. Так как $IB_1 = IX$ равны как радиусы, то равны и углы, опирающиеся на эти хорды, то есть $\angle B_1BI = \angle IBX$. Обозначим через Y вторую точку пересечения BB_1 со вписанной окружности. Из доказанного следует, что $XY \parallel A_1C_1$. А значит прямые B_1X и B_1Y изогонально сопряжены в углу $A_1B_1C_1$. Заметим, что, если спроецировать двойное отношение точек A_1, C_1, E и бесконечно удаленной точки прямой A_1C_1 равное -1 из точки X на окружность мы получим, что двойное отношение (A_1, C_1, B_1, Y) равно -1 . То есть четырехугольник со свойством, что касательные в двух его вершинах пересекаются на его диагонали, проведенной через две другие вершины, является гармоническим.
6. Используя предыдущий пункт можно легко доказать данный факт счетом углов.
7. Проведя касательные из точки B мы получаем точки A_1 и C_1 . Строим точку E . Так как описанная окружность A_1C_1I делит медиану EB_1 в отношении $2 : 1$, то сделав гомотетию с центром в E и коэффициентом 3 образ описанной окружности треугольника A_1IC_1 пересечет вписанную окружность по точке B_1 . Дальнейшие построения очевидны. Вторая точка пересечения, очевидно, даст второе решение, симметричное первому относительно биссектрисы угла B .
8. Из решения предыдущего пункта видно, что IE должно быть хотя бы в два раза меньше, чем радиус вписанной окружности. Из этого легко вывести, что угол $\angle A_1IC_1$ хотя бы 120° . Значит угол $\angle B$, дающий с ним в сумме 180° , не больше 60° .

Часть В.

Решения.

Пусть вторая точка пересечения AA_1 со вписанной окружностью — точка Q , а вторая точка пересечения CC_1 со вписанной окружностью — P . Теперь пусть K — бегающая точка по вписанной окружности. Обозначим точку пересечения KP с BC через P' , а KQ с AB через Q' .

Эту часть можно не решать. Факты из нее не используются в дальнейшем.

1. Так как угол PGQ равен $90^\circ + \frac{\angle B}{2}$, то сумма дуг PQ и A_1B_1 равна $180^\circ + \angle B$. Так как дуга A_1C_1 равна $180^\circ - \angle B$, то на дугу PQ остается $2\angle B$. Значит, если пересечь прямую, проходящую через Q параллельно BA до второго пересечения со вписанной окружностью в точке T получим, что $\angle QTP = \angle B$. А значит и $TP \parallel BC$.
2. Будем двигать точку P' по BC с постоянной скоростью. Тогда получается, что Q' будет двигаться так, что будут сохраняться двойные отношения положений точек P' и Q' . То есть отображение из точек P' в точки Q' проективное. Теперь заметим, что по предыдущему пункту P' и Q' одновременно уходят на бесконечность. А значит, наше проективное преобразование сохраняет бесконечно удаленную точку на бесконечности, то преобразование аффинное. То есть если одну точку двигать линейно, то и другая движется линейно (так как они движутся с сохранением двойного отношения). Значит, ГМТ будет прямая. Понятно, что это будет прямая Гаусса для четырехугольника AC_1A_1C . Это очевидно, если рассмотреть частные случаи $K = A_1$ и $K = C_1$.
3. Так как ГМТ из предыдущей задачи — прямая Гаусса четырехугольника A_1C_1AC , то в какой-то точке должна достигаться середина третьей “диагонали”. Пусть R' — середина RB . Тогда заметим, что точки P' и Q' должна быть на сторонах AB и BC и их серединой должна быть точка R' . Но тогда точки $PBQR$ будут образовывать параллелограмм. Собственно его мы и построили.
4. Заметим, что проецировать двойное отношение четверки точек на окружности на эту же окружность можно с точки не на этой окружности. Действительно: пусть эта точка вовне окружности. Тогда можно сделать проективное преобразование, переводящее окружность в окружность, а эту точку в бесконечно удаленную точку. Тогда проецирование из этой точки очевидно будет сохранять двойные отношения, потому что будет простой симметрией окружности относительно диаметра. Если же точка была внутри, то можно проективным преобразованием перевести окружность в окружность, а эту точку в центр. Тогда проецирование через эту точку будет симметрией относительно центра, то есть тоже будет очевидно сохранять двойные отношения. Заметим, что так как касательные в точках B_1 и A_1 пересекаются на диагонали C_1P четырехугольника $B_1C_1A_1P$, то он гармонический. Спроецируем его из точки R на эту же вписанную окружность. Получим, что A_1 и C_1 поменяются местами, точка B_1 перейдет в себя, а значит P должна перейти в точку дополняющую тройку B_1, A_1, C_1 до гармонической четверки. То есть в точку Q . А значит, точки P, Q и R лежали на одной прямой.
5. Спроектируем точки R, B_1, A, C , образующие гармоническую четверку (так как треугольник Жергонна чевианный) из бесконечно удаленной точки прямой AB на BC . Пусть R перешла в P_1 , A в B , C в C , а B_1 в B'_1 . Теперь проецируем эту четверку из точки B_1 на прямую AB . Получаем, что B'_1 перейдет в бесконечно удаленную точку этой прямой, B перейдет в себя, C в A , а значит, так как изначальная четверка была гармонической P_1 перейдет в середину. То есть $P_1 = P_2$. Воспользуемся ранее доказанным утверждением.
6. Заметим, что в положении $P' = A$ точка Q' в A_1 , а в положении $P' = C_1$ точка Q' в C . Значит когда одна точка находится в середине отрезка, то и вторая тоже.

7. Проекция из точки P точек P' , A_1 , C и бесконечно удаленной точки прямой BC на вписанную окружность переводит их в точки K , A_1 , C_1 и T . Так как двойное отношение было равно -1 , то в полученном четырехугольнике диагональ TK проходит через точку пересечения касательных проведенных в двух других вершинах A_1 и C_1 .
8. Дуга TC_1 равна дуге C_1Q , так как касательная в точке C_1 параллельна QT . Дуга C_1Q равна дуге A_1F' , так как $C_1F' \parallel QA_1$. Значит дуги C_1T и $F'A_1$ равны, откуда легко следует симметрия относительно биссектрисы угла $\angle B$.
9. Смотрите решение пятого пункта из части А. Обратный ход в его решении и предыдущие два пункта приводят к решению этого.
10. Сделаем гомотетию с центром в K , переводящую P в P' . При этом T перейдет в B , а значит Q в Q' . Так как $Q'E$ параллельно QG как средняя линия, G перейдет в M . Так как PG проходит через середину дуги QT , PQ является биссектрисой в треугольнике PQT . Значит и QA_1 тоже биссектриса. То есть G — центр вписанной окружности треугольника QTP . А значит его образ, точка M , будет центром вписанной окружности образа треугольника, то есть треугольника $Q'BP'$.

Часть С.

Решения.

1. Пересечем прямую BC' с AC в точке R . Для доказательства того, что точка B лежит на прямой $A'C'$, достаточно показать, что двойные отношения точки A, C_0, B, C_1 и A, B_0, R, B_1 равны. По теореме Чебы $\frac{AC_0}{C_0B} = \frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B}$, $\frac{AC_1}{C_1B} = \frac{AB_1}{B_1C} \cdot \frac{CA_1}{A_1B}$. Воспользовавшись этими соотношениями, а также тем, что двойные отношения точек C, A_0, B, A_1 и C, B_0, R, B_1 равны (проектирование из точки C'), получим

$$\frac{AC_0}{C_0B} \cdot \frac{C_1B}{AC_1} = \frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B} \cdot \frac{BA_1}{A_1C} \cdot \frac{CB_1}{B_1A} = \frac{AB_0}{B_0C} \cdot \frac{CB_0}{B_0R} \cdot \frac{B_1R}{B_1C} \cdot \frac{CB_1}{B_1A} = \frac{AB_0}{B_0R} \cdot \frac{B_1R}{AB_1}$$

2. Пусть прямая A_1C_1 пересекает прямую AC в точке R . Спроектируем двойное отношение $(A, C, B_1, R) = -1$ на прямую B_1C_1 из точки B' . C перейдет в точку A' , A в X , R в C_1 , B_1 в себя. Следовательно двойное отношение $(B_1, C_1, A', X) = -1$. То есть поляра точки A' проходит через точку X и полюс прямой B_1C_1 , на которой она лежит, то есть точку A . Значит это прямая AX . Она же $B'C'$ по предыдущему пункту.

3. Докажем лемму: пусть треугольник $A_1B_1C_1$ чевианный для треугольника ABC . На его сторонах выбрали точки A', B' и C' соответственно, так, что вершины треугольника ABC лежат на сторонах треугольника $A'B'C'$. Пусть A_0 — точка пересечения B_1C_1 с BC . Аналогично определим точки B_0 и C_0 . Тогда прямые AA', BB', CC' и $A_0B_0C_0$ пересекаются в одной точке.

Доказательство: рассмотрим треугольники $CA'A_0$ и $C'AC_0$. Применим для них теорему Дезарга. Получим, так как $CA' \cap C'A = B'$, $A'A_0 \cap AC_0 = C_1$, $A_0C \cap C'C_0 = A_1$, а эти точки лежат на одной прямой, то эти треугольники перспективны. Значит прямые CC' , AA' , A_0C_0 пересекаются в одной точке. Так как точки A_0, C_0, B_0 лежат на одной прямой (очевидное следствие из теорем Чебы и Менелая), то получаем, что все нужные нам прямые проходят через одну точку.

Осталось заметить, что в нашем случае один из треугольников срединный. А значит соответственные прямые пересекаются на бесконечности, то есть параллельны.

4. Применим теорему Паппа для точек A, B_1, C и C_1, B', A_1 , затем для точек A, B_1, C и C_B, B', A_B . (см. пункт 7)
5. Аналогично предыдущему пункту применяем теорему Паппа для точек A, B_0, C и C_0, B', A_0 , а затем для точек A, B_0, C и C_A, B', A_C . (см. пункт 7)
6. По лемме из пункта 3 для треугольника Жергонна.
7. $\angle B = 180^\circ - \angle A - \angle C \Rightarrow \angle BA_1C_1 = \frac{180^\circ - \angle B}{2} = \frac{\angle A + \angle C}{2} \Rightarrow \angle(A_1B, A_1C_1) = \angle(A_1C, CI) + \angle(AI, AC_1) \Rightarrow \angle(AI, AC_1) = \angle(A_1B, A_1C_1) - \angle(A_1C, CI) = \angle(A_1C, A_1C_A) - \angle(CA_1, CC_A) = \angle(IC_A, CA_1) + \angle(A_1C, C_1C_A) = \angle(IC_A, C_A C_1)$. Следовательно, точки A, C_1, C_A, I лежат на одной окружности.
8. Из предыдущего пункта следует, что C_A — проекция точки A на биссектрису, проведенную из вершины B . А значит угол AB_0C_A центральный в треугольнике ACC_A и, значит, вдвое больше угла C в нем. То есть он равен углу C треугольника ABC . Значит $B_0C_A \perp BC$, что и означает, что C_A лежит на средней линии.
9. Так как C_0C_A параллельно BA_1 , то треугольник $C_1C_0C_A$ равнобедренный. Значит $C_0C_1 = C_0C_A$. Аналогично $C_0C_1 = C_0C_B$.

10. Заметим, что окружность из предыдущего пункта ортогональна вписанной окружности, т.к. проходит через C_1 , а ее центр лежит на касательной к вписанной окружности в этой точке. Значит, так как C_A и C_B лежат на одной прямой с центром вписанной окружности, получаем, что они инверсны друг другу относительно вписанной окружности. Аналогичное верно и для пары точек A_B и A_C . Значит $IC_A \cdot IC_B = r^2 = IA_B \cdot IA_C$, где r — радиус вписанной окружности. Отсюда легко понять, что нужные точки лежат на одной окружности, которая при инверсии перейдет сама в себя, а значит она ортогональна вписанной.
11. Очевидно из свойств поляра и радикальной оси, что все эти прямые будут общей хордой этих окружностей.
12. Применим теорему Паскаля к точкам A, B, B, D, C, C . Получим, что точка пересечения касательных в точках B и C лежит на прямой NP . Аналогично получаем, что точка пересечения касательных в точках A и D лежит на этой прямой. Теперь посмотрим на поляру точки M . Это прямая, проходящая через полюсы прямых BC и AD . Но полюсы прямых BC и AD — точки пересечения пар касательных в точках B и C , а так же в точках A и D . Но по доказанному это прямая PN . Значит поляра M — PN . Аналогично для остальных.
13. То, что O_B лежит на $A'C'$ равносильно тому, что поляра O_B относительно вписанной окружности проходит через полюс прямой $A'C'$ относительно вписанной окружности, то есть через точку B' . Так как ω_B ортогональна вписанной окружности, то поляра O_B относительно вписанной окружности то же самое, что поляра I относительно ω_B . Но заметим, что для вписанного в ω_B четырехугольника $C_B C_A A_B A_C$ I является точкой пересечения противоположных сторон, а B' — точкой пересечения диагоналей. Значит поляра I проходит через B' , что и требовалось.
14. Так как окружности ω_B, ω_A и описанная окружность треугольника $C_A C_B C_1$ проходят через точки C_A и C_B , то их центры лежат на одной прямой.
15. Из решения предыдущего пункта видно, что $O_B O_A$ перпендикулярна $C_A C_B$, то есть биссектрисе угла C треугольника. А значит, и биссектрисе угла C_0 треугольника $A_0 B_0 C_0$. Получаем, что стороны треугольника $O_A O_B O_C$ — это внешние биссектрисы углов треугольника $A_0 B_0 C_0$. Значит, его вершины это центры внеписанных окружностей, откуда очевидно следует требуемое.
16. Стороны этих треугольников перпендикулярны соответствующим биссектрисам исходного треугольника.
17. Спроектируем двойное отношение (A, C, B_1, R) равное -1 из точки B' на прямую $O_A O_C$. A перейдет в O_A , C в O_C , R в бесконечно удаленную точку прямой $O_A O_C$, а значит, B_1 перейдет в M_B , что и требовалось.
18. Заметим, что $M_A, M_B, M_C, A_0, B_0, C_0$ лежат на одной окружности: это окружность Эйлера для треугольника $O_A O_B O_C$. Но тогда центр гомотетии треугольников $A_1 B_1 C_1$ и $M_A M_B M_C$ будет так же центром гомотетии их описанных окружностей, то есть окружности Эйлера изначального треугольника (так как $\omega_{M_A M_B M_C} = \omega_{A_0 B_0 C_0}$ = окружность Эйлера исходного треугольника) и вписанной окружности исходного треугольника. То есть центром гомотетии будет как раз точка Фейербаха. Но из предыдущего пункта мы знаем, что на прямой $M_A A_1$ лежит и точка A' . Значит, прямая $A_1 A'$ проходит через точку Фейербаха, ч.т.д.
19. Заметим, что так как $A_0 B_0 C_0$ — срединный треугольник для треугольника ABC и при этом ортотреугольник для треугольника $O_A O_B O_C$ то у этих треугольников совпадают окружности Эйлера. Значит, точки M_A, M_B, M_C лежат на окружности Эйлера исходного треугольника. Но мы знаем, что треугольники $A_1 B_1 C_1$ и $M_A M_B M_C$ гомотетичны, а значит гомотетичны и их

описанные окружности. Осталось показать, что центр гомотетии лежит на одной из окружностей. Покажем, что он лежит на вписанной окружности исходного треугольника. Пересечем AA' с вписанной окружностью в точке R . Тогда, так как B' лежит на поляре A' относительно вписанной окружности и на диагонали A_1C_1 четырехугольника $A_1B_1C_1R$, то B' — точка пересечения диагоналей этого четырехугольника. Аналогично получаем нужное про CC' . Раз центр гомотетии лежит на вписанной окружности, то эти окружности гомотетичны.

20. Двойственный факт пункту 18.

21. Смотрите решение следующего пункта

22. Лемма 1. $\angle(A_0F, FA_1) = (\angle(CA, CB) + \angle(BA, BC))/2$.

Доказательство: Покажем, что $\angle(A_0F, FH) = \angle(CA, CB) + \angle(BA, BC)$, где H — основание высоты, опущенной из A на BC . Тогда нужный нам факт будет очевидно следовать из леммы Архимеда. Заметим, что $\angle(A_0F, FH) = \angle(A_0B_0, B_0H)$, так как все эти точки лежат на окружности Эйлера. Так же заметим, что ввиду того, что B_0 — середина гипотенузы прямоугольного треугольника AHC , $\angle(CA, CB) = \angle(CB_0, CH) = \angle(HC, HB_0)$. Значит $\angle(A_0B_0, B_0H) = \angle(A_0B_0, A_0H) + \angle(A_0H, HB_0) = \angle(BA, BC) + \angle(CA, CB)$, ч.т.д.

Лемма 2. Точки B_C, C_B, A_1, A_0 и F лежат на одной окружности.

Доказательство: Покажем, что $\angle(A_0C_B, C_BA_1) = \angle(A_0F, FA_1)$. Из вписанности C_BIA_1B получаем, что $\angle(C_BI, C_BA_1) = \angle(BI, BA_1) = \angle(BA, BC)/2$. Из того, что $C_BA_0 = A_0C$, получаем равенство $\angle(A_0C_B, C_BC) = \angle(CC_B, C_A0) = \angle(CA, CB)/2$. Откуда получаем, что $\angle(A_0C_B, C_BA_1) = \angle(A_0C_B, C_BC) + \angle(C_BC, C_BA_1) = \frac{\angle(CA, CB) + \angle(BA, BC)}{2} = \angle(A_0F, FA_1)$. То есть C_B лежит на описанной окружности $\triangle A_1A_0F$. Аналогично получаем, что и B_C лежит на ней же. Утверждение доказано.

23. Мы получили, что A_1F — радикальная ось вписанной окружности и окружности описанной около треугольника $C_BB_CA_1$ окружностей. Так что нам осталось показать, что A' лежит на ней. Для этого достаточно заметить, что A' — центр гомотетии, переводящей треугольник $C_0C_1C_B$ в треугольник $B_0B_CB_1$, так как у этих треугольников соответственные стороны параллельны. А значит $\frac{A'C_1}{A'B_C} = \frac{A'C_B}{A'B_1}$, откуда следует равенство степеней относительно нужных окружностей $A'C_1 \cdot A'B_1 = A'C_B \cdot A'B_C$.

Часть D.

1. Автополярность треугольника $A''B''C''$ следует из того, что его вершины — точки пересечения сторон четырехвершинника $A_1B_1C_1F'$. Так как поляр C относительно вписанной окружности, прямая A_1B_1 проходит через точку C'' , то поляр C'' , прямая $A''B''$, проходит через C . Аналогично для остальных вершин.
2. Пусть X — точка пересечения AA_1 и $A''C''$. Двойное отношение точек A, B, C_1 и пересечения AB с A_1B_1 равно -1 . Из центрального проецирования из точки C'' этих четырех точек с прямой AB на прямую AA_1 следует, что A_1 — середина AX .
3. При гомотетии с центром в точке A и коэффициентом 2, прямая C_0A_1 переходит в прямую $A''C''$. Значит, они параллельны. При гомотетии с центром в B , переводящей CC_1 в A_1F' , получаем, что середина $A'A_1$ лежит на AB . Значит, BA_1C_0A'' — параллелограмм.
4. Так как BA_1C_0A'' — параллелограмм, то C_0A'' параллельно стороне BC и проходит через середину BA . Значит A'' лежит на средней линии треугольника ABC параллельной стороне AB . Тогда $C'' = C'$, так как лежит и на стороне треугольника Жергонна, соответствующей стороне AB . Аналогично $A'' = A'$. Значит $F' = F$.
5. Из третьего пункта следует, что C_0A_1 параллельна C_1A_0 , то есть $\frac{BC_0}{BA_1} = \frac{BC_1}{BA_0} \Rightarrow BC_1 \cdot BA_1 = BC_0 \cdot BA_0$. Выразив эти длины через a, b и c и домножив все на 4, получаем требуемое.
6. Из этого условия следует, что C_0A_1 параллельна C_1A_0 . Построим параллелограммы BC_1A_0C'' и BA_1C_0A'' . Тогда $A''C''$ проходит через B , так как BA'' параллельно BC'' . Причем если сделать гомотетию с центром в точке A и коэффициентом 2, то прямая C_0A_1 перейдет в прямую $A''C''$. Пусть при этой гомотетии A_1 перейдет в точку X . Тогда X лежит на прямой $A''C''$. Так как BC_1A_0C'' — параллелограмм середина C_1C'' лежит на BC . А если середина C_1C'' и AX лежат на одной прямой, то несложно понять, что прямые AA_1 и C_1C'' параллельны. Из центрального проецирования из точки C'' точек A, X, A_1 и бесконечно удаленной точки прямой AA_1 на прямую AB следует, что двойное отношение точек A, B, C_1 и пересечения AB с A_1C'' равно -1 . Значит A_1C'' проходит через точку пересечения B_1A_1 и BA , а следовательно, и через точку B_1 . Тогда, вспомнив, что C'' лежит на средней линии треугольника ABC параллельной AB , получаем, что $C'' = C'$. При этом GC_1FA_1 будет параллелограммом. Далее обратный для задач из части A счет углов дает наше условие.
7. В 3-ем пункте мы доказывали, что $C'F$ проходит через середину BA_0 . Из гомотетии с центром в C' получаем, что $C'F$ проходит через середину $A'B_0$. То есть $C'F$ — медиана треугольника $A'B_0C'$. Аналогично для $A'F$.
8. Из предыдущего пункта следует, что B_0F — медиана треугольника $A'B_0C'$.
9. Из того, что O_B является центром вневписанной окружности треугольника $A_0B_0C_0$ следует, что $O_BC_0A_1C''$ — параллелограмм, а из 2-ого пункта, BA_1C_0A' — параллелограмм. Значит $A'B = C_0A_1 = O_BC'$. то есть точки B и O_B симметричны относительно середины отрезка $A'C'$, точки S .
10. SE является прямой Гаусса четырехугольника $A_1B_1C_1F$. Тогда она проходит через середину отрезка FB_1 . Значит она является средней линией треугольника FGB_1 , а значит, параллельна BB_1 .
11. Из предыдущего пункта, SE параллельна BB_1 . Так как $BSEG$ — трапеция, а S и E середины BO_B и FG , FO_B так же параллельна этим двум прямым.

12. Заметим, что, так как S — середина BO_B , и F делит B_0S в отношении $2 : 1$, то F — центр масс треугольника B_0O_BB . Но тогда медиана из вершины O_B этого треугольника делится точкой F в отношении $2 : 1$ и заканчивается в середине BB_0 , а значит и в середине C_0A_0 . Отсюда получаем требуемое.
13. Сделаем полярное преобразование. Так как B' лежит на C_0A_0 получаем что L_B лежит на $A'C'$. Теперь нам надо доказать, что поляры точек G и E пересекаются на средней линии треугольника. Вспомним, что поляр G это прямая, параллельная BB' и проходящая через R , точку пересечения A_1C_1 с AC . Поляр M — прямая, проходящая через B параллельно A_1C_1 . Получаем, что B , B' , R и точка пересечения нужных нам поляр образуют параллелограмм. А следовательно, так как середина BR лежит на A_0C_0 и B' лежит на ней, то A_0C_0 проходит и через четвертую вершину этого параллелограмма, то есть через точку пересечения поляр G и M .
14. Заметим, что так как точка C_B лежит на A_0C_0 , то L_B лежит на ее поляре, а именно на прямой AC_A (так как она проходит через инверсный образ C_B и перпендикулярна IC_B). А значит, AL_B перпендикулярно CI . Аналогично получаем, что $AI \perp CL_B$, откуда очевидно получаем требуемое.
15. Несложно показать из счета в углах, что треугольник образованный точками симметричными вершинам треугольника Жергонна относительно соответственных биссектрис изначального треугольника гомотетичен исходному. Значит пересечение прямых, соединяющих соответственные вершины этих треугольников будет центром гомотетии вписанной и описанной окружностей. А это и есть точка G' из построения.
16. Так как точки A , C , G , I лежат на одной окружности, то если за G' положить точку, симметричную G относительно биссектрисы угла B получим, что она тоже лежит на этой окружности (потому что ее центр, по лемме о трезубце — середина дуги AC описанной окружности, а значит лежит на биссектрисе B). Так же очевидно будет, что $\angle GAI = \angle G'AI$, то есть G' изогонально сопряжена G .
17. Очевидное следствие из теоремы о 3-х колпаках для вписанной окружности, описанной окружности и окружности Эйлера.
18. Так как G и G' симметричны относительно BE , BE проходит через середину GG' . Но тогда BE средняя линия в треугольнике FGG' , а значит, параллельна FG' , а следовательно, и FM .
19. В следующем пункте будет доказано, что O_B — середина BL_B . Вспомнив, что $O_BF \parallel BG$ получаем, что O_BF — средняя линия треугольника L_BBG . Значит F — середина L_BG . Тогда E делит отрезок L_BG в отношении $3 : 1$. В этом же отношении делит отрезок BM середина отрезка A_0C_0 . Но так как прямая, соединяющая середину A_0C_0 с E — средняя линия трапеции $C_1C_0A_1A_0$, то она параллельна ее основаниям, а значит, и прямой $A'C'$. Из этого и доказанных отношений получаем, что GM тоже параллельна $A'C'$.
20. AL_B параллельна C_0O_B , так как обе перпендикулярны CI . Тогда из гомотетии с центром в B и коэффициентом 2, O_B переходит в L_B , что и означает, что она середина нужного отрезка.
21. L_BF является медианой треугольника $A_1L_BC_1$, причем из предыдущего пункта, F — середина L_BG . То есть F делит L_BE в отношении $2 : 1$. Значит, F — центр масс треугольника $A_1L_BC_1$.
22. Пусть изогональный образ точки L_B — это X . Так как L_B лежит на гиперболе Фейербаха (смотри часть X), то X лежит на прямой OI . Покажем, что X лежит на прямой A_1C_1 . Пусть X' — образ X при отражении относительно биссектрисы угла B . Так как OI проходит чрез G' , то прямая OI переходит в прямую IG . Прямая A_1C_1 переходит в себя. Прямая BX переходит

в прямую BL_B , то есть в прямую $A'C'$. Прямые $A'C'$ и A_1C_1 пересекаются на прямой IG как соответствующие стороны треугольников $A'B'C'$ и $A_1B_1C_1$. Значит X' лежит на A_1C_1 , а значит, и X на ней лежит.

Часть X.

Решения.

1. Возьмем две вершины и три произвольных образа каких-то точек с этой прямой. Тогда они задают какую-то конику. Заметим, что теперь если взять еще какую-то четвертую точку на этой прямой и посмотреть, как мы ее будем сопрягать относительно одной и относительно другой вершины, то нужные прямые пересекут уже имеющуюся конику в точках, которые должны дать с уже имеющимися тремя точками на конике одно и то же двойное отношение, так как при симметрии относительно биссектрисы двойное отношение четверки прямых сохраняется. А значит, эти прямые пересекут эту конику в одной и той же точке, ч.т.д.

2. Понятно, что есть одна точка пересечения — точка I . Пусть есть еще точка пересечения X . Тогда ее изогональный образ так же лежит на обеих кривых. А значит коника пересекает прямую и в точке X' . Но тогда получается уже три точки пересечения прямой с коникой, что невозможно.

3. Лемма: коника, проходящая через вершины треугольника является равносторонней гиперболой тогда и только тогда, когда она проходит через его ортоцентр.

Доказательство: Рассмотрим изогональный образ этой коники в этом треугольнике. Докажем, что это будет прямая. Действительно, возьмем образ двух произвольных точек. Проведем через них прямую. Тогда если взять изогональный образ этой прямой, то он будет проходить через эти две точки и вершины треугольника. Но по этим пяти точкам единственным образом определяется прямая. Рассмотрим эту прямую. Если коника проходила через ортоцентр, что прямая будет проходить через центр описанной окружности. Заметим, что эта прямая пересекает описанную окружность в двух диаметрально противоположных точках. А значит коника будет иметь две бесконечно удаленные точки, которые будут отвечать за перпендикулярные направления. В обратную сторону аналогично.

Так как на OI проходит через O , то из доказательства леммы требуемый факт очевиден.

4. Точка I просто изогонально сопряжена самой себе. A , B и C получаются изогональным сопряжением из точек пересечения OI со сторонами треугольника. H — изогональный образ точки O . G' является центром отрицательной гомотетии вписанной и описанной окружностей. Значит G' лежит на прямой OI , а значит G лежит на гиперболы. Аналогично для N : N' будет центром положительной гомотетии вписанной и описанной окружностей.

5. Пусть l пересекает описанную окружность в точках X и Y . Тогда X и Y перейдут в X' и Y' соответственно, бесконечно удаленные точки гиперболы, точка O перейдет в H . А образ бесконечно удаленной точки прямой l обозначим через Z . Тогда, так как $(X, Y, O, Z) = -1$, то и у образов точек будет такое же двойное отношение на получившейся гиперболы. Спроектируем это двойное отношение (образов) из точки X' на прямую HZ' . При этом Y' перейдет в бесконечно удаленную точку этой прямой, а значит, так как H и Z' останутся на месте, X' перейдет в середину HZ' . Но с другой стороны X' будет проецироваться по касательной к гиперболы в точке X' , то есть по одной из асимптот гиперболы. Несложно понять, что из этого следует, что середина $Z'H$ — центр гиперболы. Осталось заметить, что H — центр положительной гомотетии окружности Эйлера и описанной окружности с коэффициентом $\frac{1}{2}$, а так как Z' образ бесконечно удаленной точки при изогональном сопряжении, то Z' лежит на описанной окружности. То есть центр гиперболы лежит на окружности Эйлера.

6. Смотри решение в книжке “Геометрические свойства кривых второго порядка”.

7. Очевидно следует из предыдущего пункта и того, что H и I лежат на гиперболы Фейербаха.

8. Так как L_B — ортоцентр треугольника ACI , то по лемме из третьей задачи получаем требуемое.

9. Заметим, что на прямой BI есть ровно одна точка для которой ее поляры относительно гиперболы Фейербаха и данной окружности совпадают. Это должна быть точка пересечения диагоналей четырехугольника образованного пересечениями нашей окружности и гиперболы Фейербаха. Заметим, что когда мы берем точку пересечения BI и FB_1 , то ее поляра действительно совпадает относительно нашей окружности и гиперболы Фейербаха: она проходит через одну и ту же точку, дополняющую ее саму и точки B и I до гармонической четверки, относительно окружности она перпендикулярна BI потому что лежит на диаметре BI . Относительно гиперболы она тоже перпендикулярна BI : поляра точки F — бесконечно удаленная прямая, так как F — центр гиперболы. Поляра точки B_1 — прямая A_1C_1 , потому что если провести через B_1 прямую AC , то гармонической четверки ее дополнит нужная точки и если провести BG через B_1 то тоже в нужной. А значит, полюс прямой B_1F — бесконечно удаленная точка прямой A_1C_1 , то есть точка отвечающая за направление перпендикулярное BI . Значит точка пересечения BI и FB_1 лежит на второй общей прямой гиперболы Фейербаха и нашей окружности.

Лемма: пусть A и B две точки на равносторонней гиперболы. Окружность, построенная на AB как на диаметре пересекает гиперболу вторично в точках P и Q . Тогда PQ проходит через центр гиперболы.

Доказательство: пусть H — ортоцентр треугольника APQ . Тогда, так как гипербола равносторонняя, он лежит на ней. Заметим также, что $HPBQ$ — параллелограмм. А значит, так как все его вершины лежат на гиперболы, то его точка пересечения диагоналей является полюсом бесконечно удаленной прямой, то есть центром гиперболы.

Получается, что вторая общая прямая гиперболы и нужной нам окружности проходит через точки пересечения BI и FB_1 и через центр гиперболы, то есть точку F , а значит, она совпадает с прямой FB_1 .

10. Приносим свои извинения, но доказательство этого пункта будет приведено позже. Возможно оно уже есть на сайте конференции.
11. Прямая GM параллельна прямой $A'C'$, а F — середина GL_B . Значит GM симметрична $A'C'$ относительно F . $L_B B_0$ параллельна BB_1 . Значит, $L_B B_0$ симметрична BB_1 относительно F . Тогда в силу симметрии гиперболы Фейербаха относительно F , получаем, что нужные прямые пересекаются на точке, симметричной B относительно F , а значит, и на гиперболы Фейербаха.
12. Заметим, что для этого достаточно доказать, что полюсы прямых FB_0 и A_1C_1 лежат на прямой AC . Полюс прямой A_1C_1 по лемме из следующего пункта — точка B_1 очевидно лежат на AC . Полюс же прямой FB_0 — точка, через которую проходят поляры точек F и B_0 . Но они обе проходят через бесконечно удаленную точку прямой AC , значит все хорошо.
13. Обозначим точку симметричную B_1 относительно E через X . Тогда $B_1A_1XC_1$ — параллелограмм. Докажем, что поляра точки A' — прямая, проходящая через A_1 и параллельная B_1C_1 .

Лемма. Поляра точки A_1 относительно гиперболы Фейербаха — прямая B_1C_1 .

Доказательство: Проведем через A_1 прямую BC . Дополнив точку A_1 и две точки пересечения этой прямой (точки B и C) с гиперболы до гармонического отношения получим точку пересечения прямых B_1C_1 и BC . Проведем прямую AA_1 . Тогда эта прямая пересечет гиперболу в точках A и G . А значит, дополнив нужную тройку до гармонической четверки мы получим точку пересечения B_1C_1 с AA_1 . Значит, поляра точки A_1 — прямая B_1C_1 .

По лемме имеем: так как A' лежит на $B'C'$, то ее поляра проходит через полюс этой прямой, то есть точку A_1 . С другой стороны A' лежит на прямой FA_1 . Значит ее поляра проходит через полюс этой прямой. Но полюс этой прямой — это пересечение поляр точек F и A_1 . Поляра F — бесконечно удаленная прямая. Поляра A_1 по лемме — прямая B_1C_1 . Значит полюс

этой прямой — бесконечно удаленная точка прямой B_1C_1 . То есть мы доказали, требуемое. Воспользовавшись аналогичным утверждением про точку C' получим требуемое.

Часть F.

1. Так как GC_1Q равнобедренный ($\angle C_1QG = \angle C_1GQ = 90^\circ - \frac{\angle B}{2}$), а $QC_1Q''A$ — параллелограмм (так как диагонали делят друг друга пополам), то AGQ_1Q'' — равнобокая трапеция. Аналогично BGP_1P'' — равнобокая трапеция. Из счета углов следует, что Q'' , G и P'' лежат на одной прямой. Получаем $P''Q'' = P''G + GQ'' = AC_1 + CA_1 = AB_1 + CB_1 = AC$.
2. Касательная в точке F параллельна QP , а значит, параллельна $P'Q'$ (см. решение из части В), а значит, и $Q''P''$, но антипараллельна C_1A_1 в углу C_1FA_1 . Заметим, что так как $Q'C_1$ параллельна AG , а AG параллельно C_1F , то Q'' , C_1 и F лежат на одной прямой. Значит, $Q''C_1A_1P''$ вписан. FG — медиана в FA_1C_1 , значит симедиана в $P''FQ''$. Из счета углов следует, что FB и FG изогонально сопряжены в углу A_1FC_1 . Значит FB — медиана. FI и FG' — соответственно радиус описанной и высота треугольника FC_1A_1 . Тогда они являются соответственно высотой и прямой, содержащей радиус описанной треугольника $FQ''P''$.
3. Обозначим точку пересечения B_1T и BC за X . Применим теорему Паскаля для шестерки точек B_1, C_1, A_1, A_1, F, T . Получим, что $A'X$ параллельна A_1C_1 . Обозначим точку пересечения B_1C_1 с BC за Y , B_1K с BC за Z , а $A'E$ с BC за Z' . $(X, Z, A_1, Y) = (T, K, A_1, C_1) = -1 = (A'X, A'E, A'A_1, A'C_1) = (X, Z', A_1, Y)$. Значит, $Z = Z'$.
4. Приносим свои извинения, но доказательство этого пункта будет приведено позже. Возможно оно уже есть на сайте конференции.
5. Пусть GG' и BB' вторично пересекаются с гиперболой Фейербаха в точках X и Y соответственно. $(A, C, L_B, X) = (GA, GC, GL_B, GX) = (GA_1, GC_1, GE, GG') = -1 = (AB, CB, A'C', BB') = (A, C, L_B, Y)$. Значит $X = Y$.
6. Покажем, что D — образ гомотетии с центром в M и коэффициентом -2 . Действительно, при этой гомотетии, B_0 переходит в B , FB_0 в BB' , FG' в себя, F в D , окружность Эйлера в описанную. Значит, так как F лежит на окружности Эйлера, то D лежит на описанной.
7. При той же гомотетии, середина C_0A_0 переходит в B_0 , значит FO_B переходит в L_BB_0 . Тогда L_BB_0 так же проходит через D .
8. Приносим свои извинения, но доказательство этого пункта будет приведено позже. Возможно оно уже есть на сайте конференции.
9. В части X доказываем, что существует эллипс проходящий через $A_0, A_1, B_0, B_1, C_0, C_1$ и F . Покажем, что все три прямые являются его диаметрами, то есть проходят через его центр. Прямая FO_B проходит через середины A_0C_0 и B_0C_1 , то есть является диаметром эллипса, соответствующим направлению AC . Отсюда также следует, что касательные к эллипсу в точках пересечения его с прямой FO_B — F и S параллельны AC . Если применить теорему Паскаля к шестерке точек $B_0, C_0, C_1, A_1, A_0, B_0$, то получим, что касательная к эллипсу в точке B_0 параллельна C_1A_1 . Тогда прямая B_0E является диаметром эллипса, так как проходит через середину хорды эллипса, A_1C_1 и через точку, касательная в которой параллельна этой хорде. Осталось показать, что BB' — тоже диаметр. Для этого покажем, что его полюсом относительно эллипса является бесконечно удаленная точка. Так как $A_1C_0 \parallel A_0C_1$, то дополнив тройки B, C_1, A_0 и B, A_1, C_0 до двойного отношения равного -1 получим, что прямая, проходящая через них будет тоже параллельна A_1C_0 , а значит, и прямой $A'C'$. Теперь покажем, что поляра точки B' — прямая $A'C'$. Для этого просто заметим, что прямая $A'C'$ пересекает прямые A_0C_0 и A_1C_1 в точках, которые дополняют тройки A_0, C_0, B' и A_1, B_1, B' до гармонических.

Приносим свои извинения, но доказательство дальнейших пунктов этой части будет приведено позже. Возможно оно уже есть на сайте конференции.

Strange properties from strange condition.

Project produced by F.Ivlev, V.Mokin, A.Zaslavskiy, O.Dmitriev and R.Genodarov.

General statement of problem.

Given a triangle ABC . Let A_0, B_0 and C_0 be the middle points of its sides, A_1, B_1, C_1 be the touching points of incircle with sides BC, AC and AB respectively. Denote intersection point of lines AA_1, BB_1, CC_1 by G (we will call it Gergonne point). Let I be the incenter of triangle ABC , O is circumcenter of $\triangle ABC$, H is common point of triangle's altitudes, F is Feuerbach point of $\triangle ABC$.

We impose only one condition on the triangle: points A, I, G and C are concyclic.

Quantifier $\forall$ in brackets before the statement of a problem means that following fact is true for any triangle (not only for triangle with our condition). Note that absence of this sign does not mean that this condition is needed.

Part A.

1. $(\forall)$ Prove that angle $\angle AIC = 90^\circ + \frac{\angle B}{2}$.
2. $(\forall)$ Prove that $\angle AIC + \angle A_1B_1C_1 = 180^\circ$.
3. $(\forall)$ Prove that line passing through A_1 parallel to bisector of angle $\angle C$ intersects line through C_1 parallel to bisector of angle $\angle A$ in point which is opposite to point B_1 in incircle.
4. Prove that if points A, G, I and C are concyclic then forth vertex F' of parallelogram A_1GC_1F' lies on incircle.
5. $(\forall)$ Prove that G is a Lemoine point of triangle $A_1B_1C_1$. Lemoine point is a point which is isogonal conjugative to center of gravity of triangle.
6. Prove that in our case center of gravity of triangle $A_1B_1C_1$ lies on circumcircle of triangle A_1IC_1 .
7. Construct a triangle with our condition and given angle $\angle B$. For instance by vertex B and incircle.
8. Prove that angle $\angle B$ is less than 60° .

Part B.

Let intersection point of AA_1 with incircle which is different from A_1 be Q , and the same for CC_1 is P . Let K be moving point on incircle. Denote intersection point of KP with BC by P' , and KQ with AB by Q' .

This part is not necessary for following parts of project.

1. Prove that line passing through P parallel to BC and line passing through Q parallel to AB intersect in a point on incircle. Denote this point by T .
2. Find locus of midpoint of segments $P'Q'$.
3. Let A_1C_1 intersect AC in point R . We draw lines parallel to AB and BC through point R and intersect them with BC and AB in points P_1 and Q_1 respectively. Prove that lines PP_1 and QQ_1 have a common point on incircle.
4. ($\forall$) Prove that points P , Q and R are collinear.
5. Let P_2 be intersection point of B_1C_0 and BC and Q_2 be intersection point of B_1A_0 and AB . Prove that lines PP_2 and QQ_2 intersect on incircle.
6. Prove that line which passing through midpoint of segment AC_1 and Q and line which passing through midpoint of segment CA_1 and P intersect on incircle. From this time point K is this intersection point. It start be fixed. Points P' and Q' are fixed also and equals P' and Q' for this position of K .
7. Prove that points T , K and B lie on one line.
8. Prove that lines BK and BF' are isogonal conjugative in angle $\angle B$.
9. Prove that points K , G and F' are collinear.
10. Let E be midpoint of the segment A_1C_1 . Prove that E is incenter of triangle $P'Q'B$.

Later we will not be needed in points P , Q , P' , Q' and R (may be sometimes we will use last one). We recommend you draw your picture again without these points.

Part C.

Three lines passing through Feuerbach point.

Still this part is very important for the project but very difficult we allow using in solutions previous facts without proof. Also it will be allowed using in future solutions items from this part without proof.

In this part there are fact which are true for all nonisosceles triangles so we omit sign $\forall$ before items.

1. Let points A' , B' , C' be the intersection points of the respective sides of triangles $A_0B_0C_0$ and $A_1B_1C_1$. Prove that the vertices of triangle ABC lie on the sides of triangle $A'B'C'$
2. Prove that triangle $A'B'C'$ is autopolar with respect to (later wrt) the incircle. I. e. each of its sides is the polar line of the opposite vertex.
3. Prove that lines AA' , BB' , CC' are parallel.
4. Prove that line IG passes through the common points of the corresponding sides of triangles $A_1B_1C_1$ and $A'B'C'$.
5. Let M be a centroid of triangle ABC . Prove that line IM passes through the intersection points of the respective sides of triangles $A_0B_0C_0$ and $A'B'C'$.
6. Prove that lines AA' , BB' , CC' are parallel to a line passing through the intersection points of the respective sides of triangles $A_1B_1C_1$ and ABC . I. e. they are parallel to a polar of G in incircle.
7. Let C_A be an intersection point of CI and C_1A_1 and C_B be an intersection point of CI and C_1B_1 . Points A_B , A_C , B_A , B_C are defined by the same way. Prove that points A , C_1 , C_A , I are concyclic.
8. Prove that C_A lie on B_0C_0 .
9. Prove that circumcenter of triangle $C_AC_BC_1$ is point C_0 .
10. Prove that points C_A , C_B , A_B , A_C lie on one circle which is orthogonal to the incircle (two circles are orthogonal if their tangents in common point are orthogonal). Denote this circle by ω_B . Three analogous circles denote by ω_A and ω_C respectively.
11. Let circles ω and γ be orthogonal and let P and Q be their centers respectively. Prove that the polar of P wrt γ , the polar of Q wrt ω and the radical axis of γ and ω coincide.
12. Given inscribed quadrilateral $ABCD$. Let N be a common point of AB and CD , M be a common point of BC and AD , and P be a common point of AC and BD . Prove that NM is the polar line of P wrt circumcircle of $ABCD$.
13. Denote the center of ω_B by O_B . Points O_A and O_C are defined similarly. Prove that O_B lie on $A'C'$.
14. Prove that the midpoints of the sides of triangle ABC lie on the sides of triangle $O_AO_BO_C$.
15. Prove that triangle $A_0B_0C_0$ is orthotriangle of triangle $O_AO_BO_C$. That is points A_0 , B_0 , C_0 are the feet of the altitudes of triangle $O_AO_BO_C$.
16. Let M_B be a midpoint of side O_AO_C . Points M_A and M_C are defined by the same way. Prove that triangles $A_1B_1C_1$ and $M_AM_BM_C$ are homothetic.
17. Prove that points B' , M_B and B_1 are collinear.
18. Prove that lines A_1A' , B_1B' , C_1C' pass through the Feuerbach point of triangle ABC .

19. Prove the Feuerbach theorem. I.e. the incircle and the Euler's circle of a nonisosceles triangle touche.
20. Prove that the tangent to the incircle through F passes through the common points of the corresponding sides of triangles ABC and $A'B'C'$.
21. Prove that points B_C , C_B , A_1 , A_0 are concyclic.
22. Prove that F lies on the circle from previous item.
23. Invent another proof of the fact that line A_1A' passes through F .

Part D.

1. Let A'' be an intersection point of $F'A_1$ and B_1C_1 . Points B'' and C'' are defined similarly. Prove that triangle $A''B''C''$ is autopolar wrt the incircle and the vertices of triangle ABC lie on their sides.
2. Prove that the points which are symmetrical to points A and C wrt A_1 and C_1 respectively lie on line $A''C''$.
3. Prove that BC_1A_0C'' and BA_1C_0A'' are parallelograms.
4. Prove that $F' = F$. I.e. F' is the Feuerbach point of triangle ABC .
5. Let a be a length of BC , b be a length of AC and c be a length of AB . Prove that $(a + c - b)^2 = ac$.
6. Prove that if $(a + c - b)^2 = ac$ then our condition (about point A , G , I and C) is true.
7. Prove that F is a centroid of triangle $A'B_0C'$.
8. Let S be midpoint of $A'C'$. Prove that FB_0 pass through it.
9. Prove that S is a midpoint of segment BO_B .
10. Prove that SE is parallel to BB_1 .
11. Prove that $O_B F$ is parallel to BB_1 .
12. Prove that F is centroid of triangle $O_B A_0 C_0$.
13. ($\forall$) Let L_B be a pole of $A_0 C_0$ wrt the incircle. Prove that L_B is intersection point of $A'C'$ and GE .
14. ($\forall$) Prove that I is orthocenter of triangle ACL_B .
15. ($\forall$) Let G' be a point isogonal conjugated to point G . Prove that G' is center of homotety of the incircle and the circumcircle of the initial triangle.
16. Prove that G' is symmetrical to point G wrt bisector of angle $\angle B$.
17. ($\forall$) Prove that points F , G' and M are collinear.
18. Prove that FM is parallel to bisector of angle $\angle B$.
19. Prove that GM is parallel to $A'C'$.
20. Prove that O_B is midpoint of BL_B .
21. Prove that F is a centroid of triangle $A_1 L_B C_1$.
22. Prove that the common point of $A_1 C_1$ and OI is isogonally conjugated to L_B .

Part X.

1. ($\forall$) Prove that the image of a line which not pass through the vertices of the triangle under isogonal conjugation is a conic.
2. ($\forall$) Prove that the image of line OI under isogonal conjugation is a conic which tangents this line.
3. ($\forall$) Prove that the image of line OI under isogonal conjugation is a hyperbola with perpendicular asymptotes. This hyperbola is called Feuerbach hyperbola.
4. ($\forall$) Prove that points A, B, C, I, H, G and N lie on Feuerbach hyperbola where N is a Nagel point of triangle ABC .
5. ($\forall$) Let l be an arbitrary line passing through O . Denote by l' conic which is an image of line l under isogonal conjugation. Prove that center of l' lie on Euler circle.
6. ($\forall$) Let an equilateral hyperbola pass through the vertices of the triangle ABC and P be an arbitrary point on it. Prove that the circumcircle of the pedal triangle of point P passes through the center of this hyperbola.
7. ($\forall$) Prove that center of the Feuerbach hyperbola is a Feuerbach point.
8. ($\forall$) Prove that L_B lies on the Feuerbach hyperbola.
9. ($\forall$) Prove that line FB_1 , the circumcircle of triangle A_1C_1I and Feuerbach hyperbola have two common points.
10. Prove that locus of centers of images of lines passing through I under isogonal conjugation is an ellipsis which passes through the feet of bisectors, the midpoints of the sides and the Feuerbach point.
11. Prove that lines B_0L_B and GM intersect on the Feuerbach hyperbola.
12. ($\forall$) Prove that intersection point of lines FB_0 and A_1C_1 is a pole of line AC wrt the Feuerbach hyperbola.
13. ($\forall$) Prove that the pole of line $A'C'$ wrt the Feuerbach hyperbola is a point which is the reflection of B_1 in E .

Part F.

1. Let Q'' be a reflection point of Q in Q' . Point P'' is defined simultaneously. Prove that $P''Q'' = AC$.
2. Prove that in triangle $P''FQ''$:
 - FB is a median.
 - FI is an altitude.
 - FG' is a line joining F with the circumcircle of triangle $P''Q''F$.
 - FG is a symmedian.
3. Prove that line KB_1 passes through the intersection points of $A'E$ with BC and $C'E$ with AB .
4. Prove that line KB_1 passes through the intersection point of $A'C'$ and A_0C_0 .
5. Prove that GG' and BB' intersect on the Feuerbach hyperbola.
6. Prove that FG' and BB' intersect on the circumcircle of triangle ABC . Denote this point D .
7. Prove that line L_BB_0 passes through D .
8. Denote the Feuerbach point of triangle $BP'Q'$ by F'' . Prove that FF'' is parallel to BB_1 .
9. Prove that lines FO_B , EB_0 and BB' are concurrent.
10. Prove that the Feuerbach hyperbola of triangle $P''Q''B$ passes through point B' .
11. Prove that the Feuerbach hyperbola of triangle $P''Q''B$ passes through L_B .
12. Let C'_1 be a touching point of incircle of triangle $BP''Q''$ with side QB . Points A'_1 and B'_1 are defined simultaneously. Prove that the image of line $A'_1C'_1$ under homothety with center F and coefficient 4 is line A_1C_1 .
13. ($\forall$) Prove that lines A_0A' , B_0B' , C_0C' and the tangent to the incircle through F are concurrent. Denote this intersection point by M' .
14. Prove that M' lies on the bisector of angle $\angle B$.
15. ($\forall$) We intersect lines passing through F and parallel to AA_1 , BB_1 , CC_1 with lines AA' , BB' , CC' respectively. Prove that these three points lie on line GM .
16. ($\forall$) We intersect lines passing through M' and parallel to AA_0 , BB_0 , CC_0 with lines AA' , BB' , CC' respectively. Prove that these three points lie on line IM .

Part A.

Solutions.

1. This immediately follows from calculation of angles.
2. This item clearly follows from the previous item.
3. It is clearly follows from the fact that the angle between bisector of angle $\angle A$ and line B_1C_1 is right.
4. This item follows from two previous and the properties of the inscribed angle.
5. Let E be a midpoint of segment A_1C_1 . Let X be an intersection point of B_1E with incircle different of B_1 . Let's calculate degree of point E with respect to the circumcircle of BA_1IC_1 . We get $BE \cdot EI = EA_1 \cdot EC_1$. Now write the equation on degree wrt the incircle $EA_1 \cdot EC_1 = EX \cdot EB_1$. So by $BE \cdot EI = EX \cdot EB_1$ we obtain that quadrilateral $BXIB_1$ is inscribed. $IX = IB_1$ as radii. So angles $\angle B_1BI$ and $\angle IBX$ are equal. Let Y be an intersection point of BB_1 and the incircle different of B_1 . From the above we obtain that $XY \parallel A_1C_1$. Hence lines B_1X and B_1Y are isogonally conjugated in angle $\angle A_1B_1C_1$. Let's project cross-ratio of points A_1, C_1, E and infinity point of line A_1C_1 from point X into the incircle. Since cross-ratio of the initial quadruple equals -1 cross-ratio of images is equals -1 also. So we get that $(A_1, C_1, B_1, Y) = -1$ for any concyclic quadrilateral in which tangents through two of their vertices intersect on diagonal passing through two other vertices. As you remember such quadrilateral are called harmonic.
6. It is easy to prove this fact using previous item and angles calculation.
7. At first we draw tangents from point B wrt the incircle. So we obtain points A_1 and C_1 . Now construct midpoint of A_1C_1 point E . From previous item we know that the circumcircle of triangle A_1IC_1 divide segment B_1E in ratio $2 : 1$. So if we make homothety with center E and coefficient 3 then the image of the circumcircle of triangle A_1IC_1 pass through B_1 . So if we intersect this image with the incircle we obtain two symmetrical solutions of point B_1 . Now it is easy to construct vertices A_1 and C_1 .
8. From solution of previous item clearly follows that IE must be at most than half of radius of the incircle. From this fact it easy to prove that $\angle A_1IC_1$ is at least 120° . So angle $\angle B$ which is equal $180^\circ - \angle A_1IC_1$ is at most 60° .

Часть В.

Решения.

Пусть вторая точка пересечения AA_1 со вписанной окружностью — точка Q , а вторая точка пересечения CC_1 со вписанной окружностью — P . Теперь пусть K — бегающая точка по вписанной окружности. Обозначим точку пересечения KP с BC через P' , а KQ с AB через Q' .

Эту часть можно не решать. Факты из нее не используются в дальнейшем.

1. Since $\angle PGQ = 90^\circ + \frac{\angle B}{2}$, we obtain that the sum of arcs PQ and A_1B_1 is equal to $180^\circ + \angle B$. Since arc A_1C_1 is equal to $180^\circ - \angle B$, arc PQ is equal to $2\angle B$. Thus, if the line passing through Q and parallel to BA meets secondary the incircle in point T , then $\angle QTP = \angle B$. Therefore $TP \parallel BC$.
2. Let point P' move on BC with constant velocity. Then Q' moves in such way that the cross-ratios of different points P' and Q' are equal. Therefore the correspondence between P' and Q' is projective. But by previous item P' and Q' are infinity points of the respective lines simultaneously. Thus this correspondence is affine, i.e. point Q also moves with constant velocity. Therefore the locus of midpoints is a line. Considering the cases $K = A_1$ and $K = C_1$ we obtain that this line is the Gauss line of quadrilateral AC_1A_1C .
3. Since the locus from previous item is the Gauss line of A_1C_1AC , it contains the midpoints of third "diagonal". Let R' be the midpoint of RB . Find points P' and Q' on AB and BC respectively such that R' is the midpoint of $P'Q'$. Then $P'BQ'R$ is a parallelogram i.e. P', Q' coincide with P, Q .
4. Note that the projection of a circle to the same circle from a point not lying on this circle conserves the cross-ratios. In fact, let the center of projection lie outside the circle. Then there exists a projective map conserving the circle and transforming the projection center to an infinity point. The projection from such point coincides with the reflection in some diameter and so conserves the cross-ratios. If the projection center lies inside the circle we can transform this point to the center of the circle. In this case the projection coincides with the reflection in the center and also conserves the cross-ratios. Now note that quadrilateral $B_1C_1A_1P$ is harmonic because the tangents in points B_1 and A_1 meet on diagonal C_1P . Consider the projection of this quadrilateral from point R to the same incircle. It interchanges points A_1 and C_1 and fixes B_1 . Thus the image of P is the fourth harmonic point for B_1, A_1, C_1 , i.e. point Q . Therefore P, Q and R are collinear.
5. Points R, B_1, A, C are harmonic because the Gergonne triangle is cevian. Project these points from the infinity point of AB to BC . Let the images of R, A, C, B_1 be P_1, B, C, B'_1 respectively. Project these four points from B_1 to AB . This projection transforms B'_1 to the infinity point, fixes B and transforms C to A . Since four points are harmonic it transforms P_1 to the midpoint, i.e. $P_1 = P_2$. Now use the assertion of problem 2.
6. Note that if $P' = A$ then $Q' = A_1$, and if $P' = C_1$ then $Q' = C$. Therefore when one of points is the midpoint of the corresponding segment the second one also is the midpoint.
7. Consider the projection of line BC from P to the incircle. It transforms P', A_1, C and the infinity point to K, A_1, C_1 and T respectively. Since the cross-ratio of these points is equal to -1, the diagonal TK passes through the common point of tangents in A_1 and C_1 .
8. Arcs TC_1 and C_1Q are equal because the tangent in C_1 is parallel to QT . Arcs C_1Q and A_1F' are equal because $C_1F' \parallel QA_1$. Thus arcs C_1T and $F'A_1$ are equal which yields the symmetry wrt the bisector of $\angle B$.
9. See the solution of problem 5 from part A. Inversing its reasoning and using two previous items we obtain the assertion of the problem.

10. Consider the homothety with center K transforming P to P' . It transforms T to B and thus the image of Q is Q' . Since $Q'E$ is parallel to QG as medial line, we have that it transforms G to M . Since PG passes through the midpoint of arc QT , PQ is the bisector of triangle PQT . Then QA_1 also is the bisector. Therefore G is the incenter of triangle QTP . Thus its image M is the incenter of triangle $Q'BP'$.

Part C.
Solutions.

1. Let lines BC' and AC meet in point R . For prove that B lies on $A'C'$, it is sufficient to prove that cross-ratios (A, C_0, B, C_1) and (A, B_0, R, B_1) are equal. By the Ceva theorem $\frac{AC_0}{C_0B} = \frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B}$, $\frac{AC_1}{C_1B} = \frac{AB_1}{B_1C} \cdot \frac{CA_1}{A_1B}$. From this and an equality $(C, A_0, B, A_1) = (C, B_0, R, B_1)$ (projection from C'') we obtain

$$\frac{AC_0}{C_0B} \cdot \frac{C_1B}{AC_1} = \frac{AB_0}{B_0C} \cdot \frac{CA_0}{A_0B} \cdot \frac{BA_1}{A_1C} \cdot \frac{CB_1}{B_1A} = \frac{AB_0}{B_0C} \cdot \frac{CB_0}{B_0R} \cdot \frac{B_1R}{B_1C} \cdot \frac{CB_1}{B_1A} = \frac{AB_0}{B_0R} \cdot \frac{B_1R}{AB_1}$$

2. Let lines A_1C_1 and AC meet in point R . Project cross-ratio $(A, C, B_1, R) = -1$ to line B_1C_1 from point B' . This projection transforms C, A, R to A', X, C_1 respectively and fixes B_1 . Therefore $(B_1, C_1, A', X) = -1$, i.e. the polar of A' passes through X and the pole of B_1C_1 coinciding with A . Thus it is line AX which coincide with $B'C'$ by previous item.

3. **Lemma.** Let triangle $A_1B_1C_1$ be cevian for ABC . Points A', B' and C' on its sidelines are such that the vertices of triangle ABC lie on the sidelines of triangle $A'B'C'$. Let A_0 be the common point of B_1C_1 and BC . Points B_0 and C_0 are defined similarly. Then lines AA', BB', CC' and $A_0B_0C_0$ concur.

Proof. Consider triangles $CA'A_0$ and $C'AC_0$. We have $CA' \cap C'A = B'$, $A'A_0 \cap AC_0 = C_1$, $A_0C \cap C'C_0 = A_1$, and these three points are collinear. By Desargues theorem lines CC', AA', A_0C_0 concur. Since points A_0, C_0, B_0 are collinear (clearly follows from Ceva and Menelaos theorems), we obtain the assertion of the problem.

Now note that in our case one of considered triangles is medial. Thus the corresponding lines meet on the infinity point, i.e. they are parallel.

4. Use the Pappus theorem to points A, B_1, C and C_1, B', A_1 , and after this to points A, B_1, C and C_B, B', A_B . (see problem 7)
5. Similarly to previous item use the Pappus theorem to points A, B_0, C and C_0, B', A_0 , and after this to A, B_0, C and C_A, B', A_C . (see problem 7)
6. Use the lemma of problem 3 to the Gergonne triangle.
7. $\angle B = 180^\circ - \angle A - \angle C \Rightarrow \angle BA_1C_1 = \frac{180^\circ - \angle B}{2} = \frac{\angle A + \angle C}{2} \Rightarrow \angle(A_1B, A_1C_1) = \angle(A_1C, CI) + \angle(AI, AC_1) \Rightarrow \angle(AI, AC_1) = \angle(A_1B, A_1C_1) - \angle(A_1C, CI) = \angle(A_1C, A_1C_A) - \angle(CA_1, CC_A) = \angle(IC_A, CA_1) + \angle(A_1C, C_1C_A) = \angle(IC_A, C_A C_1)$. Therefore A, C_1, C_A, I are concyclic.
8. By previous item C_A is the projection of A to the bisector of angle B . Thus angle AB_0C_A as central angle in triangle ACC_A is twice greater than angle C of this triangle, i.e. it is equal to angle C of triangle ABC . Therefore $B_0C_A \perp BC$, and C_A lies on the medial line.
9. Since C_0C_A is parallel to BA_1 , triangle $C_1C_0C_A$ is isosceles. Thus $C_0C_1 = C_0C_A$. Similarly $C_0C_1 = C_0C_B$.
10. The circle from previous item is orthogonal to the incircle because it passes through C_1 and its center lies on the tangent to the incircle in this point. Since C_A and C_B are collinear with the incenter, they are symmetric wrt the incircle. This is also true for points A_B and A_C . Thus $IC_A \cdot IC_B = r^2 = IA_B \cdot IA_C$, where r is the inradius. Therefore these four points lie on the circle which is fixed under the inversion and so is orthogonal to the incircle.
11. By the properties of polars and radical axis all these lines coincides with a common chord of given circles.

12. Using the Pascal theorem to points A, B, B, D, C, C we obtain that the tangents in B and C meet on line NP . Similarly the tangents in A and D meet on this line. Consider now the polar of point M . This line passes through the poles of BC and AD . By above it is line PN . Thus M is the pole of PN . Similarly for two remaining points.
13. Point O_B lie on $A'C'$ iff the polar of O_B wrt the incircle passes through the pole of $A'C'$ i.e. point B' . Since ω_B is orthogonal to the incircle the polar of O_B wrt the incircle coincide with the polar of I wrt ω_B . But for quadrilateral $C_B C_A A_B A_C$ inscribed into ω_B четырехугольника I is a common point of the oppsite sidelines, and B' is a common point of the diagonals. Thus the polar of I passes through B' .
14. Since ω_B, ω_A and the circumcircle of triangle $C_A C_B C_1$ passe through points C_A and C_B , their centers are collinear.
15. By previous item $O_B O_A$ is perpendicular to $C_A C_B$, which is the bisector of angle C . Then it is also perpendicular to the bisecor of angle C_0 of triangle $A_0 B_0 C_0$. Therefore the sidelines of $O_A O_B O_C$ are the external bisectors of $A_0 B_0 C_0$. This clearly yields the assertion of the problem.
16. The sidelines of these triangles are perpendicular to the corresponding bisectors of original triangle.
17. Project cross-ratio $(A, C, B_1, R) = -1$ from B' to $O_A O_C$. This projection transforms A, C and R to O_A, O_C and infinity point respectively. Thus it transforms B_1 to M_B .
18. Note that $M_A, M_B, M_C, A_0, B_0, C_0$ lie on the Euler circle of triangle $O_A O_B O_C$. Then the homothety center of triangles $A_1 B_1 C_1$ and $M_A M_B M_C$ is also the homothety center of their circumcircles, i.e. the Euler circle of original triangle (because $\omega_{M_A M_B M_C} = \omega_{A_0 B_0 C_0}$ is the Euler circle of original triangle) and its incircle. Therefore this homothety center coincide with the Feuerbach point. But by previous item line $M_A A_1$ passes also through point A' . Thus $A_1 A'$ passes through the Feuerbach point.
19. Since $A_0 B_0 C_0$ is the medial triangle of ABC and the orthotriangle of $O_A O_B O_C$, the Euler circles of these two triangles coincide. Thus points M_A, M_B, M_C lie on the Euler circle of original triangle. But triangles $A_1 B_1 C_1$ and $M_A M_B M_C$ are homothetic, so their circumcircles are also homothetic. It is sufficient to prove that the homothety center lie on one of these circles. Let AA' meet the incircle in point R . Since B' lies on the polar of A' wrt the incircle and on the diagonal $A_1 C_1$ of quadrilateral $A_1 B_1 C_1 R$, we obtain that B' is the common point of the diagonals of this quadrilateral. The same is true for CC' . Thus the homothety center lies on the incircle and the circles touche.
20. This problem is dual to item 18.
21. See the solution of the next item.
22. **Lemma 1.** $\angle(A_0 F, F A_1) = (\angle(CA, CB) + \angle(BA, BC))/2$.

Proof. Prove that $\angle(A_0 F, FH) = \angle(CA, CB) + \angle(BA, BC)$, where H is the foot of altitude from A to BC . Then the sought assertion will follow from Archimedes lemma. Note that $\angle(A_0 F, FH) = \angle(A_0 B_0, B_0 H)$ because all these points lie on the Euler circle. Also since B_0 is the midpoint of the hypotenuse of right triangle AHC , we have $\angle(CA, CB) = \angle(CB_0, CH) = \angle(HC, HB_0)$. Thus $\angle(A_0 B_0, B_0 H) = \angle(A_0 B_0, A_0 H) + \angle(A_0 H, HB_0) = \angle(BA, BC) + \angle(CA, CB)$, q.e.d.

Lemma 2. Points B_C, C_B, A_1, A_0 and F are concyclic.

Proof. Prove that $\angle(A_0 C_B, C_B A_1) = \angle(A_0 F, F A_1)$. Since $C_B I A_1 B$ is cyclic we have $\angle(C_B I, C_B A_1) = \angle(BI, BA_1) = \angle(BA, BC)/2$. Since $C_B A_0 = A_0 C$, we obtain an equality $\angle(A_0 C_B, C_B C) = \angle(CC_B, C_A A_0) = \angle(CA, CB)/2$. From this $\angle(A_0 C_B, C_B A_1) = \angle(A_0 C_B, C_B C) + \angle(C_B C, C_B A_1) = \frac{\angle(CA, CB) + \angle(BA, BC)}{2} = \angle(A_0 F, F A_1)$. Thus C_B lies on the circumcircle of $\triangle A_1 A_0 F$. Similarly B_C lies on this circle.

- 23.** We proved that A_1F is the radical axis of the incircle and the circumcircle of triangle $C_B B_C A_1$. Thus it is sufficient to prove that A' lies on this line. Note that A' is the homothety center of triangles $C_0 C_1 C_B$ and $B_0 B_C B_1$ because the corresponding sidelines of these triangles are parallel. Therefore $\frac{A'C_1}{A'B_C} = \frac{A'C_B}{A'B_1}$, and we obtain an equality of degrees: $A'C_1 \cdot A'B_1 = A'C_B \cdot A'B_C$.

Part D.

1. Triangle $A''B''C''$ is autopolar because its vertices are the common points of quadrilateral $A_1B_1C_1F'$. Since a polar A_1B_1 of point C passes through C'' , a polar $A''B''$ of C'' passes through C . Similarly for remaining vertices.
2. Let X be a common point of AA_1 and $A''C''$. The cross-ratio of A, B, C_1 and the common point of AB and A_1B_1 is equal to -1 . Projecting these points from C'' to AA_1 we obtain that A_1 is the midpoint of AX .
3. The homothety with center A and coefficient 2 transforms line C_0A_1 to line $A''C''$. Thus these lines are parallel. Using the homothety with center B transforming CC_1 to A_1F' we obtain that the midpoint of $A'A_1$ lies on AB . Thus BA_1C_0A'' is a parallelogram.
4. By previous item C' lies on the medial line of ABC parallel to AB . Then $C'' = C'$. Similarly $A'' = A'$. Thus $F' = F$.
5. By problem 3 C_0A_1 is parallel to C_1A_0 , i.e. $BC_1 \cdot BA_1 = BC_0 \cdot BA_0$. Expressing these lengths through a, b, c and multiplying to 4 we obtain the sought equality.
6. Given equality yields that C_0A_1 is parallel to C_1A_0 . Construct parallelograms BC_1A_0C'' and BA_1C_0A'' . Line $A''C''$ passes through B . The homothety with center A and coefficient 2 transforms line C_0A_1 to $A''C''$. Let it transform A_1 to point X . Projecting from C'' points A, X, A_1 and infinity point of AA_1 to line AB we obtain that the cross-ratio of A, B, C_1 and the common point of AB and A_1C'' is equal to -1 . Thus A_1C'' passes through B_1 . Then $C'' = C'$ i.e. triangles BC_1C' and BAX have a common median. Therefore they are homothetic with center B . So C_1C' is parallel to AA_1 and GC_1FA_1 is a parallelogram. Now our condition follows from an angles calculation.
7. By problem 3 $C'F$ passes through the midpoint of BA_0 . Using the homothety with center C' we obtain that $C'F$ passes through the midpoint of $A'B_0$, i.e. $C'F$ is the median of triangle $A'B_0C'$. Similarly for $A'F$.
8. By previous item B_0F is the median of triangle $A'B_0C'$.
9. Since O_B is the circumcenter of triangle $A_0B_0C_0$ we obtain that $O_BC_0A_1C'$ is a parallelogram, and by problem 2 BA_1C_0A' is a parallelogram. Thus $A'B = C_0A_1 = O_BC'$.
10. Line SM as Gauss line of $A_1B_1C_1F$ passes through the midpoint of FB_1 . Thus as medial line of triangle FGB_1 it is parallel to BB_1 .
11. By previous item SM is parallel to O_BF . Then F and O_B lie on the reflection of line O_BF in SM , because they are the reflection of G in M and the reflection of B in S .
12. Since S is the midpoint of BO_B and F divides B_0S in ratio $2 : 1$ we obtain that F is the centroid of triangle B_0O_BB . Then the median of this triangle from O_B also is divided by F in ratio $2 : 1$. Thus the endpoint of this median coincide with the midpoint of BB_0 , and so with the midpoint of C_0A_0 . This yields the assertion of the problem.
13. Consider the polar transformation. Since B' lies on C_0A_0 we obtain that L_B lies on $A'C'$. Now we have to prove that the polars of G and M meet on the medial line. Note that the polar of G is parallel to BB' and passes through the common point R of A_1C_1 and AC . The polar of M passes through B and is parallel to A_1C_1 . Points B, B', R and the common point of the polars form a parallelogram. Since the midpoint of BR lies on A_0C_0 and B' also lies on this line, then A_0C_0 passes through the common point of the polars of G and M .

14. Since C_B lies on A_0C_0 , L_B lies on its polar, i.e. line AC_A , thus $AL_B \perp CI$. Similarly $AI \perp CL_B$ and we obtain the sought assertion.
15. By angles calculation we obtain that the reflections of vertices of Gergonne triangle in the corresponding bisectors form the triangle homothetic to the original triangle. Thus the lines joining the corresponding vertices of these triangles pass through the homothety center of the incircle and the circumcircle. But G' is the common point of these lines.
16. Clearly A, G, I, G' and C lie on the circle with center on the bisector of angle B , and G' lies inside the triangle. Also G' lies on the line symmetric to BG wrt the bisector of B . This yields the assertion of the problem.
17. Clearly follows from three homothety centers theorem for the incircle, the circumcircle and the Euler circle.
18. Since A_1 and C_1 are symmetric wrt the bisector of angle B , and A_1FC_1G is a parallelogram we obtain using two previous items that A_1FC_1G' is a delthoid with diagonal FM . Thus FM is perpendicular to A_1C_1 and parallel to the bisector of angle B .
19. In next item we will prove that O_B is the midpoint of BL_B . Therefore O_BF is a medial line of triangle L_BBG . Thus F is the midpoint of L_BG . Then F divide L_BE in ratio $2 : 1$.
20. AL_B is parallel to C_0O_B as two perpendiculars to CI . Thus the homothety with center B and coefficient 2 transforms O_B to L_B .
21. L_BF is the median of triangle $A_1L_BC_1$ and by previous item F is the midpoint of L_BG . Thus F divide L_BM in ratio $2 : 1$. Then F is the centroid of triangle $A_1L_BC_1$.
22. Let point X be isogonally conjugated to L_B . Since L_B lies on the Feuerbach hyperbola (see part X), X lies on line OI . Prove that X lies on line A_1C_1 . Let X' be the reflection of X in the bisector of angle B . Since OI passes through G' , this reflection transforms OI to IG . Also it fixes line A_1C_1 and transforms line BX to line BL_B , i.e. to line $A'C'$. Lines $A'C'$ and A_1C_1 meet on IG as corresponding sidelines of triangles $A'B'C'$ and $A_1B_1C_1$. Thus X' lies on A_1C_1 , and so X also lies on this line.

Part X

1. Take two vertices and the images of three arbitrary points on the line. They define some conic. Take an arbitrary fourth point on the line. When we conjugate the corresponding lines in two angles the conjugated lines intersect the conic at the same point because the reflection in the bisector saves the cross-ratios of four lines.
2. Clearly I is a common point. Suppose that there exists another common point X . Then its isogonally conjugated point X' also lies on the line and the hyperbola. But a line and a conic can't have three common points.

3. **Lemma.** A circumconic of a triangle is an equilateral hyperbola iff it passes through the orthocenter.
Proof. The isogonal image of a circumconic is a line because five points define a unique conic. When the conic passes through the orthocenter the corresponding line passes through the circumcenter. This line meets the circumcircle at two opposite points. Thus the conic has two infinity points corresponding to two perpendicular directions.

The problem immediately follows from the lemma.

Let R the midpoint of arc BC of the circumcircle of ABC . Then OR is parallel to IB_1 , and external angle $\angle BOR$ is twice greater than angle BRO , which is equal to $\angle B_1IR$. Thus the reflection of IB_1 in IR is the line parallel to OB . Therefore the tangent to the incircle in X is parallel to the tangent to the circumcircle in B , and this immediately yields the assertion of the problem.

4. Point I is isogonally conjugated to itself, A , B and C are isogonally conjugated to the common points of OI with the sidelines, H is isogonally conjugated to O . Since G' is the homothety center of the incircle and the circumcircle, G' lies on OI . Thus G lies on the hyperbola. Similarly for N : N' is the second homothety center of the incircle and the circumcircle.
5. Let l meet the circumcircle in points X and Y . Then X and Y are isogonally conjugated to infinity points X' and Y' of the hyperbola, O is conjugated to H . Let Z be conjugated to the infinity point of l . Since $(X, Y, O, Z) = -1$, the cross-ratio of the conjugated points is the same. Project this cross-ratio from X' to line HZ' . This projection transforms Y' to the infinity point of this line. Since H and Z' are fixed, the projection of X' is the midpoint of HZ' . But the projection of X' lie on the tangent to hyperbola in X' , i.e. on the asymptote of the hyperbola. This yields that the midpoint of $Z'H$ is the center of hyperbola. Finally note that H is the homothety center of Euler circle and the circumcircle and Z' lies on the circumcircle as the image of infinity point Z' . Thus the center lies on the Euler circle.
6. See the solution in book "Geometrical properties of conics".
7. Follows from previous item.
8. Since L_B is the orthocenter of triangle ACI , the sought assertion follows from the lemma of problem 3.
9. Note that there exists exactly one point of line BI such that its polars wrt the hyperbola and the circle coincide. It is the common point of the diagonals of the quadrilateral formed by the common points of these two conics. Take now a common point of BI and FB_1 . Its polars pass through the point which is the fourth harmonic for our point B and I . The polar wrt the circumcircle is perpendicular to BI because BI is a diameter. The polar wrt the hyperbola is also perpendicular to BI : the polar of F is the infinity line because F is the center of the hyperbola. The polar of B_1 is the line A_1C_1 , because the corresponding points on lines AC and BG are harmonic. Thus the pole of B_1F is the infinity point of A_1C_1 , i.e. the point corresponding to the direction perpendicular to BI . Therefore the common point of BI and FB_1 lies on the common chord of the hyperbola and the circle.

Lemma. Let A and B be two point on an equilateral hyperbola. A circle with diameter AB meets the hyperbola at points P and Q . Then PQ passes through the center of the hyperbola .

Proof. Let H be the orthocenter of APQ . Since the hyperbola is equilateral H lies on it. Note that $HPBQ$ is a parallelogram. Since its vertices lie on the hyperbola its center is the pole of the infinity line, i.e. the center of the hyperbola.

Now we have that the common chord passes through the common point of BI and FB_1 . Also it passes through the center F of the hyperbola. Therefore it coincide with FB_1 .

10. Line GM is parallel to $A'C'$, and F is the midpoint of GL_B . Thus GM is the reflection of $A'C'$ in F . Line L_BB_0 is parallel to O_BF and BB_1 . Thus L_BB_0 is the reflection of BB_1 in F . Since the Feuerbach hyperbola is symmetric wrt F , we obtain the assertion of the problem.
11. It is sufficient to prove that the poles of FB_0 and A_1C_1 lie on AC . The pole of A_1C_1 is point B_1 clearly lying on AC . The pole of FB_0 is the common point of polars of points F and B_0 . But these both polars pass through the infinity point of AC .
12. Denote the reflection of B_1 in E as X . Then $B_1A_1XC_1$ is a parallelogram. Prove that the polar of A' is the line passing through A_1 and parallel to B_1C_1 .

Lemma. The polar of A_1 wrt the Feuerbach hyperbola is line B_1C_1 .

Proof. Consider passing through A_1 line BC . The fourth harmonic point for A_1 and two common points of this line with the hyperbola (B and C) is the common point of B_1C_1 and BC . Take line AA_1 . It meets the hyperbola at points A and G . The fourth harmonic point for these three points is the common point of B_1C_1 and AA_1 . Thus the polar of A_1 is the line B_1C_1 .

Use the lemma. Since A' lies on $B'C'$, its polar passes through the pole A_1 of this line. On the other hand A' lies on line FA_1 . Thus its polar passes through the pole of this line. But this pole is the common point of the polars of F and A_1 . The polar of F is the infinity line. By the lemma the polar of A_1 is line B_1C_1 . Thus the pole of our line is the infinity point of line B_1C_1 . Using the similar fact for point C' we obtain the sought assertion.

Part F.

1. Since triangle GC_1Q is isosceles and $QC_1Q''A$ is a parallelogram, we obtain that AGQ_1Q'' is an isosceles trapezoid. Similarly BGP_1P'' an isosceles trapezoid. By angles calculation we obtain that Q'' , G and P'' are collinear. Then $P''Q'' = P''G + GQ'' = AC_1 + CA_1 = AB_1 + CB_1 = AC$.
2. The tangent in F is parallel to QP and $Q''P''$, also it is antiparallel to C_1A_1 wrt angle C_1FA_1 . Thus quadrilateral is $Q''C_1A_1P''$ is cyclic. Since FG is the median of triangle FA_1C_1 , it is the symmedian of triangle $P''FQ''$. By angles calculation we obtain that FB and FG are isogonally conjugated wrt angle A_1FC_1 . Thus FB is the median. FI and FG' are the radius of the circumcircle and the altitude of triangle FC_1A_1 . Therefore they are the altitude and the line passing through the circumcenter of triangle $FQ''P''$.
3. Denote the common point of B_1T and BC as X . By Pascal theorem for points B_1, C_1, A_1, A_1, F, T line $A'X$ is parallel to A_1C_1 . Let Y, Z, Z' be the common points of B_1C_1 and BC , B_1K and BC , $A'E$ and BC respectively. We have $(X, Z, A_1, Y) = (T, K, A_1, C_1) = -1 = (A'X, A'E, A'A_1, A'C_1) = (X, Z', A_1, Y)$. Thus $Z = Z'$.
4. Let GG' and BB' secondary intersect the Feuerbach hyperbola in points X and Y respectively. $(A, C, L_B, X) = (GA, GC, GL_B, GX) = (GC_1, GB_1, GBE, GG') = -1 = (AB, CB, A'C', BB') = (A, C, L_B, Y)$. Thus $X = Y$.
5. Prove that the homothety with center M and coefficient -2 transforms F to D . In fact this homothety transforms B_0 to B , FB_0 to BB' and fixes FG' . Then it transforms F to D . Since F on the Euler circle, D lies on the circumcircle.
6. The homothety from previous item transforms the midpoint of C_0A_0 to B_0 , thus it transforms FO_B to L_BB_0 . Then L_BB_0 passes through D .
7. In part X we proved that there exists an ellipse passing through $A_0, A_1, B_0, B_1, C_0, C_1$ and F . Prove that our three lines pass through its center. Line FO_B passes through A_0C_0 and B_0C_1 , thus it is a diameter conjugated to direction AC . This yields also that the tangents to ellipse in its common points F and S with FO_B are parallel to AC . By Pascal theorem for points $B_0, C_0, C_1, A_1, A_0, B_0$ the tangent in B_0 is parallel to C_1A_1 . Thus B_0E is a diameter.

Solutions of other items may be on the official site of conference.

Дробные итерации функций.

Проект представляют

А.Канель-Белов, В.Бугаенко, С.Григорьев, Н.Кудык, И.Митрофанов, А.Петухов, Б.Френкин

Всем известно обозначение $f^{(n)}(x) = f(f(\dots x) \dots)$ (n раз). Такие функции называются *итерациями* функции f . Если f обратима, то можно определить ее *целые итерации*, положив $f^{(-n)} = (f^{(-1)})^{(n)}$. Легко убедиться в том, что $(f^{(n)})^{(m)} = f^{(nm)}$, и $f^{(n)} \circ f^{(m)} = f^{(n+m)}$.

А вот как определить *дробные итерации*? Что такое, скажем, $f^{(1/2)}(x)$? Естественно это определить как функцию g такую, что $g^{(2)} = f$. Определив *функциональные корни* $f^{(1/n)}$, затем можно естественно определить рациональные степени $f^{(m/n)} = (f^{(1/n)})^{(m)}$, и, как предельный переход, вещественные итерации. (Далее хочется понять и что такое комплексные итерации? И даже – p -адические.)

Разумеется, на этом пути есть трудности. Не все так просто даже с обратимостью. Ситуация с функциональным корнем еще хитрее.

Чтобы провести полное исследование, надо изучить для начала обычные итерации функций и функциональные корни, в том числе и с чисто теоретико-множественной точки зрения. Кроме того, следует рассмотреть частные случаи, когда задача легко берется.

1 Функциональные корни

- а) Существует ли функция g , такая что $g^{(2)}(x) = \cos x$?
б) Существует ли функция g , такая что $g^{(2)}(x) = \sin x$?
в) Те же вопросы, если потребовать непрерывность функции g .
г) Те же вопросы, если потребовать конечность числа точек разрыва функции g .
- а) Существует ли функция g , такая что $g^{(3)}(x) = e^{-x}$?
б) Тот же вопрос, если потребовать конечность числа точек разрыва функции g .
- а) Существует ли функция f , определенная на интервале $(-1, 1)$, такая что $f(f(x)) = -x$?
б) Существует ли функция $f : (-1, 1) \rightarrow (-1, 1)$, определенная на интервале $(-1, 1)$ с конечным числом точек разрыва, такая что $f(f(x)) = -x$?
в) Существует ли функция $f : [-1, 1] \rightarrow [-1, 1]$, определенная на отрезке $[-1, 1]$ с конечным числом точек разрыва, такая что $f(f(x)) = -x$?
- * Существует ли всюду определенная функция f , с конечным числом точек разрыва, такая что $f(f(x))$ есть монотонно убывающая функция?
- а) Сколько перестановок из 4 элементов являются квадратом перестановки?
б) Опишите все перестановки из 9 элементов, являющиеся кубом перестановки.

2 Дробные итерации некоторых элементарных функций

- Определите дробные итерации функции f , если
 - $f(x) = x + c$,
 - $f(x) = \alpha x$,
 - $f(x) = \alpha x + c$,
 - $f(x) = \alpha x^n$.
- $f(x) = x^2 - 2$.

3. а) $z_0 \notin \mathbb{R}$, $f(z) = z^2 - 2$. Докажите, что $|f^{(n)}(z_0)| \rightarrow \infty$ при $n \rightarrow \infty$. При каких z_0 $|f^{(n)}(z_0)| = 2$?
- б) Все корни многочлена с целыми коэффициентами и со старшим коэффициентом 1 по модулю не превосходят 1. Докажите, что они являются корнями из единицы.
- в) Все корни z_i многочлена P с целыми коэффициентами и со старшим коэффициентом 1 различны. Они принадлежат отрезку $[-1.99, +1.99]$. Докажите, что множество таких многочленов конечно.

3 Немного пределов

1. На прямоугольную карту положили карту той же местности, но меньшего масштаба. Докажите, что можно проткнуть иглой обе карты так, чтобы точка прокола изображала в обеих картах одну и ту же точку на местности.
2. Найдите предел последовательности

$$\sqrt{1}, \sqrt{1 + \sqrt{1}}, \sqrt{1 + \sqrt{1 + \sqrt{1}}}, \dots$$

3. (Задача Арнольда). Найдите предел

$$\lim_{x \rightarrow 0} \frac{\sin(\operatorname{tg}(x)) - \operatorname{tg}(\sin(x))}{\arcsin(\operatorname{arctg}(x)) - \operatorname{arctg}(\arcsin(x))}$$

4 Итерации функций. Поведение при больших n .

1. Дан $\triangle ABC$ и точка x_0 . На каждом шаге разрешается выбрать одну из вершин $\triangle ABC$, соединить точку x_n , полученную на n -ом шаге, с этой вершиной и заменить ее на точку x_{n+1} , являющуюся серединой соответствующего отрезка. Докажите, что существует фигура площади 0.0001, в которую мы рано или поздно попадем вне зависимости от выбора шага.
2. $f(x) = x^2 - 10$. Докажите, что множество точек x , таких что

$$\lim_{n \rightarrow \infty} f^{(n)}(x) \neq \infty$$

можно покрыть конечным набором интервалов суммарной длины 0.0001.

5 Локальный анализ итераций вблизи неподвижных точек и циклов.

1. Решите уравнение в вещественных числах: $f^{(n)}(x) = x$ для всех n , если $f(x) = \cos(x)$.
2. Решите уравнение в вещественных числах: $f^{(n)}(x) = x$ для всех n , если $f(x) = 1 - x^2$.
3. а) Докажите, что $\sin^{(n)}(x) \rightarrow 0$ при $n \rightarrow \infty$. б) Найдите предел $\lim_{n \rightarrow \infty} \sqrt{n} \sin^{(n)}(x_0)$.
4. Проведите исследования, аналогичные предыдущему пункту, для поведения функции $f(x) = x - ax^k$, $k > 1$ в окрестности нуля.
5. Проведите исследования, аналогичные предыдущему пункту, для поведения функции $f(x) = x - \exp(-1/x^2)$ в окрестности нуля.

6 Коммутирующие функции

Определения. $f \circ g(x) = f(g(x))$. Функции f и g коммутируют, если $f \circ g = g \circ f$. Естественно ожидать, что дробные итерации функций коммутируют между собой, и в ряде случаев, наоборот, коммутирующие функции являются дробными итерациями друг друга.

1. Найдите все дифференцируемые функции, коммутирующие с функцией $y = 2x$.
2. Существует ли недифференцируемая непрерывная функция, коммутирующая с функцией $y = 2x$?
3. Дифференцируемая функция $f(x)$ коммутирует с функцией $\frac{\sin(x)}{2}$, $f'(0) = \frac{1}{1024}$. Найдите все такие функции.
4. Существует ли недифференцируемая непрерывная функция $f : (-0.1, 0.1) \rightarrow (-0.1, 0.1)$, коммутирующая с $\frac{\sin(x)}{2}$?
5. Дифференцируемая функция $f(x) : (-0.1, 0.1) \rightarrow (-0.1, 0.1)$, коммутирует с функцией $\frac{\sin(x)}{2}$. Докажите, что f однозначно определяется значением ее производной в 0.
6. Существуют ли а) непрерывные б) дифференцируемые в*) четырежды дифференцируемые функции $f, g : (-0.1, 0.1) \rightarrow (-0.1, 0.1) \rightarrow (-0.1, 0.1)$, коммутирующие с функцией $\sin(x)$, но не коммутирующие друг с другом?
7. Функция $f : (-0.1, 0.1) \rightarrow (-0.1, 0.1)$, коммутирует с $\sin(x)$ и четырежды дифференцируема. Доказать, что $f'(0) = 1$, $f''(0) = 0$.
8. Докажите, что две четырежды дифференцируемые функции, из $(-0.1, 0.1)$ в $(-0.1, 0.1)$, коммутирующие с $\sin(x)$ с равными третьими производными в точке 0 совпадают.
9. Проведите аналогичные исследования для функции $g(x) = x - ax^k$ вместо функции $\sin(x)$.

7. Итерации и сопряжения

Функции f и g сопряжены, если $f = R \circ g \circ R^{-1}$.

Упражнение. Покажите, что тогда $f^{(n)} = R \circ g^{(n)} \circ R^{-1}$.
Здесь и далее $f \sim g$ означает, что $\frac{f(x)}{g(x)} \rightarrow 1$ при $x \rightarrow 0$.

1. а) Докажите, что функции вида $\cos(n \arccos(x))$ при $n \in \mathbb{Z}$ являются многочленами и коммутируют между собой.
б) Докажите, что функции вида $\sin((2n+1) \cdot \arcsin(x))$ при $n \in \mathbb{Z}$ являются многочленами и коммутируют между собой.
в) Докажите, что функции вида $\operatorname{tg}(n \operatorname{arctg}(x))$ при $n \in \mathbb{Z}$ являются рациональными функциями (т.е. частными двух многочленов) и коммутируют между собой.

Замечание Пункты а и б дают примеры нетривиальных семейств коммутирующих многочленов. Имеется глубокая теорема Рита, показывающая что других нетривиальных семейств нет.

2. Докажите, что функция $\sin x$ не сопряжена никакому многочлену.
3. Найдите дробные итерации функции $\frac{ax+b}{cx+d} \neq \operatorname{const}$.

Дробные итерации линейных функций нам известны. Поэтому мы хотим свести вычисление дробных итераций возможно большего числа функций к дробным итерациям функций линейных. На самом деле, мы будем искать *сопрягающее отображение* R , то есть такое отображение, что функция $R \circ f \circ R^{(-1)}$ линейна. Иногда мы будем искать сопрягающую функцию локально, т. е. в некоторой окрестности неподвижной точки.

4. Пусть $f(0) = 0$, $f'(0) = k$. Найдите $(f^{(n)})'(0)$. Пусть сопряжена гладкой функцией R функции lx . Покажите что $l = k$. Покажите, что если $|k| < 1$, то $f^{(n)} \rightarrow 0$ для всякого x в некоторой окрестности нуля. В этом случае 0 называется *притягивающей точкой* f . Если $|k| > 1$, то 0 называется *отталкивающей точкой* f .
5. а) Пусть 0 есть притягивающая точка непрерывно дифференцируемой функции f . Докажите существование предела

$$\lim_{n \rightarrow \infty} \frac{f^{(n)}(0)}{k^n} =: G(x_0)$$

для всех x_0 из некоторой окрестности 0, непрерывность функции G и что $G(k \cdot G^{(-1)}(x)) = f(x)$.

б) Докажите непрерывную дифференцируемость G .

в*) Докажите, что если f – бесконечно дифференцируема, то и G тоже бесконечно дифференцируема.

6. Докажите тождество

$$\frac{\sqrt{x}}{2} \cdot \frac{\sqrt{2+\sqrt{x}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{x}}}}{2} \dots = \frac{4-x^2}{\sqrt{2 \ln\left(\frac{x+\sqrt{x^2-4}}{2}\right)}}.$$

Определение. Точка x называется *предельной точкой* множества M если в любой ее окрестности найдется бесконечно много точек из M . *Орбитой* точки x под действием функции f называется множество $\{f^{(n)}(x)\}$, где $n \in \mathbb{Z}$.

7. Пусть f, g – бесконечно дифференцируемые коммутирующие функции при $x \neq 0$, $f(x) \sim x^\lambda, g(x) \sim x^\delta$ при $x \rightarrow 0$. Тогда $f = g^{(\log_\delta \lambda)}$.

8. Пусть x_0 и x_1 есть две «соседние» неподвижные точки коммутирующих непрерывно дифференцируемых функций f и g , т.е. для некоторой точки x точки x_0 и x_1 будут предельными для каждой из орбит $\{f^{(n)}(x)\}_{n=-\infty}^{+\infty}, \{g^{(n)}(x)\}_{n=-\infty}^{+\infty}$. Пусть x_0 – притягивающая, x_1 – отталкивающая точки для f . Докажите, что тогда

$$\log_{|g'(x_0)|} |f'(x_0)| = \log_{|g'(x_1)|} |f'(x_1)|.$$

9. Докажите, что функции в задачах 6.1, 6.3, 6.5, 6.7 являются дробными итерациями соответствующих функций.

10. Пусть f монотонно возрастающая бесконечно дифференцируемая функция, $f(0) = 0$, и $f(x) \neq x$ при $x \neq 0$. Существует ли бесконечное семейство попарно некоммутирующих бесконечно дифференцируемых функций, коммутирующих с f ?

8. Немного о многочленах

1. Пусть $P(x)$ – многочлен степени $n > 1$. Тогда для каждого m существует конечное число многочленов степени m коммутирующих с P .

2. Пусть $P(x)$ – многочлен степени $n > 1$, $Q(x)$ – многочлен степени $m > 1$, $P \circ Q = Q \circ P$, $P(x_0) = Q(x_0) = x_0$, $P'(x_0) > 1$, и в любой проколотой окрестности x_0 есть точка x_i такая что $P^{(k)}(x_i) \rightarrow \infty$ при $k \rightarrow \infty$. Докажите, что $P'(x_0)^{\log_n(m)} = Q'(x_0)$.

Замечание. Важно, что условие коммутируемости многочленов – *алгебраично*, т.е. представляет собой систему полиномиальных уравнений на коэффициенты. Поэтому значение производной в любой неподвижной или циклической точке можно считать алгебраическим числом. В предположении трансцендентности степеней вида $\alpha^{\log_n(m)}$, где α – алгебраическое число, не являющееся рациональной степенью n получаем, что тогда k есть рациональная степень n . Было бы интересно вывести из этого факта классификацию коммутирующих многочленов. Это очень важно, так как указывает на связь динамических систем с теорией трансцендентных чисел, и теорией диофантовых приближений.

Часть 1

Задача 1-1.

Доказательство. а) Положим функцию g периодичной с периодом 2π и зададим ее на отрезке $[-\pi, \pi]$. Рассмотрим отрезок $[x_1, x_0]$, $x_1 = 1$, $y_1 = \frac{\pi}{2}$ и пусть t_0 – его середина. Обозначим n -ные прообразы точек x_0, t_0 через x_n, t_n , взятые из отрезка $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Пусть $[t_0, x_0] \xrightarrow{g} [x_1, t_0]$ – действует сдвигом на t_0 . Теперь, положим $[x_1, t_0] \xrightarrow{g} [t_1, x_1]$ действует так, что $g^{(2)} \equiv \sin$ на отрезке $[t_1, x_1]$, затем аналогично для $[x_2, t_1]$ и т. д. Аналогично для отрезка $[-\frac{\pi}{2}, 0]$. Положим $g(x) = g(\pi - x)$, $\forall x \in [\frac{\pi}{2}, \pi]$ и аналогично для отрезка $[-\pi, -\frac{\pi}{2}]$. Легко видеть, что полученная таким образом функция будет искомой и, более того, непрерывной.

б) Разобьем все точки на классы, образ которых после применения функции $\cos$ совпадает. Будем задавать каждый класс представителем с отрезка $[0, \pi]$, класс содержащий точку x обозначим за $[x]$. Теперь зададим действие функции g на классах следующим образом: для класса, содержащего неподвижную точку ξ положим $g([\xi]) = \xi$, а все остальные классы разобьем на множества вида:

$$\{ \dots, [\cos^{(-1)}(\alpha)], [\alpha], [\cos(\alpha)], [\cos^{(2)}(\alpha)], \dots \}.$$

Теперь разобьем эти множества на пары и для пары, порожденной классами $[\alpha], [\beta]$, зададим следующее действие

$$g([\cos^{(n)}(\alpha)]) = \cos^{(n)}(\beta), g([\cos^{(n)}(\beta)]) = \cos^{(n+1)}(\alpha).$$

Видно, что квадрат полученной функции будет равен $\cos$.

г) Будем доказывать от противного: пусть такая функция g есть. Для начала, покажем, что в неподвижной точке ξ такая функция g не может быть непрерывной. Во-первых, эта точка будет неподвижной и для g т.к. если $\psi = g(\xi) \neq \xi$, то $\cos(\psi) = g(g(\psi)) = g(g(g(\xi))) = \psi$, противоречие. Пусть g непрерывна в точке ξ , тогда она будет монотонна в некоторой окрестности точки ξ поскольку в малой окрестности не будет точек разрыва и каждое значение должно приниматься не более одного раза поскольку это прообраз окрестности точки ξ под действием $\cos$. Но этого не может быть поскольку в таком случае её вторая итерация будет монотонно возрастать в окрестности точки ξ , что неверно. $\square$

Задачи 1-2, 1-3, 1-4. Решения этих задач содержится в статье В. Викола и А. Апостолова (mcsme.ru), см. приложение.

Задача 1-5.

Доказательство. Рассмотрим каких видов бывают перестановки.

1. Тожественная перестановка. Её квадратом будет она сама.
2. Транспозиция. Её квадратом будет тождественная.
3. Произведение двух непересекающихся транспозиций. Их квадрат – тождественная.
4. Цикл длины 3. Его квадрат будет циклом длины 3, обратным к данному.
5. Цикл длины 4. Его квадрат будет произведением непересекающихся транспозиций

Получаем всего $1 + 3 + 8$ перестановок, которые являются квадратами других перестановок.

Используя аналогичные рассуждения в случае 9 элементов мы получим, что кубом может быть любая перестановка без циклов длины 6 и с 0 или 3 циклами длины 3. $\square$

Часть 2

Задача 2-1.

Доказательство. а) Пусть $f(x) = x + c$. Тогда $f^{(\lambda)}(x) = x + \lambda c$.

б) Пусть $f(x) = \alpha x$. Тогда $f^{(\lambda)}(x) = \alpha^\lambda x$.

в) Пусть $f(x) = \alpha x + c$. Мы можем считать, что $\alpha \neq 1$ (ср. с пунктом а). Тогда

$$f(x) = \alpha \left(x - \frac{c}{1 - \alpha} \right) + \frac{c}{1 - \alpha}.$$

Откуда

$$f^{(\lambda)}(x) = \alpha^\lambda \left(x - \frac{c}{1 - \alpha} \right) + \frac{c}{1 - \alpha}.$$

г) Пусть $f(x) = ax^n$. Мы можем считать, что $a \neq 1$ (ср. с пунктом б). Отметим так же, что решение этого пункта повторяет решение пункта в и это не случайно. Тогда

$$f(x) = \sqrt[n]{c}(x/\sqrt[n]{c})^n.$$

Откуда

$$f^{(\lambda)}(x) = \sqrt[n]{c}(x/\sqrt[n]{c})^{\lambda n}.$$

□

Задача 2-2.

Доказательство. Пусть $f(x) := x^2 - 2$. Подставим вместо x в f выражение $u + \frac{1}{u}$. Получим

$$f(u + \frac{1}{u}) = u^2 + \frac{1}{u^2}.$$

Откуда

$$f^{(\lambda)}(u + \frac{1}{u}) = u^{2^\lambda} + \frac{1}{u^{2^\lambda}}.$$

Следовательно,

$$f^{(\lambda)}(x) = \left(\frac{x + \sqrt{x^2 - 1}}{2}\right)^{2^\lambda} + \left(\frac{x - \sqrt{x^2 - 1}}{2}\right)^{2^\lambda}.$$

□

Задача 2-3-а.

Доказательство. Положим $z = u + \frac{1}{u}$. Так как $z \notin \mathbb{R}$, $|u| \neq 1$. По предыдущей задаче

$$f^{(n)}(z) = f^{(n)}(u + \frac{1}{u}) = u^{2^n} + \frac{1}{u^{2^n}}.$$

Очевидно, что

$$\lim_{n \rightarrow \infty} |u^{2^n} + \frac{1}{u^{2^n}}| = +\infty.$$

□

Задача 2-3-б.

Доказательство. Пусть $f(x)$ — это многочлен степени n с целыми коэффициентами и старшим коэффициентом 1. Пусть $x_1, \dots, x_n$ — корни многочлена f . Все коэффициенты многочлена

$$f_n(x) := (x - x_1) \dots (x - x_n)$$

являются по теореме Виета симметрическими многочленами от $x_1, \dots, x_n$ с целыми коэффициентами. Следовательно, все корни многочлена f_n выражаются как целочисленные многочлены через элементарные симметрические многочлены ($:=$ коэффициенты многочлена f). Откуда все коэффициенты многочлена f_n — целы. Так как $|x_i| = 1$ для всякого i , $|x_i^k| = 1$ для всяких i и k . Откуда для всякого k все коэффициенты многочлена f не превосходят $n!$. А, следовательно, существуют различные числа k_1, k_2 такие, что $f_{k_1} = f_{k_2}$. Но тогда множества чисел

$$\{x_1^{k_1}, \dots, x_n^{k_1}\} \text{ и } \{x_1^{k_2}, \dots, x_n^{k_2}\}$$

совпадают. Откуда все числа x_i есть корни из 1 (см. также «Математическое Просвещение», 2004 год, выпуск 9). $\square$

Эта задача принадлежит М. Концевичу.

Задача 2-3-в.

Доказательство. Пусть n — степень многочлена $P(x)$, а $\{x_1, \dots, x_n\}$ — корни $P(x)$. Тогда корни многочлена

$$u^n P(u + \frac{1}{u})$$

есть решения всевозможных уравнений $u + \frac{1}{u} = x_i$. Так как $x_i \in [-1.99, 1.99]$, все решения этих уравнений комплексны и равны по модулю 1. Очевидно, многочлен $u^n P(u + \frac{1}{u})$ имеет целые коэффициенты, и, следовательно, по задаче **2-3-б** все его корни — корни из единицы. Пусть u_i — корень степени m_i из единицы, являющийся корнем многочлена $P(x)$. Тогда u_i^r — корень многочлена $u^n P(u + \frac{1}{u})$ для всякого целого r такого, что $(r, m_i) = 1$ (см. «Математическое Просвещение», 2004 год, выпуск 9).

Существует такое N , что для всякого $m > N$ и всякого примитивного корня m -ой степени из единицы u существует число r , взаимно простое с m такое, что $2\operatorname{Re} u^r > 1.99$. Откуда следует, что существует конечное множество, которому принадлежат все корни всякого многочлена $P(x)$, удовлетворяющего условию задачи. $\square$

Часть 3

Задача 3-1.

Доказательство. Пусть K – большая карта. Введём отображение $f : K \rightarrow K$, каждой точке большой карты ставящее в соответствие ту точку, на которой лежит соответственная точка маленькой карты. Задача переформулируется следующим образом: найти неподвижную точку отображения f . Очевидно, $f(K)$ – некоторый прямоугольник, лежащий в K , $f(f(K))$ – прямоугольник, лежащий в $f(K)$ и так далее. Получаем последовательность вложенных друг в друга подобных прямоугольников, большие стороны которых образуют геометрическую прогрессию со знаменателем, меньшим 1. Эти прямоугольники имеют единственную общую точку x . Предположим, что $a \neq 0$ – расстояние между x и $f(x)$. Найдётся прямоугольник $f^{(m)}(K)$ с длиной диагонали меньшей, чем a . Так как $f(x)$ лежит внутри $f(f^{(m)}(K))$, а $f^{(m+1)}(K)$ лежит внутри $f^{(m)}(K)$, то расстояние между x и $f(x)$ меньше, чем a . Противоречие. Следовательно, $x = f(x)$. $\square$

Задача 3-2.

Доказательство. Рассмотрим функцию $f(x) = \sqrt{1+x}$. Наша последовательность – это $x_n := f^{(n)}(1)$. Решая уравнение $f(x) = x$, получим, что $\frac{1+\sqrt{5}}{2}$ – единственная неподвижная точка преобразования f . При этом при $0 < x < \frac{1+\sqrt{5}}{2}$ выполнено двойное неравенство $x < f(x) < \frac{1+\sqrt{5}}{2}$. Стало быть, последовательность x_n является строго возрастающей и ограниченной, а, следовательно, имеет некий предел h . Так как функция f непрерывна, то последовательность $f(x_n)$ сходится к $f(h)$, а значит, $f(h) = h$. Таким образом, $h = \frac{1+\sqrt{5}}{2}$. $\square$

Задача 3-3.

Доказательство. Обозначим $\sin(\operatorname{tg}(x)) := f(x)$, $\operatorname{tg}(\sin(x)) := g(x)$. Требуется найти предел

$$\lim_{x \rightarrow 0} \frac{f(x) - g(x)}{g^{(-1)}(x) - f^{(-1)}(x)}.$$

Заметим, что f , g , $f^{(-1)}$ и $g^{(-1)}$ являются бесконечно дифференцируемыми функциями в окрестности нуля и все они сохраняют 0. Также заметим, что $\lim_{x \rightarrow 0} \frac{f(x)}{x} = 1$. То же самое верно для функций g , $f^{(-1)}$ и $g^{(-1)}$.

Пусть у функции $h(x) = g^{(-1)}(x) - f^{(-1)}(x)$ первые $k - 1$ производных в нуле являются нулями, а k -тая производная нулём не является. Тогда

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(x) - f^{(-1)}(x)}{x^k} = \frac{\overbrace{h'' \cdots'}^k(0)}{k!}.$$

Вместо x подставим $f(x)$. Получим

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(f(x)) - f^{(-1)}(f(x))}{(f(x))^k} = \frac{\overbrace{h'' \cdots'}^k(0)}{k!}.$$

Следовательно,

$$\lim_{x \rightarrow 0} \frac{g^{(-1)}(x) - f^{(-1)}(x)}{g^{(-1)}(f(x)) - x} = 1.$$

Из того, что $\lim_{x \rightarrow 0} f^{(-1)}(x) = 1$, следует, что

$$\lim_{x \rightarrow 0} \frac{f^{(-1)}(f(x)) - f^{(-1)}(g(x))}{f(x) - g(x)} = 1.$$

Введём обозначение $f^{(-1)}(g(x)) = s(x)$. Тогда задача сводится к нахождению предела

$$\lim_{x \rightarrow 0} \frac{x - s(x)}{s^{(-1)}(x) - x}.$$

Если $s(x)$ в окрестности нуля разлагается в ряд Тейлора как

$$x + ax^k + \dots,$$

то ряд Тейлора функции $s^{(-1)}(x)$ имеет вид

$$x - ax^k + \dots$$

Следовательно, предел отношения числителя к знаменателю равен 1. $\square$

Часть 4

Задача 4-1.

Доказательство. Введём систему координат такую, что точка A имеет координаты $(0, 0)$, точка $B - (0, 1)$, точка $C - (1, 0)$. Пусть точка X имеет координаты (a, b) . Тогда после применения "притягивания" к одной из наших точек, мы получим точку с одним из следующих наборов координат.

$$\left(\frac{a}{2}, \frac{b}{2}\right), \quad \left(\frac{a}{2} + \frac{1}{2}, \frac{b}{2}\right), \quad \left(\frac{a}{2}, \frac{b}{2} + \frac{1}{2}\right)$$

Ясно, что для любого $\varepsilon > 0$ существует n такое, что после какого-то числа операций притягивания координаты a и b станут больше $-\varepsilon$, и, следовательно, получившаяся точка будет принадлежать углу, почти совпадающему с углом $\angle CBA$. Таким образом, после какого-то числа итераций любая точка обязательно попадет в треугольник, подобный треугольнику ABC с коэффициентом $1 + \varepsilon$ и содержащий ABC . Следовательно, любая точка вне треугольника или будет к границе ближе, чем на ε , или попадёт внутрь треугольника. Без ограничения общности далее считаем, что исходная точка X лежит внутри треугольника.

После операции притягивания к A множество $X \subset \triangle ABC$ треугольника переходит в множество X_A , имеющее в 4 раза меньшую площадь. Всего таких множеств 3: X_A, X_B, X_C . Откуда видно, что площадь

$$X_A \cup X_B \cup X_C$$

небольше $3/4$ площади X . Таким образом, образ n -го шага наших итераций при действии на треугольник ABC представляют собой объединение треугольников («ковёр Серпинского»), общей площадью не больше $(3/4)^n$. Следовательно, можно выделить фигуру $\mathcal{F}$ площади 0.00000001 такую, что после какого-то числа притягиваний любая точка обязательно попадёт в $\mathcal{F}$. $\square$

Задача 4-2.

Доказательство. Обозначим через $f(x) = x^2 - 10$. Уравнение $f(x) = x$ имеет ровно два решения в вещественных числах, а именно $x_{1,2} = \frac{1 \pm \sqrt{41}}{2}$. Отметим, что x_1, x_2 - неподвижные точки отображения $x \rightarrow f(x)$. Для определённости считаем, что $x_2 > x_1$. Пусть x_2^* это корень уравнения

$f(x) = x_2$, отличный от x_2 . Пусть y_1, y_2 — это корни уравнения $f(x) = x_2^*$, причём такие, что $y_1 < y_2$. Заметим, что f монотонна на отрезках $[x_2^*, y_1]$ и $[y_2, x_2]$ и образы этих отрезков совпадают с отрезком $[x_2^*, x_2]$. Важно, что производная f на $[x_2^*, y_1]$ и $[y_2, x_2]$ неменьше 3.

Для всех $x \in [-10, x_2^*] \cup [x_2, +\infty)$ последовательность $x, f(x), f(f(x)), \dots$ стремится к бесконечности и возрастает, начиная со второго члена. Откуда множество точек, для которых предел последовательности

$$x, f(x), f(f(x)), \dots$$

не существует либо не совпадает с бесконечностью, совпадает с

$$\cap_i f^{(-i)}([x_2^*, x_2]) = \cap_i f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]).$$

Прообраз $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2])$ состоит из 2^{i+1} кусков и каждый кусок биективно отображается на какой-то кусок $f^{(-i+1)}([x_2^*, y_1] \cup [y_2, x_2])$. Так как производная f неменьше трёх на $[x_2^*, y_1] \cup [y_2, x_2]$, суммарная длина $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2])$ не больше $2/3$ суммарной длины $f^{(-i+1)}([x_2^*, y_1] \cup [y_2, x_2])$. Откуда очевидно, что $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]) < 0.0000001$ для какого-то i и, следовательно, $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]) < 0.0000001$ является искомой системой отрезков, содержащей все точки x , для которых предел последовательности $x, f(x), f(f(x)), \dots$ не существует или не равен бесконечности. $\square$

Часть 5

Задача 5-1.

Доказательство. Найдем производную функции

$$(f^{(n)}(x) - x)' = -\sin(f^{(n-1)}) \cdot (f^{(n-1)})' - 1.$$

Заметим, что продолжая раскрывать таким образом производную, мы получим, что первое слагаемое по модулю не превосходит единицы. Значит функция $f^{(n)}(x) - x$ монотонно убывает. При этом, очевидно, нулём будет решение уравнения $\cos x = x$ и это будет единственным решением исходного уравнения. $\square$

Задача 5-2.

Доказательство. Решим для начала уравнение $f(x) = x$ т.е. $1 - x^2 = x \Leftrightarrow x^2 + x - 1 = 0$ решениями которого будут $x_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$. Также, видно, что при $x < \frac{-1 - \sqrt{5}}{2}$ значения $f^{(n)}(x)$ будут убывать. Образом отрезка $[-1, 0]$ будет отрезок $[0, 1]$, значит решений уравнения на этом отрезке нет. Аналогично, можно взять его прообраз. прообраз его прообраза и т.д. и получить, что решений уравнения нет на отрезке $[\frac{-1 - \sqrt{5}}{2}, 0]$. Далее, обозначим $\frac{-1 + \sqrt{5}}{2}$ за φ и заметим, что $\forall x \in [0, \varphi] f(x) \in [\varphi, 1]$ и $\forall x \in [\varphi, 1] f(x) \in [0, \varphi]$. Значит, для нечётных итераций f корней кроме $x_{1,2}$ не будет. Рассмотрим теперь $f^{(2)}$. Она задаётся многочленом $2x^2 - x^4$ — многочленом степени 4. У $f^{(2)}(x) - x$ четыре корня, два из которых это $x_{1,2}$, а оставшиеся 2 это 0 и 1. Из этого следует, что на интервале $[0, \varphi]$ график функции $f^{(2)}$ расположен по одну сторону от прямой $y = x$ и при итерациях $f^{(2)}$, которые суть чётные итерации f , значение $f^{(2k)}(x)$ будет изменяться монотонно в пределах интервала $(0, \varphi)$, а значит решений на нём не будет. Аналогично для интервала $(\varphi, 1)$. Таким образом, будет два решения $\frac{-1 \pm \sqrt{5}}{2}$ для всех n и ещё два решения 0 и 1 для чётных n . $\square$

Задача 5-3-а.

Доказательство. Хорошо известно, что при $0 < x < \frac{\pi}{2}$ верно, что $x < \sin(x)$. Поэтому последовательность

$$x, \sin(x), \sin(\sin(x)), \dots$$

убывает при $0 < x < \frac{\pi}{2}$. Пусть $\alpha(x)$ — её предел. Тогда

$$\sin(\alpha(x)) = \sin(\lim_{n \rightarrow \infty} \sin^{(n)}(x)) = \lim_{n \rightarrow \infty} \sin^{(n+1)}(x) = \alpha(x).$$

И так как $\alpha(x) \geq 0$, отсюда вытекает, что $\alpha(x) = 0$. $\square$

Задача 5-3-б.

Доказательство. Пусть f, g — пара функций таких, что

$$\lim_{x \rightarrow 0} f(x) = \lim_{x \rightarrow 0} g(x) = 0.$$

Если $\lim_{x \rightarrow 0} \frac{g(x)}{f(x)} = 0$, мы будем позволять себе заменять функцию $g(x)$ на обозначение $o(f(x))$. Мы докажем несколько более общее утверждение, чем утверждение задачи 5-3-б.

Утверждение. Если $f(x) = x - \frac{x^3}{6} + o(x^3)$, то $\lim_{n \rightarrow \infty} \sqrt{n} f^{(n)}(x_0) = \sqrt{3}$ для всех x_0 , достаточно близких к 0. Обозначим через $SQ(x)$ функцию $\sqrt{x}$. Рассмотрим функцию:

$$\tilde{f} := SQ^{(-1)} \circ f \circ SQ.$$

Легко видеть, что $(SQ^{(-1)} \circ f \circ SQ)(x) = x + \frac{1}{3} + o(1)$.

Предложение. Пусть для некоторой функции $\tilde{f}$ верно, что

$$\tilde{f}(x) = x + \frac{1}{3} + o(1).$$

Тогда для всех x , достаточно малых по модулю, $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(x)}{n} = \frac{1}{3}$.

Доказательство. Для всякого достаточно малого по модулю x и $\varepsilon > 0$ существует N такое, что для всякого $n > N$ верно, что

$$f^{(n+1)}(x) \in [f^{(n)}(x) + \frac{1}{3} - \varepsilon, f^{(n)}(x) + \frac{1}{3} + \varepsilon].$$

Откуда для всякого $n > N$ верно, что

$$f^{(n)}(x) \in [f^{(N)}(x) + \frac{1}{3}(n - N) + (n - N)\varepsilon, f^{(N)}(x) + \frac{1}{3}(n - N) - (n - N)\varepsilon]$$

и, следовательно,

$$\frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n - N} < \frac{f^{(n)}(x)}{n - N} < \frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n - N}.$$

Откуда видно, что существует N' такое, что для всех $n > N'$ верно, что

$$\frac{1}{3} - 2\varepsilon < \frac{f^{(n)}(x)}{n} < \frac{1}{3} + 2\varepsilon.$$

Следовательно, $\lim_{n \rightarrow \infty} \frac{f^{(n)}(x)}{n} = \frac{1}{3}$. □

Пусть $x = SQ(y)$. Заметим, что

$$SQ^{(-1)}(f^{(n)}(x)) = SQ^{(-1)}(f^{(n)}(SQ(y))) = (SQ^{(-1)} \circ f \circ SQ)^{(n)}(y).$$

Напомним, что $\tilde{f} := SQ^{(-1)} \circ f \circ SQ$. По предыдущему предложению, $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(y)}{n} = \frac{1}{3}$. Откуда

$$\lim_{n \rightarrow \infty} \frac{\left(\frac{1}{f^{(n)}(x)}\right)^2}{n} = \frac{1}{3}.$$

Откуда $\lim_{n \rightarrow \infty} \sqrt{n} f^{(n)}(x) = \sqrt{3}$. □

Идея второго решения. Снова воспользуемся идеей сопряжения. Пусть $SQ = (e^{-\frac{1}{x^2}})^{(-1)}$. Тогда

$$SQ^{(-1)} \circ \sin(x) \circ SQ \sim e^{-\frac{1}{3}}x.$$

Пусть $x = SQ(y)$. Тогда

$$SQ^{(-1)}(\sin^{(n)}(SQ(y))) = SQ^{(-1)}(\sin(SQ))^{(n)}(y) = e^{-\frac{n}{3}+o(n)}y.$$

Тогда $\sqrt{n} \sin^{(n)}(x) = \sqrt{3}(1 + o(1))$. □

Задача 5-4.

Доказательство этой задачи дословно повторяет доказательство задачи 5-3-2, но мы считаем нужным его воспроизвести.

Доказательство. Мы докажем несколько более общее утверждение, чем утверждение задачи 5-3-2.

Утверждение. Если $f(x) = x - ax^k + o(x^k)$, то

$$\lim_{n \rightarrow \infty} {}^{k-1}\sqrt{n} f^{(n)}(x) = {}^{k-1}\sqrt{\frac{1}{(k-1)a}}$$

для всех x , достаточно близких к 0.

Обозначим через $SQ(x)$ функцию ${}^{k-1}\sqrt{x}$. Рассмотрим функцию:

$$\tilde{f} := SQ^{(-1)} \circ f \circ SQ.$$

Легко видеть, что $(SQ^{(-1)} \circ f \circ SQ)(x) = x + (k-1)a + o(1)$.

Предложение. Пусть для некоторой функции $\tilde{f}$ верно, что

$$\tilde{f}(x) = x + \alpha + o(1).$$

Тогда для всех x , достаточно малых по модулю, $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(x)}{n} = \alpha$.

Доказательство. Упражнение для Читателя. □

Пусть $x = SQ(y)$. Заметим, что

$$SQ^{(-1)}(f^{(n)}(x)) = SQ^{(-1)}(f^{(n)}(SQ(y))) = (SQ^{(-1)} \circ f \circ SQ)^{(n)}(y).$$

Напомним, что $\tilde{f} := SQ^{(-1)} \circ f \circ SQ$. По предыдущему предложению,
 $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(y)}{n} = (k-1)a$. Откуда

$$\lim_{n \rightarrow \infty} \frac{\left(\frac{1}{f^{(n)}(x)}\right)^{(k-1)}}{n} = \sqrt[k-1]{\frac{1}{(k-1)a}}.$$

Откуда $\lim_{n \rightarrow \infty} \sqrt[k-1]{n} f^{(n)}(x) = \sqrt[k-1]{\frac{1}{(k-1)a}}$. Для всякого достаточно малого по модулю x и $\varepsilon > 0$ существует N такое, что для всякого $n > N$ верно, что

$$f^{(n+1)}(x) \in [f^{(n)}(x) + \frac{1}{3} - \varepsilon, f^{(n)}(x) + \frac{1}{3} - \varepsilon].$$

Откуда для всякого $n > N$ верно, что

$$f^{(n)}(x) \in [f^{(N)}(x) + \frac{1}{3}(n-N) + (n-N)\varepsilon, f^{(N)}(x) + \frac{1}{3}(n-N) - (n-N)\varepsilon]$$

и, следовательно,

$$\frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n-N} < \frac{f^{(n)}(x)}{n-N} < \frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n-N}.$$

Откуда видно, что существует N' такое, что для всех $n > N'$ верно, что

$$\frac{1}{3} - 2\varepsilon < \frac{f^{(n)}(x)}{n} < \frac{1}{3} + 2\varepsilon.$$

Следовательно, $\lim_{n \rightarrow \infty} \frac{f^{(n)}(x)}{n} = \frac{1}{3}$. □

Задача 5-5.

Доказательство. Пусть $f(x) = x - \exp(-1/x^2)$, $x_n = f^{(n)}(x)$. Положим $y_n = 1/x_n$. Тогда $y_{n+1} - y_n \sim y_n \exp(y_n^{-2})$.

Заменяем разностное уравнение дифференциальным – асимптотика не меняется. Надо оценить функцию $f(n)$, удовлетворяющую уравнению

$y' = ye^{-y^2}$ или $dy/ye^{y^2} = 1$. Или $\int_1^h e^{u^2} d(u^2)/u^2 = 2h + C$. Отметим, что при больших y величина y^2 по сравнению с $\exp(y^2)$ ведет себя как константа. Поэтому с точки зрения асимптотики можно перейти к функции z такой что

$$\frac{1}{2h^2} \int_1^h du^2 e^{u^2} \sim t \text{ откуда } \frac{e^{h^2}}{2h^2} \sim n$$

Или

$$h^2 \sim \ln(n) + 2 \ln(h) \sim \ln(n) + \ln(\ln(n)) \text{ и } h \sim \sqrt{\ln(n)}.$$

Это означает, что $\lim \sqrt{\ln(n)} \cdot x_n = 1$. □

Часть 6

Задача 6-1.

Доказательство. Пусть $f(x)$ коммутирует с $y(x)$. Тогда $2f(x) = f(2x)$. Заметим, что

$$f(1) = 2f\left(\frac{1}{2}\right) = 4f\left(\frac{1}{4}\right) = \dots,$$

а значит $f(0) = 2f(0)$ и, следовательно, $f(0) = 0$. Покажем, что функция $\frac{f(x)}{x}$ постоянна. Действительно,

$$\frac{f(x)}{x} = \frac{f\left(\frac{x}{2}\right)}{\frac{x}{2}} = \frac{f\left(\frac{x}{4}\right)}{\frac{x}{4}} = \dots = f'(0)$$

для всякого x . Откуда $f(x) = f'(0)x$. □

Задача 6-2.

Доказательство. Рассмотрим произвольную непрерывную функцию $f_{2,4}$, определённую на отрезке $[2, 4]$ и равную 0 в его концах. С помощью формул

$$f(2x) = 2f(x), f(-x) = f(x), f(0) = 0$$

продолжим функцию $f_{2,4}$ на всю числовую прямую. Очевидно, что она определена и непрерывна во всех точках, включая ноль. Если функция $f_{2,4}$ недифференцируема в какой-то внутренней точке, то, очевидно, недифференцируема и f . □

По задаче **7-5** функция $\frac{\sin(x)}{2}$ сопряжена функции $\frac{x}{2}$ с помощью гладкой функции R . Таким образом, задачи **6-4** и **6-5** являются прямыми аналогами (и следствиями) задач **6-1** и **6-2**. В силу сопряжённости функций $\sin\left(\frac{x}{2}\right)$ и $\frac{x}{2}$, задача **6-3** вытекает из следующего утверждения.

Утверждение. Положим $f(x) = \frac{x}{2}$. Существует и единственная коммутирующая с f дифференцируемая функция $g(x)$ такая, что $g'(0) = \frac{1}{1024}$. Она равна

$$f^{(10)}(x) = \frac{1}{1024}x.$$

Функция $R(x) = e^{-\frac{1}{x^2}}$ сопрягает функцию $\sin(x)$ функции $\tilde{f}$ такой, что $\tilde{f}'(0) = \frac{1}{3}$. Таким образом, применяя задачу **7-5**, мы сводим задачи **6-7**,

6-8 и **6-6-в** к задаче **6-1**. К задачам **6-6-а** и **6-6-б** приводятся контрпримеры, аналогичные примеру задачи **6-2**.

Задача 6-9 совпадает с задачей **5-4**.

Часть 7

Задача 7-1.

Доказательство. Докажем верность первого и третьего утверждения по индукции.

а) База. Для $n = 1$, очевидно, верно.

Переход: $n \rightarrow n + 1$.

$$\begin{aligned} & \cos(n \cdot \arccos(x)) = \\ &= x \cos((n-1) \cdot \arccos(x)) - \sin(\arccos(x)) \sin((n-1) \arccos(x)) = \\ &= x^2 \cos((n-2) \cdot \arccos(x)) - \sin^2(\arccos(x)) \sin((n-2) \arccos(x)) - \\ & \quad 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)) = \\ &= x^2 \cos((n-2) \cdot \arccos(x)) - (1 - \cos^2(\arccos(x))) \cos((n-2) \arccos(x)) - \\ & \quad 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)). \end{aligned}$$

Заметим, что первые два слагаемых по предположению индукции являются многочленами. Рассмотрим третий член:

$$\begin{aligned} & 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)) = \\ &= 2x \cos(\arccos(x)) \cos((n-2) \arccos(x)) - 2x \cos((n-1) \arccos(x)), \end{aligned}$$

что тоже является полиномом.

б) Воспользуемся предыдущим пунктом:

$$\begin{aligned} & \sin((2n-1) \arcsin(x)) = \sin((2n-1)(\frac{\pi}{2} - \arccos(x))) = \\ &= \sin(\frac{(2n-1)\pi}{2} - (2n-1) \arccos(x)) = \pm \cos((2n-1) \arccos(x)), \end{aligned}$$

что является полиномом.

в) База опять очевидна. Переход: $n \rightarrow n + 1$.

$$\operatorname{tg}(n \operatorname{arctg}(x)) = \frac{\operatorname{tg}((n-1) \operatorname{arctg}(x)) + x}{1 - x \operatorname{tg}((n-1) \operatorname{arctg}(x))}.$$

В этой дроби и верхняя и нижняя часть по предположению индукции рациональные функции. А отношение двух рациональных функций тоже рациональная функция. $\square$

Задача 7-2.

Доказательство. Пусть утверждение не верно. Тогда существует полином P и функция R : $P = R \circ \sin \circ R^{(-1)}$. Так как $R^{(-1)}$ существует, то R является биекцией на рациональных числах. Рассмотрим множество $U := \{x : \sin(x) = 0\}$. $R^{(-1)}(U)$ (обозначим это множество за V) счётно из счётности U и биективности R . Тогда для любого $x \in V$ $P(x) = R \circ \sin \circ R^{(-1)}(x) = R(0) = \text{const}$. Значит, полином принимает какое-то значение счётное число раз. А такое невозможно. $\square$

Задача 7-3.

Доказательство. Если $c = 0$, то этот случай был разобран в предыдущих задачах. Пусть $c \neq 0$.

У нас есть функция $f = \frac{ax+b}{cx+d}$. Если мы найдем функцию R : $R \circ f \circ R^{(-1)} = g$, где g линейна, то тогда можно положить: $f^{(k)} = R^{(-1)} \circ g^{(k)} \circ R$. А дробные итерации линейных функций уже известны. Покажем, как найти R . После сопряжения функцией $R_1 = x + \frac{a}{c}$ функция f превращается в функцию $f_1 = \alpha + \frac{\beta}{x}$, где α и β - алгебраические выражения от изначальных переменных. После этого сопрягая функцию f_1 с помощью $R_2 = x\sqrt{\beta}$, получаем функцию $f_2 = s + \frac{1}{x}$. И, наконец, сопрягая функцию f_2 с помощью $R_3 = 1 + \frac{1}{x+\lambda}$, где λ - корень уравнения $\lambda(\lambda - s) - 1 = 0$, получаем линейную функцию. Итого, мы нашли R , которое равняется $R_3 \circ R_2 \circ R_1$. $\square$

Задача 7-4.

Доказательство. Заметим, что

$$(f^n)'(0) = f'(f(f(\dots)))(0) \cdot f'(f(\dots))(0) \cdots f'(0) = k^n.$$

Далее

$$\begin{aligned} (R \circ f \circ R^{(-1)})'(0) &= R'(f(R^{(-1)}(0)))f'(R^{(-1)}(0))(R(-1))'(0) = \\ &= f'(0) \cdot R'(0) \cdot (R(-1))'(0) = f'(0). \end{aligned}$$

Напомним, что $|f'(0)| = |k| < 1$. Возьмём $q : |k| < q < 1$. Из определения производной существует окрестность нуля такая, что в этой окрестности $|f(x)| < q|x|$. Следовательно, для точек из этой окрестности,

$$|f^n(x)| < q^n x,$$

и, значит, $f^{(n)}(x) \Rightarrow 0$ при $n \rightarrow \infty$. $\square$

Задача 7-5.

Доказательство. Для доказательства утверждения нам будут полезны следующие факты.

Предложение. Пусть f — дважды дифференцируемая функция такая, что $f(0) = 0$ и $f'(0) = k$, где $0 < k < 1$. Тогда

$$\exists C > 0 \exists \varepsilon > 0 \mid \forall x \in (-\varepsilon, \varepsilon) \mid f^{(n)}(x)' < Ck^n.$$

Доказательство. Пусть f, g — пара функций таких, что

$$\lim_{x \rightarrow 0} f(x) = \lim_{x \rightarrow 0} g(x) = 0.$$

Если функция $\frac{g(x)}{f(x)}$ определена и ограничена в какой-то окрестности 0, мы будем позволять себе заменять функцию $g(x)$ на обозначение $O(f(x))$.

Выпишем явно выражение для $f^{(n)}(x) =$

$$f'(x)f'(f(x))\dots f'(f^{(n-1)}(x)).$$

Так как

$$f'(f^{(m)}(x)) = k(1 + O(f^{(m)}(x))) =$$

верно, что

$$\frac{f^{(n)'}(x)}{k^n} = (1 + O(x))(1 + O(f(x)))\dots(1 + O(f^{(n-1)}(x))).$$

Так как ряд

$$x + f(x) + f(f(x)) + \dots$$

сходится абсолютно, существует константа C такая, что $f^{(n)}(x) < Ck^n$. $\square$

Для функции f и целого числа m мы будем обозначать m -ую производную через $f^{[m]}$.

Предложение. Пусть f — гладкая функция такая, что $f(0) = 0$ и $f'(0) = k$, где $-1 < k < 1$. Тогда

$$\forall m \geq 1 \exists C_m > 0 \exists \varepsilon_m > 0 \mid \forall x \in (-\varepsilon_m, \varepsilon_m) \mid f^{(n)}(x)^{[m]} < C_m k^n.$$

Доказательство. Нам будет полезна следующая лемма:

Лемма. Пусть для какого-то $m > 0$ существует такая константа C , что для всякого $r \leq m$ верно, что $f^{(n)}(x)^{[m]} \leq Ck^n$, то для всякого r такого, что $1 < r \leq m$ верно, что $(f'(f^{(n)}(x)))^{[r]} \leq C'k^n$ для какой-то константы C' .

Доказательство. При дифференцировании $f'(f^{(n)}(x))$ не более m раз в каждом слагаемом присутствует $f^{(n)}$ или производная $f^{(n)}$ порядка не более m . $\square$

Напомним, что $f^{(n)}(x)' =$

$$f'(x)f'(f(x))\dots f'(f^{(n-1)}(x)).$$

Заметим, что $f^{(n-1)}(x)^{[m]} = (f^{(n-1)}(x)^{[1]})^{[m-1]}$. Докажем наше утверждение по индукции. База - доказана предшествующим предложением. Переход $m \rightarrow m+1$. Выражение $f^{(n)}(x)'$ есть произведение n сомножителей и применение к $f^{(n)}(x)'$ производной m -раз есть сумма n^m слагаемых, причём в каждом из слагаемых затрагивается не более m сомножителей $f^{(n)}(x)'$. Рассмотрим все выражения, в которых затрагивается ровно $r \leq m$ сомножителей. В силу того, что производная затронутого сомножителя $f'(f^{(s)}(x))$ не превосходит $C'k^s$, сумма указанного набора затронутых сомножителей не превосходит

$$m!k^{n-r} \sum_{i_1, \dots, i_r \leq n} \prod_{q=1}^r (C'k^{i_q}) = m!C'^r k^{n-r} \prod_{q=1}^r (1 + \dots + k^n) \leq m!C'^r k^{n-r} \left(\frac{1}{1-k} \right)^r.$$

Очевидно, что сумма всех этих выражений по всем r не превосходит $C''k^n$ для какого-то числа $C'' > 0$. $\square$

Если для множества $\mathcal{F}$ непрерывно дифференцируемых функций существует константа C такая, что $\forall f \in \mathcal{F}$ верно, что

$$|f(x)| < C \text{ и } |f'(x)| < C$$

для всякого x , то существует сходящаяся последовательность $f_1, f_2, \dots, f_n$ попарно различных функций из $\mathcal{F}$ (см. замечательную книжку «Анализ» В. А. Зорича, в частности теорему Арцеля-Асколи). Так как m -ые производные последовательности $\frac{f^{(n)}}{k^n}$ равномерно ограничены для всякого $m \geq 1$, существует возрастающая последовательность $n_1, n_2, \dots$ такая,

что последовательность $\frac{f^{(n_1)}}{k^{n_1}}, \frac{f^{(n_2)}}{k^{n_2}}, \dots$ сходится равномерно и равномерно сходится ряд её m -ых производных для всякого $m \geq 1$. Отсюда следует, что последовательность

$$\frac{f^{(n_1)}}{k^{n_1}}, \frac{f^{(n_2)}}{k^{n_2}}, \dots$$

равномерно сходится, а, следовательно, сходится к функции G , являющейся поточечным пределом той же последовательности. Как следствие, функция G гладка. Из тождества

$$\frac{f^{(n-1)}(f(x))}{k^{n-1}} = k \frac{f^{(n)}(x)}{k^n}$$

следует, что

$$G(f(x)) = kG(x).$$

Так производная в 0 всех функций последовательности $\frac{f^{(n)}(x)}{k^n}$ равна 1, производная $G(x)$ в 0 равна 1. Следовательно, G обратима в окрестности 0 и $f(x) = G^{(-1)}(kG(x))$. $\square$

Замечание. Вместо теоремы Арцеля-Асколи можно воспользоваться следующим фактом: если последовательность функций $\{f_i\}_{i \in \mathbb{Z}_{\geq 0}}$ сходится, а их вторые производные ограничены в совокупности, то и последовательность первых производных тоже сходится.

Задача 7-6.

Доказательство. Сделаем замену $\frac{x}{2} = \cos(t)$. Тогда левая часть будет иметь вид

$$\prod_{k=1}^n \cos\left(\frac{t}{2^k}\right).$$

Домножим и разделим на $\frac{2^n}{t} \sin\left(\frac{t}{2^n}\right)$, что стремится к единице при $n \rightarrow \infty$. Получится $\frac{\cos(2t)}{t}$. После замены x на $2 \arccos t$, получаем утверждение задачи. $\square$

Данный результат может быть также получен из задачи 7-5.

Задачи 7-8 и 7-9 непосредственно следуют из задач 7-1–7-5. Из задач 7-1–7-9 вытекает решение задачи 8-2.

Задача 7-10.

Идея доказательства. Для отображения $f(x) := x - e^{-\frac{1}{x^2}} (x \geq 0)$ верно, что $f(x) < x$ для всякого $x \geq 0$. Единственной его неподвижной точкой является точка x . Точки $\{x_i\}$ задаются следующими соотношениями:

$$f(x_i) = x_{i+1}, \quad x_0 = 1.$$

Пусть $\delta(x)$ — произвольная гладкая функция на отрезке $[x_0, x_1]$, обладающая нулевыми производными в концах. Функция $f(x) + \delta(x)$ продолжается до гладкой функции на всей прямой без 0. Так как все производные функции $e^{-\frac{1}{x^2}}$ равны 0, продолженная функция будет гладкой в 0. $\square$

Часть 8

Задача 8-1.

Доказательство. Пусть $Q(x)$ — это многочлен степени m , коммутирующий с $P(x)$. Пусть $q_1, \dots, q_{m-1}$ — корни $Q'(x)$. Тогда многочлен $Q(x) - Q(q_i)$ имеет кратные корни для всякого i . Откуда следует, что многочлен

$$Q(x) - Q(P^{(r)}(q_i))$$

имеет кратные корни для всякого i и всякого целого r . Откуда следует, что множество чисел $\{Q(P^{(n)}(q_i))\}$ конечно, и не превосходит m по мощности. Откуда следует, что существует многочлен, корнями которого q_i являются для всякого многочлена $Q(x)$, удовлетворяющего условиям задачи.

Таким образом, достаточно показать, что существует только конечное число функций $Q(x)$, коммутирующих с $P(x)$ и обладающих заданным набором нулей производной с кратностями. Такие функции выражаются как $\alpha Q_0 + \beta$ для каких-то чисел α и β и заданной функции Q_0 . Коэффициент Q_0 принимает конечное число значений потому, что старшие коэффициенты многочленов

$$\alpha Q_0(P(x)) + \beta = P(\alpha Q_0(x) + \beta)$$

должны совпадать. Равенство же

$$\alpha Q_0(P(0)) + \beta = P(\alpha Q_0(0) + \beta)$$

оставляет лишь конечное число возможностей для β . $\square$

Задача 8-2 следует из задач **7-1–7-9**.

Дробные итерации функций.

10 августа 2011 г.

9. Линеаризация функции в окрестности неподвижной точки. Комплексная динамика

Для домашнего размышления

Пусть $f(0) = 0$, $f'(0) = k \neq 0$. Нас интересует, когда функцию $f(x)$ можно сопрячь с функцией $k \cdot x$ в окрестности нуля. Очень часто коммутирующие функции являются дробными итерациями друг друга.

1. Пусть f аналитична и $|k| \neq 1$. Тогда существует аналитическая G такая, что $f(x) = G(kG^{-1}(x))$. Пусть $k^n = 1$. Приведите пример аналитической функции f , не сопряженной с линейной в окрестности 0 для любого целого n .
2. Пусть k не есть корень из единицы. Тогда f сопряжена линейной как формальный степенной ряд.
3. Покажите, что при некотором k этот ряд может расходиться.
4. Докажите, что для некоторых k таких что $|k| = 1$ функция f все же всегда сопряжена линейной если она аналитична.

Функциональные корни

Влад Викал

Апостол Апостолов

Функциональное уравнение $f \circ f = g$, где g — строго убывающая, непрерывная функция, не имеет непрерывных решений, определенных на всей числовой прямой. В статье исследуется ситуация, когда допускается конечное или счетное число разрывов. В частности, показано, что если разрешить f иметь лишь конечное число разрывов, то уравнение не имеет решений на числовой прямой.

1. ВВЕДЕНИЕ

Всем хорошо знакомо обозначение $f^{(k)}(x) = \overbrace{f \circ f \circ \dots \circ f}^{k \text{ раз}}(x)$. Функция $f^{(k)}(x)$ называется k -й итерацией функции f . При этом $f^{(-1)}(x)$ обозначает обратную функцию, а $f^{(-k)}(x)$ есть $(f^{(-1)})^{(k)}(x)$. Ясно, что $(f^{(m)})^{(n)}(x) = f^{(mn)}(x)$. Естественно определить $f^{(1/2)}(x)$ как функцию g , такую что $g(g(x)) = f(x)$ (аналогично определяется $f^{(1/k)}(x)$ и далее $f^{(r/q)}(x)$). Такую функцию мы назовем *функциональным или итерационным корнем*. Функциональные корни являются важным инструментом анализа динамических систем, так как они делают возможным естественный переход от дискретного времени к непрерывному. Действительно, пусть имеется последовательность моментов времени $\dots, -1, 0, 1, \dots$ и состояние системы меняется по закону $w(t+1) = g(w(t))$. Если мы переходим к непрерывному времени, то, например, преобразование $w(t) \rightarrow w(t+1/2)$ должно определяться такой функцией f , что $f(f(x)) \equiv g(x)$.

Математические приложения функциональных корней включают также численные методы, анализ данных в хаотических системах и многое другое. Итерирование играет важную роль и при описании эволюции систем в других научных областях, как например, в экологии, эпидемиологии, оптимизации промышленных процессов, теории автоматов и теории турбулентности. Более подробно об этих вопросах см. [1–10].

Нас интересует вопрос о существовании функционального корня второй степени, т. е. о функциональном уравнении

$$f \circ f = g. \quad (1)$$

Легко видеть, что если g монотонно убывает, то уравнение (1) не имеет решений в классе непрерывных функций. В самом деле, монотонно убывающая функция принимает каждое свое значение по разу, т. е. равенство $g(x) = g(y)$ влечет

равенство $x = y$. Поскольку из $f(x) = f(y)$ следует $f(f(x)) = f(f(y))$, что равносильно $g(x) = g(y)$, приходим к выводу, что f принимает каждое свое значение ровно один раз. Вместе с непрерывностью f это влечет ее монотонность, т. е. f либо монотонно возрастает, либо монотонно убывает. В обоих случаях $f \circ f$ монотонно возрастает, что противоречит выбору g .

С другой стороны, если разрешить функции f быть разрывной, то уравнение (1) часто имеет решение, например при $g(x) = -x$. Этот случай интересен тем, что множество функций f , удовлетворяющих уравнению

$$f(f(x)) = -x, \quad (2)$$

— это в *точности* множество функций, графики которых переходят в себя при повороте на 90° относительно начала координат.

ЗАДАЧИ

1. Проверьте это свойство графиков решений уравнения (2).
2. Постройте функцию f со счетным числом точек разрыва, удовлетворяющую уравнению (2) и определенную на всей числовой прямой.
УКАЗАНИЕ. Положим $f(0) = 0$, $x_0 = 0$. Выберем последовательность x_k , $k = 1, \dots$, такую что $x_k > 0$, $x_k \rightarrow \infty$. Представим $\mathbb{R} \setminus \{0\}$ в виде объединения непересекающихся пар полуинтервалов $D_k = (x_{k-1}, x_k] \cup [-x_k, -x_{k-1})$. Пусть $y_k = \frac{x_{k-1} + x_k}{2}$. Построим кусочно-линейное решение уравнения (2) с областью определения D_k , переставляющее полуинтервалы $(x_{k-1}, y_k]$, $(y_k, x_k]$, $[-x_k, -y_k)$, $[-y_k, -x_{k-1})$.
3. Постройте решение уравнения (2) с областью определения $(-1, 1)$. А также найдите функциональные корни любой степени $f^{(2k)} = -x$ со счетным числом точек разрыва. Проверьте, что всегда $f(0) = 0$, и, кроме того, отображение f биективно.

2. ЭФФЕКТЫ ЧЕТНОСТИ

Интересные эффекты возникают, когда рассматривается решение функционального уравнения $f(f(x)) = g(x)$, где g — непрерывная монотонно убывающая функция, в классе *функций с конечным (а не счетным) числом точек разрыва*.

На 53-й Московской математической олимпиаде А. Я. Беловым была предложена следующая задача.

ЗАДАЧА. *Существует ли функция f с конечным числом точек разрыва, удовлетворяющая условию $f(f(x)) = -x$, область определения которой есть а) отрезок $[-1, 1]$; б) открытый интервал $(-1, 1)$?*

Ответы в пунктах а) и б) неожиданно оказываются разными. В пункте а) ответ «существует», в пункте б) ответ «нет»!

Напомним, что *орбитой точки x_0* называется множество

$$\text{orb}(x_0) = \{f^{(n)}(x_0) \mid n \in \mathbb{N}\}.$$

Аналогично, *орбитой множества I* является семейство множеств

$$\text{orb}(I) = \{ \{f^{(n)}(I)\} \mid n \in \mathbb{N} \}.$$

РЕШЕНИЕ ПУНКТА а). Построим функцию $f: [-1, 1] \rightarrow [-1, 1]$ с конечным числом точек разрыва, такую, что $f(f(x)) = -x$. Положим $f(0) = 0$, и пусть функция f действует по правилу $1/2 \mapsto -1 \mapsto -1/2 \mapsto 1 \mapsto 1/2$. На оставшихся открытых интервалах функция действует как изображено на рис. 1, т. е. $f((-1/2, 0)) = (-1, -1/2)$, $f((0, 1/2)) = (1/2, 1)$, $f((1/2, 1)) = (-1/2, 0)$, $f((-1, -1/2)) = (0, 1/2)$. Сравните с рис. 2, где изображена орбита точки x . $\square$

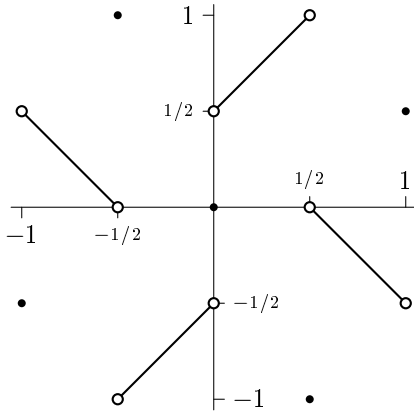


Рис. 1. График f

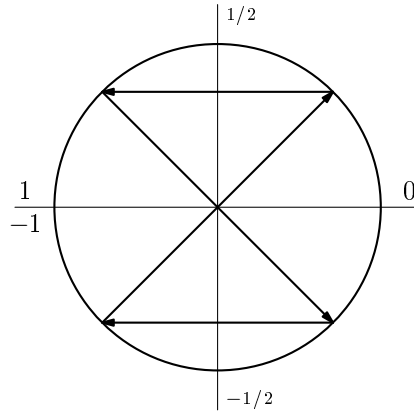


Рис. 2. Орбита x

РЕШЕНИЕ ПУНКТА б). Покажем, что не существует функции $f: (-1, 1) \rightarrow (-1, 1)$ с конечным числом точек разрыва, для которой $f(f(x)) = -x$.

Если такая функция существует, то f биективна, а 0 — единственная неподвижная точка.

В самом деле, $f(x) = f(y) \Rightarrow f(f(x)) = f(f(y)) \Rightarrow -x = -y \Rightarrow x = y$; $z = -(-z) = f(f(-z)) = f(s)$, где $s = f(-z)$; $f(x) = x \Rightarrow f(x) = f(f(x)) = -x$, откуда $x = -x$, т. е. $x = 0$.

Покажем, что орбита каждой точки, кроме нуля, содержит в точности 4 элемента.

В самом деле, $f(f(f(f(x)))) = -(-x) = x$. Если $x \neq 0$, то, как мы видели, $f(x) \neq x$, $f(f(x)) = -x \neq x$ и если $x = f(f(f(x)))$, то $f(x) = f(f(f(f(x)))) = x$, т. е. $x = 0$.

Рассмотрим множество $A = \{a_1, a_2, \dots, a_n\}$ точек разрыва функции f и положим

$$A^* := \{0\} \cup \bigcup_{a \in A} \text{orb}(a).$$

Это множество *вполне инвариантно* относительно f , т. е.

$$f(y) \in A^* \iff y \in A^*.$$

Пусть $b_1, b_2, \dots, b_m$ — элементы множества A^* , перечисленные в порядке возрастания. Поскольку орбита любой точки из A^* , кроме нуля, содержит 4 элемента, то

$$m = 4k + 1, \quad k \in \mathbb{N}. \quad (3)$$

Положим $I_1 = (-1, b_1)$, $I_{m+1} = (b_m, 1)$, и для $2 \leq j \leq m$ пусть $I_j = (b_{j-1}, b_j)$.

Применяя лемму 2, приведённую ниже, к $I = (-1, 1)$ и $M = A^*$, получаем, что f -орбита каждого интервала I_j состоит из 4 элементов. Поэтому $m + 1 = 4p$ для некоторого $p \in \mathbb{N}$. Но это противоречит уравнению (3), т. е. существованию функции f с конечным числом точек разрыва. $\square$

Здесь мы наблюдаем *комбинаторный аспект* задачи. Мы показали, что длина орбиты каждой точки, кроме неподвижной, равна 4 и потому количество интервалов полученного разбиения имеет вид $4k + 1$. Но оказывается, что и длина орбиты каждого интервала тоже равна 4, откуда получаем противоречие.

3. ОСНОВНАЯ ТЕОРЕМА

Естественно возникает более общий вопрос: *дана строго убывающая непрерывная функция g , определенная на всей числовой прямой. Может ли существовать функция f с конечным числом точек разрыва, такая что $f \circ f = g$?*

Ответ на этот вопрос дает

ОСНОВНАЯ ТЕОРЕМА. *Пусть $g: \mathbb{R} \rightarrow \mathbb{R}$ — строго монотонно убывающая непрерывная функция. Тогда не существует итерационного корня второй степени из g с конечным числом точек разрыва.*

Вначале докажем несколько вспомогательных утверждений.

ЛЕММА 1. *Пусть на некотором интервале заданы функции f и g , причем g непрерывна и взаимно однозначна. Пусть f и g коммутируют, т. е. $f \circ g = g \circ f$. Тогда непрерывность функции f в некоторой точке x_0 равносильна ее непрерывности в точке $g(x_0)$.*

ДОКАЗАТЕЛЬСТВО. Заметим, что из биективности и непрерывности функции g следует биективность и непрерывность функции $g^{(-1)}$. Поэтому достаточно доказать только одну импликацию, а потом заменить g на $g^{(-1)}$.

Пусть f непрерывна в точке x_0 . Положим $y_0 = g(x_0)$ и рассмотрим произвольную последовательность (y_n) , такую что $y_n \rightarrow y_0$. Положим $x_n = g^{(-1)}(y_n)$. Тогда $x_n \rightarrow x_0$, поскольку $g^{(-1)}$ — непрерывная функция. Так как f непрерывна в точке x_0 , то

$$f(y_n) = f(g(x_n)) = g(f(x_n)) \rightarrow g(f(x_0)) = f(g(x_0)),$$

что и требовалось. $\square$

Пусть $f \circ f = g$. В этом случае f и g коммутируют, и мы получаем

СЛЕДСТВИЕ 1. *При условии (1) орбита точки разрыва функции f под действием g состоит из точек разрыва. Если множество точек разрыва конечно, то и орбита любой из них конечна.*

СЛЕДСТВИЕ 2. Пусть $I = \bigcap_{k=0}^{\infty} g^{(k)}(\mathbb{R})$, где g — строго убывающая функция, $f^{(s)}(x) = g(x)$. Если функция f имеет конечное множество точек разрыва, то все они принадлежат I .

ДОКАЗАТЕЛЬСТВО. Любая точка вне I имеет бесконечную орбиту. Остается применить следствие 1. $\square$

ЗАДАЧА 4. Пусть g — строго убывающая непрерывная функция, $g(\mathbb{R})$ — открытый луч. Тогда для любого $s > 1$ уравнение $f^{(s)}(x) = g(x)$ не имеет решений в классе функций с конечным числом точек разрыва.

УКАЗАНИЕ. С помощью следствия 2 можно показать, что f непрерывна и убывает на $\mathbb{R} \setminus g(\mathbb{R})$. Если c — граница $g(\mathbb{R})$, то $f(c) \neq c$, иначе было бы $g(c) = c$. По непрерывности $f(c) \in g(\mathbb{R})$, откуда $f(\mathbb{R} \setminus g(\mathbb{R})) \subset g(\mathbb{R})$. В то же время $f(g(\mathbb{R})) = g(f(\mathbb{R})) \subset g(\mathbb{R})$, т. е. $f(\mathbb{R}) \subset g(\mathbb{R})$. Так как f взаимно однозначна, то $g(\mathbb{R}) \subsetneq g(\mathbb{R})$ — противоречие.

Отметим, что отсюда вытекает решение задачи К. Малькова, опубликованной в сборнике «Математическое просвещение», №3, 1999, с. 232, под номером 3.3; решение К. Малькова опубликовано в «Математическом просвещении», №5, 2001, с. 227–228.

ЛЕММА 2. Пусть $I \subseteq \mathbb{R}$ — открытый интервал, а $f: I \rightarrow I$ — биективная функция. Рассмотрим множество точек $M \subset I$, $|M| = t$, вполне инвариантное относительно f . Пусть $\{I_j\}_{j=1}^{m+1}$ — разбиение I на открытые интервалы точками множества M . Тогда:

- (i) Если f непрерывна на каждом интервале I_j , то $f(I_j) = I_k$ для некоторого $1 \leq k \leq t + 1$.
- (ii) Если, дополнительно к (i), $f \circ f$ строго убывает, то $f^{(4)}(I_j) = I_j$ для всех $1 \leq j \leq t + 1$.
- (iii) Если, дополнительно к (i) и (ii), некоторая точка x_0 принадлежит M и $f(f(x_0)) = x_0$, то орбита каждого интервала I_j имеет 4 элемента.

ДОКАЗАТЕЛЬСТВО. (i) Занумеруем интервалы разбиения слева направо и рассмотрим некоторый интервал I_j . Функция f отображает I_j на $f(I_j)$ непрерывно и биективно, поэтому $f(I_j) = (c, d)$ для некоторых $c, d \in I$. Поскольку $I_j \cap M = \emptyset$, а M вполне инвариантно относительно f , то $(c, d) \subseteq I_k$ для некоторого $1 \leq k \leq t + 1$. Используя $f^{(-1)}$ и рассуждая аналогично, получаем, что $f(I_j) = I_k$.

(ii) Так как $f^{(2)}$ строго убывает, то $f^{(4)}$ строго возрастает. Имеется ровно $j - 1$ интервалов слева от I_j . Применяя утверждение (i) к $f^{(4)}$, получаем, что существует ровно $j - 1$ интервалов слева от $f^{(4)}(I_j)$. Следовательно, $f^{(4)}(I_j) = I_j$.

(iii) Из (ii) следует, что орбита каждого интервала I_j состоит из 1, 2 или 4 элементов. Предположим, что $f(f(I_j)) = I_j$. Так как функция $f \circ f$ строго

убывает и непрерывна на I_j , то по теореме о промежуточном значении существует $x \in I_j$, для которого $f(f(x)) = x$. Но строго убывающая функция может иметь лишь одну неподвижную точку. Значит, $x = x_0 \in M$, — противоречие. Следовательно, орбита каждого интервала имеет длину 4. $\square$

ЛЕММА 3. Пусть g — строго убывающая непрерывная функция и выполнено уравнение $f \circ f = g$. Тогда функции f и g имеют единственную неподвижную точку, причем общую.

ДОКАЗАТЕЛЬСТВО. Очевидно, что строго убывающая функция может иметь лишь одну неподвижную точку. Если при этом функция непрерывна, то по теореме о промежуточном значении такая точка x_0 существует. Тогда $f(x_0) = f(g(x_0)) = g(f(x_0))$, т.е. $f(x_0)$ также является неподвижной точкой функции g . Значит, $f(x_0) = x_0$. Обратно, если $f(x) = x$, то $g(x) = f(f(x)) = x$, откуда $x = x_0$. $\square$

ЛЕММА 4. Пусть $I \subset \mathbb{R}$ — открытый интервал, а $f, g: I \rightarrow I$ таковы, что $f \circ f = g$, причем g непрерывна и биективна, а f имеет конечное число точек разрыва. Тогда каждая из этих точек либо является неподвижной точкой функции g , либо имеет f -орбиту из 4 элементов.

ДОКАЗАТЕЛЬСТВО. Пусть A — множество точек разрыва функции f . Поскольку g и f коммутируют, то по следствию 1 леммы 1 $g(A) \subseteq A$. Так как A конечно, а функция g инъективна, то $g(A) = A$. Пусть $a \in A$ и $g(a) \neq a$. Поскольку $g \circ g$ строго возрастает и $g(g(A)) = A$, то $g(g(a)) = a$, т.е. $f^{(4)}(a) = a$. Так как $g(a) \neq a$, то $f(a) \neq a$ и $f^{(3)}(a) = f^{(-1)}(a) \neq a$, т.е. a имеет орбиту из 4 точек. $\square$

ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ. Допустим, что существует функция f , обладающая свойствами из условия теоремы. Очевидно, $g^{(n+1)}(\mathbb{R}) \subseteq g^{(n)}(\mathbb{R})$ для всех $n \in \mathbb{N}$. Поскольку g непрерывна и строго монотонна, то $g^{(k)}(\mathbb{R})$ — открытый интервал в $\mathbb{R}$. Положим

$$I = \bigcap_{k=0}^{\infty} g^{(k)}(\mathbb{R}).$$

Поскольку g непрерывна и строго убывает, то уравнение $g(x) = x$ имеет ровно одно решение x_0 . Тогда $g^{(k)}(x_0) = x_0$ для всех $k \in \mathbb{N}$, откуда $x_0 \in I$, т.е. $I \neq \emptyset$.

Поскольку I — счетное пересечение открытых интервалов, то I связно. При этом $g(I) = I$. Легко видеть, что I не может быть полуинтервалом в силу монотонности g . Предположим, что $I = [a, b]$ для некоторых $a < b$. Так как g строго убывает, то $g(a) = b$, $g(b) = a$. Но концы промежутка не влияют на наши рассуждения, так что можно считать I открытым интервалом.

Пусть множество A_{ext} состоит из всех точек разрыва функции f и точки x_0 . Из следствия 2 леммы 1 вытекает, что $A_{\text{ext}} \subset I$. Применив леммы 3 и 4 к $f, g: I \rightarrow I$, получаем, что множество A_{ext} состоит из $4p + 1$ элементов для некоторого $p \in \mathbb{N}$. Соответствующее разбиение интервала I должно состоять из $4p + 2$ открытых интервалов. Применив к I лемму 2(iii) с $M = A_{\text{ext}}$, получаем,

что орбита каждого интервала I_j состоит из четырех элементов и потому число интервалов должно делиться на 4, тогда как оно имеет вид $4p+2$. Таким образом, предположение о существовании функции f ведет к противоречию. $\square$

4. ПОПЫТКА ДАЛЬНЕЙШЕГО ОБОБЩЕНИЯ

Естественно попытаться обобщить основную теорему. А что если функция $g: \mathbb{R} \rightarrow \mathbb{R}$ монотонно убывает, но не обязательно непрерывна? Ясно, что если g имеет бесконечное число точек разрыва, то функциональный корень f , для которого $f \circ f = g$, тоже имеет бесконечное число точек разрыва. Поэтому потребуем, чтобы *функция g имела конечное число точек разрыва*.

Оказывается, в этом случае уравнение (1) может иметь решения, определенные на всей числовой прямой.

ПРЕДЛОЖЕНИЕ 1. *Существует открытый интервал $I \subset \mathbb{R}$ и функции $f, g: I \rightarrow I$ с конечным числом точек разрыва, такие что g строго убывает и $f(f(x)) = g(x)$ для всех $x \in I$.*

ДОКАЗАТЕЛЬСТВО. Здесь мы начинаем не с выбора функции g с последующим построением f , а с построения самой функции f . Для облегчения вычислений рассмотрим $I = (-16, 16)$, вместо $(-1, 1)$.

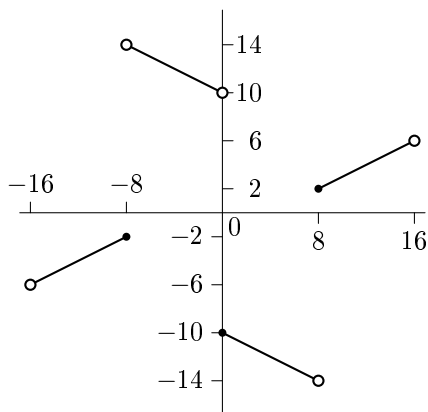
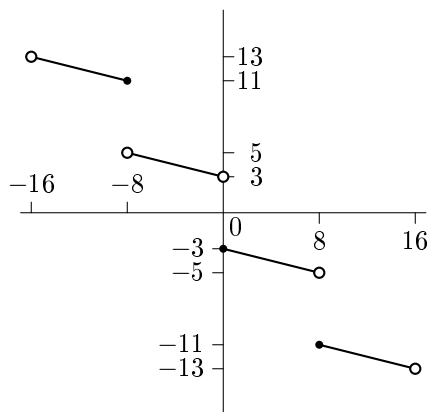
$$\text{Пусть } f: (-16, 16) \rightarrow \mathbb{R}, \quad f(x) = \begin{cases} \frac{x}{2} + 2 & \text{при } x \in (-16, -8), \\ -\frac{x}{2} + 10 & \text{при } x \in (-8, 0), \\ -\frac{x}{2} - 10 & \text{при } x \in (0, 8), \\ \frac{x}{2} - 2 & \text{при } x \in (8, 16), \\ -2 & \text{при } x = -8, \\ -10 & \text{при } x = 0, \\ 2 & \text{при } x = 8. \end{cases}$$

Легко проверить, что f имеет 3 точки разрыва и что $g := f \circ f$ строго убывает и тоже имеет 3 точки разрыва. Чтобы лучше увидеть получившуюся картину, см. рис. 3 и рис. 4. $\square$

ЗАМЕЧАНИЕ 1. Отметим, что график функции f симметричен (за исключением одной точки) относительно поворота плоскости на 180° (см. также рис. 1).

Благодарности

Мы хотим поблагодарить Алексея Белова и Гётца Пфандера, которые познакомили нас с функциональным уравнением $f \circ f = -\text{id}$, а также Александра Буфетова за полезные замечания и Бориса Френкина за редакционную правку.

Рис. 3. График f Рис. 4. График g

Мы особенно благодарны Алексею Белову, который поддержал наши попытки обобщить это функциональное уравнение.

СПИСОК ЛИТЕРАТУРЫ

- [1] Block L., Guckenheimer J., Misiurewicz M., Young L.-S. *Periodic points of one-dimensional maps* // Springer Lecture Notes in Mathematics, vol. 819. Springer Verlag, Berlin, 1980. P. 18–34.
- [2] Katok A., Hasselblatt B. *Introduction to the Modern Theory of Dynamical Systems*. Cambridge University Press, 1995.
- [3] Kuczma M., Choczewski B., Ger R. *Iterative Functional Equations*. Cambridge University Press, 1990.
- [4] Misiurewicz M., Nitecki Z. *Combinatorial Patterns for Maps of the Interval* // Mem. Amer. Math. Soc., 1990. Vol. 456.
- [5] Misiurewicz M. *Formalism for studying periodic orbits of one dimensional maps* // European Conference on Iteration Theory (ECIT 87), World Scientific, Singapore, 1989. P. 1–7.
- [6] Stefan P. *A Theorem of Sharkovski on the Existence of Periodic Orbits of Continuous Endomorphism of the Real Line* // Commun. math. Phys., 1977. Vol. 54. P. 237–248.
- [7] Targonski G. *Topics in Iteration Theory*. Vandenhoeck and Ruprecht, Göttingen, 1981.
- [8] Targonski G. *Progress of iteration theory since 1981* // Aequationes Math., 1995. Vol. 50. P. 50–72.

- [9] Шарковский А. Н. *Существование циклов непрерывного преобразования прямой в себя* // Укр. матем. ж., 1964. Т. 16, №1. С. 61–71.
- [10] *Одномерная динамика и теорема Шарковского* // X летняя конференция турнира городов. М.: МЦНМО, 1999. С. 21–25, 79–91.

Влад Викал, Международный Университет Бремен;
28759 Bremen, Germany;
e-mail: v.vicol@iu-bremen.de

Апостол Апостолов, Международный Университет Бремен;
28759 Bremen, Germany;
e-mail: a.apostolov@iu-bremen.de

Fractional iterations of functions.

A.Kanel-Belov, V.Bugaenko, S.Grigorjev, N.Kudyk, I.Mitrofanov, A.Petuhov, B.Frenkin

We denote $f^{(n)}(x) = f(f(\dots x) \dots)$ (n times). Functions $f^{(n)}$ are *iterations* of f . If f is invertible, then *integer iterations* exist and $f^{(-n)} = (f^{(-1)})^{(n)}$. It is easy to see that $(f^{(n)})^{(m)} = f^{(nm)}$ and $f^{(n)} \circ f^{(m)} = f^{(n+m)}$.

How to define *fractional iterations*? What does it mean: *functional root* $g(x) = f^{(1/2)}(x)$? It is natural to assume that $g^{(2)} = f$. After defining *functional roots* $f^{(1/n)}$ one can define rational powers $f^{(m/n)} = (f^{(1/n)})^{(m)}$ and try to define real iterations via limit. (By the way, it is interesting what is the sense of complex or p -adic iterations.)

This way meets some difficulties. Invertibility of functions already is not always clear. We shall start from investigation of usual iterations and functional roots from set-theoretic point of view and from some important partial cases.

1 Functional roots

1. a) Does there exist a function g such that $g^{(2)}(x) = \cos x$?
b) Does there exist a function g such that $g^{(2)}(x) = \sin x$?
c) The same questions for continuous function g .
d) The same questions for function g with finitely many discontinuity points.
2. a) Does there exist a function g such that $g^{(3)}(x) = e^{-x}$?
b) The same question for a function g with finitely many discontinuity points.
3. a) Does there exist a function $f : (-1, 1) \rightarrow (-1, 1)$ such that $f(f(x)) = -x$?
b) The same question for function f with finitely many discontinuity points.
c) Does there exist a function $f : [-1, 1] \rightarrow [-1, 1]$ with finitely many discontinuity points such that $f(f(x)) = -x$?
4. * Does there exist a function $f : \mathbb{R} \rightarrow \mathbb{R}$ with finitely many discontinuity points such that $f(f(x)) = g$ for some strictly decreasing function g ?
5. a) How many permutations on 4-element set are squares?
b) Describe all permutations on 9-element set which are cubes.

2 Fractional iterations of some elementary functions

1. a) Let $f(x) = x + c$. What are fractional iterations of f ? b) Let $f(x) = \alpha x$. What are fractional iterations of f ?
c) Let $f(x) = \alpha x + c$. What are fractional iterations of f ?
d) Let $f(x) = \alpha x^n$. What are fractional iterations of f ?
2. Let $f(x) = x^2 - 2$. What are fractional iterations of f ?
3. a) $z_0 \notin \mathbb{R}$, $f(z) = z^2 - 2$. Prove that $|f^{(n)}(z_0)| \rightarrow \infty$ if $n \rightarrow \infty$. Find the set of initial points z_0 such that $|f^{(n)}(z_0)| = 2$.
b) Let P be a polynomial with integer coefficients with oldest coefficient equal 1. Let all complex roots P are in the unit disc $|z| \leq 1$. Prove that they are roots of unit.
c) Let P be a polynomial with integer coefficients with oldest coefficient equal 1. Let all complex roots P are distinct and in the line segment $[-1.99, +1.99]$. Prove that the set of such polynomials is finite.

3 Some limits

1. On the rectangular map M somebody put a map N of same landscape but smaller massstab. Prove that one can touch them with spike such that booth spiked places maps same point on the landscape.
2. Find limit of the sequence

$$\sqrt{1}, \sqrt{1 + \sqrt{1}}, \sqrt{1 + \sqrt{1 + \sqrt{1}}}, \dots$$

3. (Arnolds problem). Find the limit

$$\lim_{x \rightarrow 0} \frac{\sin(\operatorname{tg}(x)) - \operatorname{tg}(\sin(x))}{\arcsin(\operatorname{arctg}(x)) - \operatorname{arctg}(\arcsin(x))}$$

4 Iterations. Big n behavior.

1. A $\triangle ABC$ and point x_0 are given. On n -th step one choose one of the vertices of the $\triangle ABC$ join x_n with this vertex and replace point x_n to the point x_{n+1} which is midpoint of this line segment. Prove that there exist a figure S of arrear 0.0001 attracting all the points x_n for all sufficiently large n for all such processes.
2. $f(x) = x^2 - 10$. Prove that the set of all points x such that

$$\lim_{n \rightarrow \infty} f^{(n)}(x) \neq \infty$$

can be coved by finite set of intervals of total length 0.0001.

5 Iterations near stability points and circles.

1. Solve equations for each n in real numbers $f^{(n)}(x) = x$ if $f(x) = \cos(x)$.
2. Solve equations for each n in real numbers $f^{(n)}(x) = x$ if $f(x) = 1 - x^2$.
3.) Prove that $\sin^{(n)}(x) \rightarrow 0$ for $n \rightarrow \infty$.) Find $\lim_{n \rightarrow \infty} \sqrt{n} \sin^{(n)}(x_0)$.
4. Generalize previous problem for $f(x) = x - ax^k, k > 1$.
5. Generalize previous problem for $f(x) = x - \exp(-1/x^2)$.

7. Conjugacy and iterations

Functions f and g are called *conjugated* whenever $f = R \circ g \circ R^{-1}$ for some function R .

Exercise. Show that in this case $f^{(n)} = R \circ g^{(n)} \circ R^{-1}$.

We use notation $f \sim g$ whenever $\frac{f(x)}{g(x)} \xrightarrow{x \rightarrow 0} 1$.

1. a) Show that for any $n \in \mathbb{Z}$ the function $\cos(n \arccos(x))$ is a polynomial, and that any two functions of this kind commute one with each other.
 b) Show that for any $n \in \mathbb{Z}$ the function $\sin((2n + 1) \cdot \arcsin(x))$ is a polynomial, and that any two functions of this kind commute one with each other.
 c) Show that for any $n \in \mathbb{Z}$ the function $\tan(n \arctan(x))$ is *rational*, i.e. is a quotient of two polynomials. Show that any two functions of this kind commute one with each other.

Remark. Parts a and b provides nontrivial examples of commuting families of polynomials. By the deep theorem of Reed any other nontrivial family of commuting polynomials essentially coincides with a or b.

2. Show that the function $\sin x$ is not conjugated to a polynomial.
3. Find fractional iterations of functions $\frac{ax+b}{cx+d}$ for any a, b, c, d .

Hence we can explicitly describe fractional iterations of linear functions, we wish to connect them with as many fractional iterations of other functions as possible. Essentially we wish to find a big enough class of functions f for which exists a *conjugating function* R such that

$$R \circ f \circ R^{(-1)}$$

is a linear function. From time to time it is reasonable to find such conjugating function in some neighborhood of some point.

4. Let f be a function such that $f(0) = 0, f'(0) = k$. Evaluate $(f^{(n)})'(0)$. Assume that f is conjugated to lx for some number l with some smooth (i.e. infinitely differentiable) conjugating function R . Prove that in this case $k = l$. If $|k| < 1$ then $f^{(n)}(x) \xrightarrow{n \rightarrow \infty} 0$ in for all x from some neighborhood of 0. In this case we call 0 an *attracting* point of f . If $|k| > 1$ we call 0 a *repelling* point of f .

5. a) Let 0 be an attracting point of a continuously differentiable function f . Prove that for all x_0 from some neighborhood of 0 the limit

$$\lim_{n \rightarrow \infty} \frac{f^{(n)}(0)}{k^n} = G(x_0)$$

exists. Prove that G is continuous and that $G(k \cdot G^{(-1)}(x)) = f(x)$.

b) Prove that G is continuously differentiable.

c*) Prove that if f smooth then G is smooth.

6. Prove the following equality.

$$\frac{\sqrt{x}}{2} \cdot \frac{\sqrt{2+\sqrt{x}}}{2} \cdot \frac{\sqrt{2+\sqrt{2+\sqrt{x}}}}{2} \dots = \frac{4-x^2}{\sqrt{2 \ln\left(\frac{x+\sqrt{x^2-4}}{2}\right)}}.$$

Definition. Let $M \subset \mathbb{R}$ be a set. We call $x \in M$ a *limit point* of M if any neighborhood of x contains infinitely many points of M . We call the set $\{f^{(n)}(x)\}_{n \in \mathbb{Z}_{\geq 0}}$ an *orbit* of x under the action of f .

7. Let f, g be a pair of commuting smooth functions such that $f(0) = g(0) = 0$ and $f(x) \sim x^\lambda, g(x) \sim x^\delta$. Then $f = g^{(\log_\delta \lambda)}$ (Here you have to define fractional iterations in a spirit of the introduction).
8. We call two points x_0, x_1 of an invertible function f *neighbor* if there exists a point x such that $\lim_{n \rightarrow -\infty} f^{(n)}(x) = x_0$ and $\lim_{n \rightarrow +\infty} f^{(n)}(x) = x_1$.

Let x_0 and x_1 be common neighbor fixed points of commuting invertible continuously differentiable functions f and g . Assume x_0 is attracting and x_1 is repelling for both f and g . Prove that in this case

$$\log_{|g'(x_0)|} |f'(x_0)| = \log_{|g'(x_1)|} |f'(x_1)|.$$

9. Prove that functions of problems 6.1, 6.3, 6.5, 6.7 are fractional iterations of the corresponding functions.
10. Let f be a decreasing function such that $f(0) = 0$ and $f(x) \neq x$ for all $x \neq 0$. Does there exist an infinite family $\mathfrak{F}$ of pairwise noncommuting functions such that any element of $\mathfrak{F}$ commutes with f ?

8. More about polynoms

1. Let $P(x)$ be a polynom of degree $n > 1$. Then for all m the set of polynoms of degree m such that they commute with f is finite.
2. Let $P(x)$ be a polynom of degree $n > 1$, $Q(x)$ be a polynom of degree $m > 1$ such that
 - a) $P \circ Q = Q \circ P$, b) $P(x_0) = Q(x_0) = x_0$, c) $P'(x_0) > 1$, d) in any punctured neighborhood of x_0 there exists a point x_i such that $P^{(k)}(x_i) \xrightarrow{k \rightarrow \infty} \infty$.
 Prove that $P'(x_0)^{\log_n(m)} = Q'(x_0)$.

Remark. We note that the condition "to be commutative" is *algebraic*, i.e. is equivalent to a system of polynomial equations on coefficients. Therefore we could assume that the value of derivatives in all fixed point are algebraic. In assumption of transcendency of powers $\alpha^{\log_n(m)}$, where α is some algebraic number and n is not a rational power of α , we have that k is a rational power of n . It is interesting to derive the classification of commuting polynoms from this observation. This problem is really valuable because it provides a connection between dynamical systems, theory of transcendence numbers and theory of Diofant approximations.

Part 1

Problem 1-1.

Proof. a) Let a function g be determined on $[-\pi, \pi]$ and periodical with period 2π . Consider the segment $[x_1, x_0]$, $x_1 = 1$, $y_1 = \frac{\pi}{2}$ and let t_0 be its midpoint. Denote by x_n, t_n the n -th preimages of x_0, t_0 taken in $[-\frac{\pi}{2}, \frac{\pi}{2}]$. Suppose $[t_0, x_0] \xrightarrow{g} [x_1, t_0]$ acts on t_0 as a translation. Now let $[x_1, t_0] \xrightarrow{g} [t_1, x_1]$ act so that $g^{(2)} \equiv \sin$ on $[t_1, x_1]$, similarly for $[x_2, t_1]$ and so on. Similarly for $[-\frac{\pi}{2}, 0]$. Let $g(x) = g(\pi - x)$, $\forall x \in [\frac{\pi}{2}, \pi]$ and similarly for $[-\pi, -\frac{\pi}{2}]$. It is easily seen that the resulting function satisfies the conditions of Problem 1-1 and moreover is continuous.

b) Divide all points into classes such that their images under $\cos$ are the same. Each class will be represented by a point of $[0, \pi]$. The class containing a point x will be denoted by $[x]$. Now determine the action of the function g on the classes as follows. For the class containing a fixed point x_0 let $g([x_0]) = x_0$. Divide the remaining classes into sets of the form

$$\{\dots, [\cos^{(-1)}(\alpha)], [\alpha], [\cos(\alpha)], [\cos^{(2)}(\alpha)], \dots\}.$$

The divide these sets into pairs, and for the pair generated by classes $[\alpha], [\beta]$ determine the following action: $g([\cos^{(n)}(\alpha)]) = g([\cos^{(n)}(\beta)])$, $g([\cos^{(n)}(\beta)]) = g([\cos^{(n+1)}(\alpha)])$. Clearly the square of the resulting function is $\cos$. $\square$

Solutions of **problems 1-2, 1-3, 1-4** are contained in a paper of V. Vikola and A. Apostolov, see "Matematicheskoe prosveschenie", year 2004, vol. 9.

Problem 1-5.

Proof. Let us consider what are possible forms of the substitutions.

1. The identical substitution. It is its own square.
2. A transposition. Its square is the identical substitution.
3. A product of two disjoint transpositions. Its square is the identical substitution.
4. A cycle of length 3. Its square is the cycle of length 3 inverse to the original one.
5. A cycle of length 4. Its square is a product of disjoint substitutions.

In total, we get $1 + 3 + 8$ substitutions which are squares of substitutions. In the case of 9 elements, a similar argument implies that the cubes are any substitutions without cycles of length 6 and with 0 or 3 cycles of length 3. $\square$

Part 2

Problem 2-1.

Proof. a) Let $f(x) = x + c$. Then $f^{(\lambda)}(x) = x + \lambda c$.

b) Let $f(x) = \alpha x$. Then $f^{(\lambda)}(x) = \alpha^\lambda x$.

c) Let $f(x) = \alpha x + c$. We assume that $\alpha \neq 1$ (cf. a). Then

$$f(x) = \alpha \left(x - \frac{c}{1 - \alpha} \right) + \frac{c}{1 - \alpha}.$$

Therefore

$$f^{(\lambda)}(x) = \alpha^\lambda \left(x - \frac{c}{1 - \alpha} \right) + \frac{c}{1 - \alpha}.$$

d) Let $f(x) = ax^n$. We assume that $a \neq 1$ (cf. b). The solution of this problem is similar to part c and this is not an occasion.

$$f(x) = \sqrt[n]{c}(x/\sqrt[n]{c})^n.$$

$$f^{(\lambda)}(x) = \sqrt[n]{c}(x/\sqrt[n]{c})^{\lambda n}.$$

$\square$

Problem 2-2.

Proof. Let $f(x) := x^2 - 2$. We substitute x in f by $u + \frac{1}{u}$. We have

$$f(u + \frac{1}{u}) = u^2 + \frac{1}{u^2}.$$

Further

$$f^{(\lambda)}(u + \frac{1}{u}) = u^{2^\lambda} + \frac{1}{u^{2^\lambda}}.$$

Then

$$f^{(\lambda)}(x) = \left(\frac{x + \sqrt{x^2 - 1}}{2} \right)^{2^\lambda} + \left(\frac{x - \sqrt{x^2 - 1}}{2} \right)^{2^\lambda}.$$

$\square$

Problem 2-3-a.

Proof. Set $z = u + \frac{1}{u}$. As $z \notin \mathbb{R}$, $|u| \neq 1$. By the previous theorem

$$f^{(n)}(z) = f^{(n)}\left(u + \frac{1}{u}\right) = u^{2^n} + \frac{1}{u^{2^n}}.$$

We have

$$\lim_{n \rightarrow \infty} \left| u^{2^n} + \frac{1}{u^{2^n}} \right| = +\infty.$$

□

Problem 2-3-b.

Proof. Let $f(x)$ be a polynomial of degree n with the highest coefficient 1. Let $x_1, \dots, x_n$ be roots of f . The coefficients

$$f_n(x) := (x - x_1) \dots (x - x_n)$$

are symmetric polynomials of $x_1, \dots, x_n$ with integer coefficients. Therefore all coefficients of f_n are polynomials of the elementary symmetric polynomials (:=coefficients of f). Therefore all coefficients of f_n are integers. As $|x_i| = 1$ for all i , $|x_i^k| = 1$ for all i and k . Therefore for any k the coefficients of f is smaller or equal to $n!$. Hence there exist different numbers k_1, k_2 such that $f_{k_1} = f_{k_2}$. But then the set of numbers

$$\{x_1^{k_1}, \dots, x_n^{k_1}\} \text{ and } \{x_1^{k_2}, \dots, x_n^{k_2}\}$$

coincide. Therefore x_i -th are roots of unity (see also "Matematicheskoe Prosveschenie", year 2004, vol. 9). □

This problem was invented by M. Kontsevich.

Problem 2-3-c.

Proof. Let n be a degree of $P(x)$ and $\{x_1, \dots, x_n\}$ be roots of $P(x)$. Then the roots of

$$u^n P\left(u + \frac{1}{u}\right)$$

are solutions of equality $u + \frac{1}{u} = x_i$. As $x_i \in [-1.99, 1.99]$, all roots are purely complex and has length 1. Therefore polynomial $u^n P(u + \frac{1}{u})$ has integer coefficients, and all roots of this polynomial are roots of unity by Problem **2-3-b**. Let u_i be root of unity of degree m_i , such that u_i is a root of $P(x)$. Then u_i^r

is a root of polynomial $u^n P(u + \frac{1}{u})$ for any integer r such that $(r, m_i) = 1$ (see also [1], year 2004, vol. 9).

There exists N such that $m > N$ and for any primitive root of unity u of degree m there exists number r , such that $(m, r) = 1$ and $2\operatorname{Re} u^r > 1.99$. Therefore there exists a finite set $\mathcal{S}$ such that any root of a polynomial $P(x)$, which satisfies the conditions of the problem, lies in $\mathcal{S}$. $\square$

Part 3

Problem 3-1.

Proof. Let K be a big map. Introduce the map $f : K \rightarrow K$ that maps each point of the big map to its point lying under the corresponding point of the small map. Then the problem reformulates as follows: find a fixed point for f . Clearly $f(K)$ is a rectangle in K , $f(f(K))$ is a rectangle in $f(K)$ and so on. We obtain a sequence of similar rectangles embedded into each other, such that their greater sides form a geometrical progression whose denominator is less than 1. These rectangles have a single common point x . Suppose $a \neq 0$ is the distance between x and $f(x)$. There exists a rectangle $f^{(m)}(K)$ whose diagonal has length less than a . Since $f(x)$ lies inside $f(f^{(m)}(K))$ and $f^{(m+1)}(K)$ lies inside $f^{(m)}(K)$, the distance between x and $f(x)$ is less than a , a contradiction. Thus $x = f(x)$. $\square$

Problem 3-2.

Proof. Consider the function $f(x) = \sqrt{1+x}$. Our sequence has the form $x_n := f^{(n)}(1)$. Solving the equation $f(x) = x$ we see that $\frac{1+\sqrt{5}}{2}$ is a single fixed point of f . Furthermore for $0 < x < \frac{1+\sqrt{5}}{2}$ we have the double inequality $x < f(x) < \frac{1+\sqrt{5}}{2}$. Hence the sequence x_n is strictly increasing and bounded and hence has some limit h . Since f is continuous, the sequence $f(x_n)$ tends to $f(h)$, whence $f(h) = h$. Thus $h = \frac{1+\sqrt{5}}{2}$. $\square$

Problem 3-3.

Proof. Denote $f(x) := \sin(tg(x))$, $g(x) := tg(\sin(x))$. We have to find the limit

$$\lim_{x \rightarrow 0} \frac{f(x) - g(x)}{g^{-1}(x) - f^{-1}(x)}.$$

Observe that f , g , f^{-1} and g^{-1} are infinitely differentiable in some neighborhood of zero and fix 0. Now observe that $\lim_{x \rightarrow 0} \frac{f(x)}{x} = 1$. The same is true for g , f^{-1} and g^{-1} .

Suppose that for $h(x) = g^{-1}(x) - f^{-1}(x)$ first $k - 1$ derivatives are zeroes at zero and the k th derivative is not. Then

$$\lim_{x \rightarrow 0} \frac{g^{-1}(x) - f^{-1}(x)}{x^k} = \frac{\overbrace{h'' \cdots'}^{k \text{ times}}(0)}{k!}.$$

Substitute $f(x)$ for x . We get

$$\lim_{x \rightarrow 0} \frac{g^{-1}(f(x)) - f^{-1}(f(x))}{(f(x))^k} = \frac{\overbrace{h'' \cdots'}^{k \text{ times}}(0)}{k!}.$$

Hence

$$\lim_{x \rightarrow 0} \frac{g^{-1}(x) - f^{-1}(x)}{g^{-1}(f(x)) - x} = 1.$$

From $\lim_{x \rightarrow 0} f^{-1}(x) = 1$ we get

$$\lim_{x \rightarrow 0} \frac{f^{-1}(f(x)) - f^{-1}(g(x))}{f(x) - g(x)} = 1.$$

Let $s(x) := f^{-1}(g(x))$. Then the problem reduces to finding the limit

$$\lim_{x \rightarrow 0} \frac{x - s(x)}{s^{-1}(x) - x}.$$

If $s(x)$ in a neighborhood of zero decomposes to the Taylor series of the form $x + ax^k + \dots$ then the Taylor series for $s^{-1}(x)$ has the form $x - ax^k + \dots$. Thus the limit of the ratio of the numerator and the denominator equals 1. $\square$

Part 4

Problem 4-1.

Proof. We introduce a coordinate system such that A has coordinates $(0, 0)$, point $B = (0, 1)$, point $C = (1, 0)$. Let X be a point of coordinates (a, b) . Then after an "attraction" to one of the points A, B, C we have points with coordinates.

$$\left(\frac{a}{2}, \frac{b}{2}\right), \quad \left(\frac{a}{2} + \frac{1}{2}, \frac{b}{2}\right), \quad \left(\frac{a}{2}, \frac{b}{2} + \frac{1}{2}\right)$$

Hence, for any $\varepsilon > 0$ there exists n such that after several "attractions" both coordinates a and b becomes bigger then $-\varepsilon$. Therefore after several attractions distance between any point and $\triangle ABC$ becomes smaller than ε . Without loss of generality we assume that $x \in \triangle ABC$.

Attraction to A of a set $\mathcal{X} \subset \triangle ABC$ produces a set $\mathcal{X}_A$, which is 4 times smaller by area. It is easy to see that area of

$$\mathcal{X}_A \cup \mathcal{X}_B \cup \mathcal{X}_C$$

is smaller than $3/4$ of area of $\mathcal{X}$ or is equal to it. Thus after n -th attraction any point of ABC comes to union of triangles (Sierpinski's curpet), the common area of which is $(3/4)^n$ of ABC or smaller. Therefore there exists a figure $\mathcal{F}$ with area 0.00000001 such that any sequence of attractions of any point hits $\mathcal{F}$. $\square$

Problem 4-2.

Proof. Denote $f(x) = x^2 - 10$. The equation $f(x) = x$ has exactly two real solutions, namely $x_{1,2} = \frac{1 \pm \sqrt{41}}{2}$. Note that x_1, x_2 are fixed points of the map $x \rightarrow f(x)$. For certainty assume $x_2 > x_1$. Let x_2^* be the root of $f(x) = x_2$ distinct from x_2 , and let y_1, y_2 be roots of $f(x) = x_2^*$ such that $y_1 < y_2$. Observe that f is monotonous at segments $[x_2^*, y_1]$ and $[y_2, x_2]$ and the images of these segments coincide with $[x_2^*, x_2]$. It is important that the derivative of f at $[x_2^*, y_1]$ and $[y_2, x_2]$ is not less than 3.

For all $x \in [-10, x_2^*] \cup [x_2, +\infty)$ the sequence $x, f(x), f(f(x)), \dots$ tends to infinity and increases starting with the second term. Hence the set of points x such that the limit for $x, f(x), f(f(x)), \dots$ does not exist or is not infinite, coincides with

$$\cap_i f^{(-i)}([x_2^*, x_2]) = \cap_i f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]).$$

The preimage $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2])$ consists of 2^{i+1} pieces, and each piece maps bijectively to some piece $f^{(-i+1)}([x_2^*, y_1] \cup [y_2, x_2])$. Since the derivative

of f is not less than 3 on $[x_2^*, y_1] \cup [y_2, x_2]$, the total length $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2])$ does not exceed $2/3$ of the total length of $f^{(-i+1)}([x_2^*, y_1] \cup [y_2, x_2])$. Thus it is evident that $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]) < 0.0000001$ for some i . Hence $f^{(-i)}([x_2^*, y_1] \cup [y_2, x_2]) < 0.0000001$ is the required system of segments that contains all points x such that the limit of $x, f(x), f(f(x)), \dots$ does not exist or is not infinity. $\square$

Part 5

Problem 5-1.

Proof. Let us find the derivative of

$$(f^{(n)}(x) - x)' = -\sin(f^{(n-1)}) \cdot (f^{(n-1)})' - 1.$$

Observe that further similar decomposition of the derivative shows that the first term has the absolute value not greater than 1. Hence the function $f^{(n)}(x) - x$ monotonically decreases. Furthermore the zero clearly is a solution for $\cos x = x$, and this is the only solution for the original equation. $\square$

Problem 5-2.

Proof. Let us start with solving of the equation $f(x) = x$, that is, $1 - x^2 = x \Leftrightarrow x^2 + x - 1 = 0$. Its solutions are $x_{1,2} = \frac{-1 \pm \sqrt{5}}{2}$. Furthermore for $x < \frac{-1 - \sqrt{5}}{2}$ the values of $f^{(n)}(x)$ decrease. The image of $[-1, 0]$ is the segment $[0, 1]$, hence the equation has no solutions on this segment. Similarly we may take its preimage, the preimage of its preimage and so on to obtain that the equation has no solutions on $[\frac{-1 - \sqrt{5}}{2}, 0]$. Now denote $\frac{-1 + \sqrt{5}}{2}$ by φ and observe that $\forall x \in [0, \varphi] f(x) \in [\varphi, 1]$ and $\forall x \in [\varphi, 1] f(x) \in [0, \varphi]$. Thus for iterations of f with odd numbers the only roots are $x_{1,2}$. Now consider $f^{(2)}$. It is determined by the polynomial $2x^2 - x^4$ of degree 4. The function $f^{(2)}(x) - x$ has four roots, two of which are $x_{1,2}$ and two others are 0 and 1. This implies that on $[0, \varphi]$ the graph of $f^{(2)}$ is located on one side of line $y = x$, and iterations $f^{(2)}$ that are iterations of f with even numbers will change the value of $f^{(2k)}(x)$ monotonously inside the interval $(0, \varphi)$. Hence this interval contains no solutions. Similarly for $(\varphi, 1)$. Thus there exist two solutions $\frac{-1 \pm \sqrt{5}}{2}$ for all n and two more solutions 0 and 1 for even n . $\square$

Problem 5-3-b.

Proof. Let f, g be a pair of functions such that

$$\lim_{x \rightarrow 0} f(x) = \lim_{x \rightarrow 0} g(x) = 0.$$

If $\lim_{x \rightarrow 0} \frac{g(x)}{f(x)} = 0$ then we will allow notation $o(f(x))$ for $g(x)$. We will prove a statement more general than that of Problem 5-3-b.

Statement. If $f(x) = x - \frac{x^3}{6} + o(x^3)$ then $\lim_{n \rightarrow \infty} \sqrt{n} f^{(n)}(x_0) = \sqrt{3}$ for all x_0 sufficiently close to 0. To prove this, denote the function $\sqrt{x}$ by $SQ(x)$. Consider the function

$$\tilde{f} := SQ^{-1} \circ f \circ SQ.$$

It is easy to see that $(SQ^{-1} \circ f \circ SQ)(x) = x + \frac{1}{3} + o(1)$.

Proposition. Suppose for some function $\tilde{f}$ we have

$$\tilde{f}(x) = x + \frac{1}{3} + o(1).$$

Then for all x with sufficiently small absolute value we have $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(x)}{n} = \frac{1}{3}$.

Proof. For any x with sufficiently small absolute value and for all $\varepsilon > 0$ there exists N such that for any $n > N$ we have

$$f^{(n+1)}(x) \in [f^{(n)}(x) + \frac{1}{3} - \varepsilon, f^{(n)}(x) + \frac{1}{3} + \varepsilon].$$

Hence for any $n > N$ we have

$$f^{(n)}(x) \in [f^{(N)}(x) + \frac{1}{3}(n - N) + (n - N)\varepsilon, f^{(N)}(x) + \frac{1}{3}(n - N) - (n - N)\varepsilon]$$

and thus

$$\frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n - N} < \frac{f^{(n)}(x)}{n - N} < \frac{1}{3} - \varepsilon + \frac{f^{(n)}(x)}{n - N}.$$

Consequently there exists N' such that for all $n > N'$ we have

$$\frac{1}{3} - 2\varepsilon < \frac{f^{(n)}(x)}{n} < \frac{1}{3} + 2\varepsilon.$$

Hence $\lim_{n \rightarrow \infty} \frac{f^{(n)}(x)}{n} = \frac{1}{3}$. □

Suppose $x = SQ(y)$. Note that

$$SQ^{(-1)}(f^{(n)}(x)) = SQ^{(-1)}(f^{(n)}(SQ(y))) = (SQ^{(-1)} \circ f \circ SQ)^{(n)}(y).$$

Remind that $\tilde{f} := SQ^{(-1)} \circ f \circ SQ$. By the above Proposition, $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(y)}{n} = \frac{1}{3}$. Hence

$$\lim_{n \rightarrow \infty} \frac{\left(\frac{1}{f^{(n)}(x)}\right)^2}{n} = \frac{1}{3}.$$

Thus $\lim_{n \rightarrow \infty} \sqrt{n} f^{(n)}(x) = \sqrt{3}$. □

For conjugating function (SQ) we can use the function $e^{-\frac{1}{x^2}}$ as well. Investigate this case by yourself.

Problem 5-3-4. The solution of this problem coincides with that of Problem 5-3-2 but we find it worth while to repeat it.

Proof. We will prove a statement more general than that of Problem 5-3-2.

Statement. If $f(x) = x - ax^k + o(x^k)$ then

$$\lim_{n \rightarrow \infty} {}^{k-1}\sqrt{n} f^{(n)}(x) = {}^{k-1}\sqrt{\frac{1}{(k-1)a}}$$

for all x sufficiently close to 0.

Denote the function ${}^{k-1}\sqrt{x}$ by $SQ(x)$ and consider the function

$$\tilde{f} := SQ^{-1} \circ f \circ SQ.$$

It is easy to see that $(SQ^{-1} \circ f \circ SQ)(x) = x + (k-1)a + o(1)$.

Statement. Suppose for some function $\tilde{f}$ we have

$$\tilde{f}(x) = x + \alpha + o(1).$$

Then for all x with sufficiently small absolute value we have $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(x)}{n} = \alpha$.

Suppose $x = SQ(y)$. Note that

$$SQ^{(-1)}(f^{(n)}(x)) = SQ^{(-1)}(f^{(n)}(SQ(y))) = (SQ^{(-1)} \circ f \circ SQ)^{(n)}(y).$$

Remind that $\tilde{f} := SQ^{(-1)} \circ f \circ SQ$. By the above Proposition $\lim_{n \rightarrow \infty} \frac{\tilde{f}^{(n)}(y)}{n} = (k-1)a$. Hence

$$\lim_{n \rightarrow \infty} \frac{\left(\frac{1}{f^{(n)}(x)}\right)^{(k-1)}}{n} = {}^{k-1}\sqrt{\frac{1}{(k-1)a}}.$$

Thus $\lim_{n \rightarrow \infty} {}^{k-1}\sqrt{n} f^{(n)}(x) = {}^{k-1}\sqrt{\frac{1}{(k-1)a}}$. □

Problem 5-5.

Proof. Let $f(x) = x - \exp(-1/x^2)$, $x_n = f^{(n)}(x)$ and let $y_n = 1/x_n$. Then we have $y_{n+1} - y_n \sim y_n \exp(y_n^{-2})$.

Change our equation with a differentiable because it will not change asymptotics. Let estimate function $f(n)$ for which $y' = ye^{-y^2}$, $dy/ye^{y^2} = 1$, or $\int_1^h \exp(u^2)/u^2 du^2 = 2h + C$. We can see that for sufficiently large y y^2 is constant comparing to $\exp(y^2)$, From asymptotic point of view we can change function to z such that

$$\frac{1}{2h^2} \int_1^h du^2 e^{u^2} \sim t, \text{ so } \frac{e^{h^2}}{2h^2} \sim n$$

or

$$h^2 \sim \ln(n) + 2 \ln(h) \sim \ln(n) + \ln(\ln(n)) \quad h \sim \sqrt{\ln(n)}.$$

$$\text{Hence } \lim \sqrt{\ln(n)} \cdot x_n = 1.$$

□

Part 6**Problem 6-1.**

Proof. Let $f(x)$ commute with $y(x)$. Then $2f(x) = f(2x)$. Note that

$$f(1) = 2f\left(\frac{1}{2}\right) = 4f\left(\frac{1}{4}\right) = \dots,$$

and so $f(0) = 2f(0)$, hence $f(0) = 0$. Let us show that $\frac{f(x)}{x}$ is a constant. In fact,

$$\frac{f(x)}{x} = \frac{f\left(\frac{x}{2}\right)}{\frac{x}{2}} = \frac{f\left(\frac{x}{4}\right)}{\frac{x}{4}} = \dots = f'(0)$$

for any x . Hence $f(x) = f'(0)x$. □

Problem 6-2.

Proof. Consider an arbitrary continuous function $f_{2,4}$ defined on $[2, 4]$ and equal to 0 at its endpoints. By formulas

$$f(2x) = 2f(x), f(-x) = f(x), f(0) = 0$$

extend $f_{2,4}$ to the whole real axis. Obviously the resulting function is defined and differentiable at all points including zero. If $f_{2,4}$ is not differentiable in some internal point then obviously the same holds for f . □

Part 7

Problem 7-1

Proof. a) We will prove this problem using mathematical induction. The base obviously holds.

Inductive step: $n \rightarrow n + 1$.

$$\begin{aligned}
 & \cos(n \cdot \arccos(x)) = \\
 &= x \cos((n-1) \cdot \arccos(x)) - \sin(\arccos(x)) \sin((n-1) \arccos(x)) = \\
 &= x^2 \cos((n-2) \cdot \arccos(x)) - \sin^2(\arccos(x)) \sin((n-2) \arccos(x)) - \\
 & \quad 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)) = \\
 &= x^2 \cos((n-2) \cdot \arccos(x)) - (1 - \cos^2(\arccos(x))) \cos((n-2) \arccos(x)) - \\
 & \quad 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)).
 \end{aligned}$$

It is clear that the first and the second summand of this sum are polynomials. As

$$\begin{aligned}
 & 2x \sin(\arccos(x)) \sin((n-2) \arccos(x)) = \\
 &= 2x \cos(\arccos(x)) \cos((n-2) \arccos(x)) - 2x \cos((n-1) \arccos(x)),
 \end{aligned}$$

, $\cos(n \arccos(x))$ is a polynomial.

b) We have

$$\begin{aligned}
 & \sin((2n-1) \arcsin(x)) = \sin((2n-1)(\frac{\pi}{2} - \arccos(x))) = \\
 &= \sin(\frac{(2n-1)\pi}{2} - (2n-1) \arccos(x)) = \pm \cos((2n-1) \arccos(x)),
 \end{aligned}$$

Therefore $\sin((2n-1) \arcsin(x))$.

) We will prove this problem using mathematical induction. The base obviously holds.

Inductive step: $n \rightarrow n + 1$.

$n \rightarrow n + 1$.

$$\tan(n \arctan(x)) = \frac{\tan((n-1) \arctan(x)) + x}{1 - x \tan((n-1) \arctan(x))}.$$

In this fraction the numerator and the denominator are rational functions. Therefore the quotient of them is a rational function too. $\square$

Problem 7-2.

Proof. The set of roots of $\sin(x) = 0$ is denumerable. From the other hand the number of roots of $P(x) = a$ is always countable for any a . Therefore $\sin(x)$ is not conjugated to a polynomial. $\square$

Problem 7-3

Proof. We assume that $c \neq 0$ (cf. 2-1-c). If we find a function R such that $R \circ f \circ R^{(-1)}$ is a linear function. Hence we know all fractional iterations of linear function, such function R provide a solution of problem 7-3. First we conjugate f by function $R_1 = x + \frac{a}{c}$. We have

$$f_1 := R_1 \circ f \circ R_1^{(-1)} = \alpha + \frac{\beta}{x},$$

where α and β are some numbers. Then we conjugate f_1 by $R_2 := x\sqrt{\beta}$. We have

$$f_2 = R_2 \circ f_1 \circ R_2^{(-1)} = s + \frac{1}{x}$$

. Let λ be a number such that $\lambda(\lambda - s) - 1 = 0$. We conjugate f_2 by $R_3 := 1 + \frac{1}{x+\lambda}$. We have

$$f_3 := R_3 \circ f_2 \circ R_3^{(-1)}.$$

The function f_3 is linear. □

Problem 7-4.

Proof. Note that

$$(f^n)'(0) = f'(f(f(\cdots)))(0) \cdot f'(f(\cdots))(0) \cdots f'(0) = k^n.$$

Then

$$\begin{aligned} (R \circ f \circ R^{(-1)})'(0) &= R'(f(R^{(-1)}(0)))f'(R^{(-1)}(0))(R(-1))'(0) = \\ &= f'(0) \cdot R'(0) \cdot (R(-1))'(0) = f'(0). \end{aligned}$$

We recall that $|f'(0)| = |k| < 1$. Let q be a real number such that $q : |k| < q < 1$. As $|f'(0)| < q$, there exists a neighborhood of 0 such that for any point from this neighborhood $|f(x)| < q|x|$. Therefore for any point x of this neighborhood

$$|f^n(x)| < q^n x,$$

and hence $f^{(n)}(x) \Rightarrow 0$ for $n \rightarrow \infty$. □

Problem 7-5.

Proof. We'll start our proof with some useful facts.

Proposition. Let f be a twice differentiable function such that $f(0) = 0$ and $f'(0) = k$, for $0 < k < 1$. Then

$$\exists C > 0 \exists \varepsilon > 0 \mid \forall x \in (-\varepsilon, \varepsilon) \mid f^{(n)}(x)' < Ck^n.$$

Proof. Let f, g be functions such that

$$\lim_{x \rightarrow 0} f(x) = \lim_{x \rightarrow 0} g(x) = 0.$$

If function $\frac{g(x)}{f(x)}$ exists and is bounded in 0 neighborhood, we will write $O(f(x))$ instead of $g(x)$.

Let us find $f^{(n)}(x) =$

$$f'(x)f'(f(x))\dots f'(f^{(n-1)}(x)).$$

By

$$f'(f^{(m)}(x)) = k(1 + O(f^{(m)}(x))) =$$

we conclude that

$$\frac{f^{(n)'}(x)}{k^n} = (1 + O(x))(1 + O(f(x)))\dots(1 + O(f^{(n-1)}(x))).$$

Series

$$x + f(x) + f(f(x)) + \dots$$

is absolutely convergent, there exists constant number C such that $f^{(n)}(x) < Ck^n$. $\square$

For function f and integer m we will write $f^{[m]}$ for m -th derivative of f .

Proposition. Let f be a function such that $f(0) = 0$ and $f'(0) = k$, for $-1 < k < 1$. Then

$$\forall m \geq 1 \exists C_m > 0 \exists \varepsilon_m > 0 \mid \forall x \in (-\varepsilon_m, \varepsilon_m) \mid f^{(n)}(x)^{[m]} < C_m k^n.$$

Proof. We will use the following lemma:

Proposition. Let exist a constant C for some $m > 0$ that, for each $r \leq m$ we have $f^{(n)}(x)^{[m]} \leq Ck^n$, then for each r such that $1 < r \leq m$ we have $(f'(f^{(n)}(x)))^{[r]} \leq C'k^n$ for some constant C' .

Proof. When we differentiate $f'(f^{(n)}(x))$ at most m times in each summand has $f^{(n)}$ or derivative $f^{(n)}$ with order not more than m . $\square$

Let us recall $f^{(n)}(x)' =$

$$f'(x)f'(f(x))\dots f'(f^{(n-1)}(x)).$$

Note that $f^{(n-1)}(x)^{[m]} = (f^{(n-1)}(x)^{[1]})^{[m-1]}$. We will prove the statement using induction. Base is a previous Proposition. Inductive step $m \rightarrow m+1$. Expression $f^{(n)}(x)'$ is a product of n parts and taking its m -th derivative is a sum of n^m summands, each having no more than m factors $f^{(n)}(x)'$ changed. Consider all expressions with exactly $r \leq m$ factors changed. Derivative of changed factor $f'(f^{(s)}(x))$ is less or equal to $C'k^s$, sum of changed factors is less or equal to

$$m!k^{n-r} \sum_{i_1, \dots, i_r \leq n} \prod_{q=1}^r (C'k^{i_q}) = m!C'^r k^{n-r} \prod_{q=1}^r (1 + \dots + k^n) \leq m!C'^r k^{n-r} \left(\frac{1}{1-k} \right)^r.$$

Obviously, summing those for all r is less or equal to $C''k^n$ for some $C'' > 0$. $\square$

If for a set $\mathcal{F}$ of continously differentiable functions there exists C such that $\forall f \in \mathcal{F}$ we have

$$|f(x)| < C \text{ and } |f'(x)| < C$$

for each x , then there exists a sequence of distinct functions $f_1, f_2, \dots, f_n$ from $\mathcal{F}$ ([?]Z) Arzel-Ascoli's theorem). From evenly boundeness of m -th derivatives of $\frac{f^{(n)}}{k^n}$ for each $m \geq 1$, there exists a sequence $n_1, n_2, \dots$ such that sequence $\frac{f^{(n_1)}}{k^{n_1}}, \frac{f^{(n_2)}}{k^{n_2}}, \dots$ converges evenly with series of its m -th derivatives for all $m \geq 1$. Hence, sequence

$$\frac{f^{(n_1)}}{k^{n_1}}, \frac{f^{(n_2)}}{k^{n_2}}, \dots$$

converges evenly, hence, it converges to G , which is the limit of this sequence at each point, from which we conclude that G is smooth. From the equality

$$\frac{f^{(n-1)}(f(x))}{k^{n-1}} = k \frac{f^{(n)}(x)}{k^n}$$

we have

$$G(f(x)) = kG(x).$$

Derivative at 0 of all functions in sequence $\frac{f^{(n)}(x)}{k^n}$ equals 1, so derivative of $G(x)$ at 0 is 1. Hence, G is invertible in 0 neighborhood $f(x) = G^{(-1)}(kG(x))$. $\square$

Remark. Instead of Arzel-Ascoli theorem we can use the following fact: for a sequence of functions $\{f_i\}_{i \in \mathbb{Z}_{\geq 0}}$ converges and their second derivatives are uniformly bounded, then sequence of first derivatives converges too.

Problem 7-6.

Proof. We set $\frac{x}{2} = \cos(t)$. Then the left side can be written is this way:

$$\prod_{k=1}^n \cos\left(\frac{t}{2^k}\right).$$

We multiply and divide it by $\frac{2^n}{t} \sin\left(\frac{t}{2^n}\right)$, which is earning to 1 when $n \rightarrow \infty$. We have $\prod_{k=1}^n \cos\left(\frac{t}{2^k}\right) \sim \frac{\cos(2t)}{t}$. After changing back x to $2 \arccos t$ we solve the problem. This problem can also be solved by using problem 7-5.

Problems 7-8 and 7-9 immediately follows from the problems 7-1–7-5. From the problems 7-1–7-9 one can easily get solutions for problems 8-2. $\square$

Problem 7-10.

Scetch of a proof. We set $f(x) := x - e^{-\frac{1}{x^2}} (x \geq 0)$. For any $x > 0$ we have $f(x) < x$. The only fixed point of f is 0. We define points $\{x_i\}$ in such way that

$$f(x_i) = x_{i+1}, \quad x_0 = 1.$$

Let $\delta(x)$ be a smooth function on $[x_0, x_1]$, which has zero derivatives of all orders at x_0 and x_1 . Function $f(x) + \delta(x)$ is extendable to the smooth function on $\mathbb{R}_{\geq 0}$. As any derivative of $e^{-\frac{1}{x^2}}$ equals 0, the extension would be smooth at 0. $\square$

Part 8

Problem 8-1.

Proof. Let $Q(x)$ be a polynomial of degree m , such that $Q(x)$ commutes with $P(x)$. Let $q_1, \dots, q_{m-1}$ be roots of $Q'(x)$. Then the polynomial $Q(x) - Q(q_i)$ has multiple roots for all i . Therefore the polynomial

$$Q(x) - Q(P^{(r)}(q_i))$$

has multiple roots for any integer i and any integer r . Hence the set of numbers $\{Q(P^{(n)}(q_i))\}$ is finite and has not more than m elements. Therefore there exists a finite set $\mathcal{S}$ such that for any polynomial Q which satisfies the conditions of the problem the roots of $Q'(x)$ are contained in $\mathcal{S}$.

Hence it is enough to show that there exists only finite set of polynomials Q , such that roots of Q' lies in $\mathcal{S}$ and $Q(x)$ commutes with $P(x)$. Such functions expressed as $\alpha Q_0 + \beta$, where Q_0 depends only on the set of roots of Q' and α, β are some numbers. The set of possible coefficients α is finite because the highest coefficients of

$$\alpha Q_0(P(x)) + \beta = P(\alpha Q_0(x) + \beta)$$

have to coincide. Hence the equality

$$\alpha Q_0(P(0)) + \beta = P(\alpha Q_0(0) + \beta)$$

provides only finite number of possibilities for β . □

Problem 8-2 follows from problems **7-1–7-9**.

References

[Z] Vladimir Zorich, Mathematical Analysis I,II, UT, Springer, 2004.

Fractal iterations of functions.

10 августа 2011 г.

9. Complex dynamics

For home thinking

Let $f(0) = 0$, $f'(0) = k \neq 0$. When $f(x)$ is conjugated with $k \cdot x$ in some neighborhood of zero?

1. Let f analytic function and $|k| \neq 1$. Then there exist analytic function G such that $f(x) = G(kG^{(-1)}(x))$. Let $k^{2011} = 1$. Give an example of such function which is not conjugate to linear one.
2. Let k is not a root of unity. Then f is conjugated to linear one as a formal power series.
3. Prove that this series can be divergent.
4. Prove that for some k such that $|k| = 1$ this power series must converge.

On the Functional Equation $f \circ f = g$

Vlad Vicol* and Apostol Apostolov†

Abstract

The functional equation $f \circ f = g$ for continuous g has no continuous solutions defined on intervals. If f may have finitely many discontinuities, we show that solutions exist on closed, but not on open intervals.

1 Introduction

The functional equation

$$f(f(x)) = g(x) \quad \text{for all } x \in \mathbb{R} \quad (1)$$

with a strictly decreasing function g has no solution f in the class of continuous functions. Indeed, because $g : \mathbb{R} \rightarrow \mathbb{R}$ is strictly decreasing, it is injective. This implies injectivity of f , and, by continuity, f is strictly monotone. In both cases, $f \circ f$ is strictly increasing, contradicting the decay of g .

Nevertheless, if we allow f not to be continuous, even for the easiest example of a decreasing function g , say $g = -id$, the problem becomes intricate and very complex (Section 2). For countable many discontinuities we can construct a solution of $f \circ f = -id$, but in the class of functions with **finitely** many points of discontinuity the situation is not quite predictable: for f defined on a closed interval there exist solutions (see Proposition 2), but for f defined on open intervals (e.g. $\mathbb{R}$), no solution exists (see Theorem 1).

All the results we obtain for functions $f, g : I \rightarrow I$ for an open interval I extend to functions $\tilde{f}, \tilde{g} : \mathbb{R} \rightarrow \mathbb{R}$, since any open interval is homeomorphic to $\mathbb{R}$. For example given homeomorphism $h : (-1, 1) \rightarrow \mathbb{R}$, $h(x) = \tan(\frac{\pi}{2}x)$, and function $f : (-1, 1) \rightarrow (-1, 1)$ such that $f \circ f = -id_{(-1,1)}$. Then function $\tilde{f} : \mathbb{R} \rightarrow \mathbb{R}$, $\tilde{f} = h^{-1} \circ f \circ h$ satisfies $\tilde{f} \circ \tilde{f} = -id_{\mathbb{R}}$.

*International University Bremen; 28759 Bremen, Germany; v.vicol@iu-bremen.de

†International University Bremen; 28759 Bremen, Germany; a.apostolov@iu-bremen.de

2 $f \circ f = -id$ and the "odd-even effects" on orbits

We denote by f^n the function $\underbrace{f \circ f \circ \dots \circ f}_{n \text{ times}}$.

The *orbit* of a point x_0 is the set $\text{orb}(x_0) = \{f^n(x_0) \mid n \in \mathbb{N}\}$. Similarly, the orbit of an interval I is the set of sets $\text{orb}(I) = \{f^n(I) \mid n \in \mathbb{N}\}$.

Let us first focus on the functional equation $f \circ f = -id$. In this case it is easy to show that f is bijective. Indeed, if $f(x) = f(y)$, then $f(f(x)) = f(f(y))$ and hence $-x = -y$. Surjectivity of f follows from the equation $f(-f(x)) = x$ for all $x \in (-1, 1)$. Further observe that $f(x) = x$ implies $f(f(x)) = f(x) = x$, hence $-x = x$ and $x = 0$. Thus 0 is the only fixed point of f .

Then, for all $x \in (-1, 1)$, $f^4(x) = f(f(f(f(x)))) = -(-x) = x$; hence, the number of elements in any orbit has to divide 4. If $x = f(f(x))$, then $x = -x$ and $x = 0$. If $x = f(x)$, then by uniqueness of the fixed point $x = 0$. Thus the orbit of every point, except zero, has exactly 4 elements. Also the orbit of every point of discontinuity has 4 elements. These observations are central to the construction and the understanding of the functional equation $f \circ f = -id$.

But does it matter whether there are finitely or infinitely many such points? We shall see that this does matter and that in addition to this the domain on which our functions are defined is equally as important.

Proposition 1. *There exists a function $f : (-1, 1) \rightarrow (-1, 1)$ with countably many points of discontinuity such that $f(f(x)) = -x$ for all $x \in (-1, 1)$.*

PROOF. Let us construct f inductively:

Step 1: Split the open interval $(-1, 1)$ into 5 parts

$$I_1^1 = (-1, -\frac{2}{3}], \quad I_2^1 = (-\frac{2}{3}, -\frac{1}{3}], \quad I_3^1 = (-\frac{1}{3}, \frac{1}{3}), \quad I_4^1 = [\frac{1}{3}, \frac{2}{3}), \quad I_5^1 = [\frac{2}{3}, 1).$$

Map f acts as follows (homeomorphically): $I_5^1 \rightarrow I_2^1 \rightarrow I_1^1 \rightarrow I_4^1 \rightarrow I_3^1$.

Step k: Split the middle interval $I_3^{k-1} = (-\frac{1}{3^{k-1}}, \frac{1}{3^{k-1}})$ into 5 parts:

$$\begin{aligned} I_1^k &= (-\frac{1}{3^{k-1}}, -\frac{1}{3^k}], & I_2^k &= (-\frac{2}{3^k}, -\frac{1}{3^k}], & I_3^k &= (-\frac{1}{3^k}, \frac{1}{3^k}), \\ I_4^k &= [\frac{1}{3^k}, \frac{2}{3^k}), & I_5^k &= [\frac{2}{3^k}, \frac{1}{3^{k-1}}). \end{aligned}$$

Map f acts as follows: $I_5^k \rightarrow I_2^k \rightarrow I_1^k \rightarrow I_4^k \rightarrow I_3^k$.

Also set $f(0) = 0$. Then the constructed function is obviously well defined, injective, and surjective (since $\lim_{k \rightarrow \infty} (\frac{1}{3})^k = 0$). Moreover, it satisfies $f(f(x)) = -x$, hence the construction is done. ■

Proposition 2. *There exists a functions $f : [-1, 1] \rightarrow [-1, 1]$ with finitely many points of discontinuity such that $f(f(x)) = -x$ for all $x \in [-1, 1]$.*

PROOF. Let's construct f . Set $f(0) = 0$ and let f map $1/2 \rightarrow -1 \rightarrow -1/2 \rightarrow 1 \rightarrow 1/2$. The remaining open intervals are mapped as in below, i.e., $f((-1/2, 0)) = (-1, -1/2)$, $f((0, 1/2)) = (1/2, 1)$ (using symmetry over the vertical axis), and $f((1/2, 1)) = (-1/2, 0)$, $f((-1, -1/2)) = (0, 1/2)$ (using symmetry over the origin). Compare with Figure 2, where the orbit of a point x is depicted using symmetry. ■

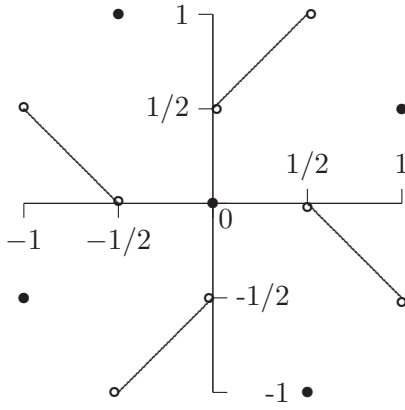


Figure 1: The graph of f

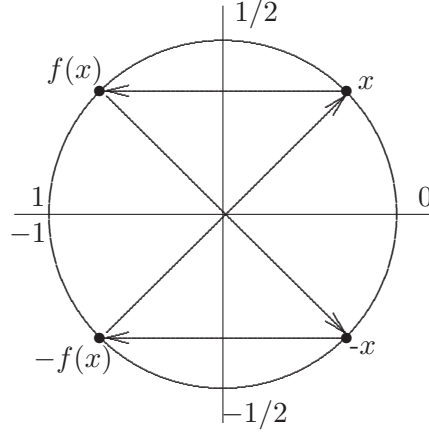


Figure 2: The orbit of x

Note that solving the equation $f(f(x)) = -x$ is equivalent to the fact that the graph of f is symmetric under a plane rotation of 90° (see Figure 1).

Theorem 1. *There exists **no** function $f : (-1, 1) \rightarrow (-1, 1)$ with finitely many points of discontinuity such that $f(f(x)) = -x$ for all $x \in (-1, 1)$.*

PROOF. Suppose there exists f which satisfies (1). Then, as showed above, f is bijective and 0 is the only fixed point. We also proved that the orbit of every point, except zero, contains exactly 4 elements.

Consider the set $A = \{a_1, a_2, \dots, a_n\}$ of points of discontinuity of f , and define

$$A^* := \text{orb}(A) \cup \{0\}.$$

Then A^* contains all the discontinuity points of f and their orbits. This means that A^* is fully invariant under f , i.e.

$$f(y) \in A^* \text{ iff } y \in A^*.$$

For further use let's set $A^* = \{b_1, b_2, \dots, b_m\}$, where without loss of generality we can assume that $b_1 < b_2 < \dots < b_m$. Since the orbit of any point in A^* has 4 elements, with the exception of the fixed point 0, we deduce

$$m = 4k + 1 \quad \text{for some } k \in \mathbb{N}. \quad (2)$$

Then define $I_1 = (-1, b_1)$ and for $2 \leq j \leq m$ let $I_j = (b_{j-1}, b_j)$; $I_{m+1} = (b_m, 1)$.

Using Lemma (1) below, for $I = (-1, 1)$ and $M = A^*$, we get that the f -orbit of each I_j has 4 elements, and hence $m + 1 = 4p$ for some $p \in \mathbb{N}$. But this contradicts (2): $4p - 1 = m = 4k + 1$, and therefore the existence of f with finitely many points of discontinuity. ■

Here we can see the combinatorial aspect of the problem. We show that the orbits of the points of discontinuity are even (4), and hence the number of intervals in the induced partition should be odd ($4k+1$). But it turns out that the orbit of the intervals is also even (4) and hence the contradiction is reached.

3 $f \circ f = g$, g continuous

We shall now pose a more general problem: given a strictly decreasing continuous function g , does there exist a function f with **finitely many points of discontinuity** such that $f \circ f = g$? The answer of this question is our main result in this article.

Main Theorem: *Let $g : \mathbb{R} \rightarrow \mathbb{R}$ be a strictly decreasing and continuous function. There exists **no** function $f : \mathbb{R} \rightarrow \mathbb{R}$ with only finitely many points of discontinuity such that $f(f(x)) = g(x)$ for all $x \in \mathbb{R}$.*

Before we can prove this theorem we will first have to provide the following lemmas:

Lemma 1. *Let $I \subseteq \mathbb{R}$ be an open interval and $f : I \rightarrow I$ be a bijective function. Consider a set of points $M \subset I$ with $|M| = m$ for some $m \in \mathbb{N}$, such that $x \in M$ iff $f(x) \in M$. Let $\{I_j\}_{j=1}^{m+1}$ be the partition of I into open intervals induced by M . Then:*

- i. If f is continuous on each I_j , then $f(I_j) = I_k$ for some $1 \leq k \leq m+1$.*
- ii. If in addition to i., $f \circ f$ is strictly decreasing, then $f^4(I_j) = I_j$ for all $1 \leq j \leq m+1$.*
- iii. In addition to i., ii., if there exists a point $x_0 \in I$ such that $f(f(x_0)) = x_0$, then x_0 is unique. Further, if $x_0 \in M$, then the orbit of each I_j has 4 elements.*

PROOF. Fix some I_j in the partition. Using a canonical numbering of the I_j 's we may assume that for $p < j$, I_p is to the left of I_j and vice versa. f maps I_j to $f(I_j)$ continuously and bijective; hence $f(I_j) = (c, d)$ for some $c, d \in I$. Since $I_j \cap M = \emptyset$ and M is fully invariant under f , we conclude that $f(I_j) \cap f(M) = \emptyset$, i.e., $(c, d) \cap M = \emptyset$. This implies that $(c, d) \subseteq I_k$

for some $1 \leq k \leq m+1$. If $(c, d) \subsetneq I_k$, then c (or d) $\in I_k$. But using f^{-1} , we get $f^{-1}(c) \in I_j$ and thus $c = f(f^{-1}(c)) \in f(I_j) = (c, d)$, a contradiction. Thus we've showed that $f(I_j) = I_k$ for some $1 \leq k \leq m+1$, and statement (i) is proven.

Using that f^2 is strictly decreasing, we immediately get that f^4 is strictly increasing. There exist *exactly* $j-1$ intervals to the left of I_j . Then by applying f^4 and (i), there will be *exactly* $j-1$ intervals to the left of $f^4(I_j)$. Thus we conclude that $f^4(I_j) = I_j$ and (ii) is proven.

By (ii), we get that the orbit of each I_j has either 1, 2, or 4 elements (since it has to divide 4 a orbit of 3 is impossible). If $f \circ f$ has a fixed point, then it is unique since the function $h_1 = f^2 - \text{id}$ is strictly decreasing. If we would have that $f(f(I_j)) = I_j$ then, using the continuity of h_1 on each I_k and the Intermediate Value Theorem, we would get that there exists $x \in I_j$ such that $h_1(x) = 0$, i.e. $x = x_0 \in M$, a contradiction. Using that f^2 is injective and $f^2(x_0) = x_0$, we get that $f(x_0) = f(f^2(x_0)) = f^2(f(x_0))$ and hence $f(x_0) = x_0$. If there exists another fixed point x of f then $f(x) = x = f(f(x))$ and hence x_0 is the only fixed point of both f and $f \circ f$. Using the same argument as above, the function $h_2(x) = f(x) - x$ is continuous on each I_j and hence we cannot have $f(I_j) = I_j$. Thus the orbit of each interval can only have 4 elements, and (iii) is proven. ■

Lemma 2. *Let I and J be open intervals, such that $J \subseteq I$. Take two functions $f, g: I \rightarrow J$, such that f and g commute ($f \circ g = g \circ f$) and g is continuous and bijective. Then, f is continuous at x_0 iff f is continuous at $g(x_0)$.*

$$\begin{array}{ccc}
 x \bullet & \xrightarrow{g} & \bullet g(x) \\
 \downarrow f & & \downarrow f \\
 f(x) \bullet & \xrightarrow{g} & \bullet g(f(x)) = f(g(x))
 \end{array}$$

PROOF. Due to symmetry it is enough to prove only one implication. One only needs to switch the mapping g with g^{-1} . Note that the bijectivity and continuity of g implies the bijectivity and continuity of g^{-1} .

Let f be continuous at $x_0 \in I$ and set $y_0 = g(x_0) \in J$. Take any sequence $(y_n) \subset J$, such that $y_n \rightarrow y_0$. g^{-1} is bijective, thus for any $n \in \mathbb{N}$ there exists exactly one $x_n \in I$ such that $g(x_n) = y_n$. Further, $x_n \rightarrow x_0$, since g^{-1} is continuous. Using the fact that f is continuous at x_0 we conclude

$$f(y_n) = f(g(x_n)) = g(f(x_n)) \rightarrow g(f(x_0)) = f(g(x_0)) = f(y_0)$$

Thus f is continuous at $g(x_0) = y_0$, and the lemma is proven. ■

Lemma 3. *Let $I \subset \mathbb{R}$ be an open interval and $f, g : I \rightarrow I$ such that $f \circ f = g$, g is continuous and bijective. Then if f has only finitely many points of discontinuity, the orbit of each non-fixed point has exactly 4 elements.*

PROOF. Let A be the set of points of discontinuity of f . Since g and f obviously commute, we can apply Lemma 2 and get that the g -image of a discontinuity point of f is a discontinuity point of f , i.e. $g(A) \subseteq A$. Since A is finite and g injective we conclude that $g(A) = A$. Take any $a \in A$. Let $l \in \mathbb{N}_0$ be the number of elements in A that are strictly smaller than a . Since $g \circ g$ is strictly increasing and $g(g(A)) = A$, there will be *exactly* l elements in A that are strictly less than $g(g(a))$, hence $g(g(a)) = a$. $f(a) \neq a$ and $g(a) = f(f(a)) \neq a$ since a is not a fixed point of f or g , but $f^4(a) = a$. ■

Now we can proceed with the proof of our Main Theorem:

PROOF OF MAIN THEOREM. Assume that there exists an f satisfying the conditions of the theorem.

Obviously, $g(\mathbb{R}) \subseteq \mathbb{R}$, and for all $n \in \mathbb{N}$, $g^{n+1}(\mathbb{R}) \subseteq g^n(\mathbb{R})$. Since g is continuous and strictly monotone, $g^k(\mathbb{R})$ is an open interval in $\mathbb{R}$. Let

$$I = \bigcap_{k=0}^{\infty} g^k(\mathbb{R}).$$

First, let's show that I is not empty. Since g is strictly decreasing, $h(x) = g(x) - x$ has $\lim_{x \rightarrow \infty} h(x) = -\infty$ and $\lim_{x \rightarrow -\infty} h(x) = \infty$. Since h is continuous and strictly decreasing, the equation $h(x) = 0$ has exactly one solution, say x_0 . Note that this implies $f(x_0) = f(g(x_0)) = g(f(x_0))$ and thus $f(x_0) = x_0$. $g(x_0) = x_0$ implies $g^k(x_0) = x_0$ for all $k \in \mathbb{N}$, hence $x_0 \in I$. Since $I \neq \emptyset$ is a countable intersection of open intervals, we can say that it is an interval. Further $g(I) = I$, that is: g is bijective on I . It is easy to see that I cannot be a semi-open interval due to the monotonicity of g . Hence I is either closed or open.

If I is closed, then $I = [a, b]$ for some $a < b$. But since g is strictly decreasing, we get $g(a) = b$, $g(b) = a$. So since the endpoints would not intervene in our reasoning, we consider I as being open.

As one can easily see, if $x \notin I$, then $g(x) \notin I$. Now define A as the set of points at which f is discontinuous. Since it is finite we can represent it as $A = \{a_1, a_2, \dots, a_n\}$.

Take any $x_0 \in \mathbb{R} \setminus A$, and let $y_0 = g(x_0)$. Since A is finite and g is a continuous local bijection, we can find a neighborhood U of y_0 and a neighborhood V of x_0 such that $U \cap A = \emptyset$, $V \cap A = \emptyset$ and $g(V) = U$. Obviously, f and g commute. Hence we can apply Lemma 2 for $g : I \rightarrow U$, $U, V \subseteq I$, and get $y_0 = g(x_0) \in \mathbb{R} \setminus A$. Conversely, $g(x_0) \in \mathbb{R} \setminus A$ implies $x_0 \in \mathbb{R} \setminus A$. Hence we

find that A is fully invariant under f (and g). But from this we conclude that $g(A) \subseteq A$, and since g is injective $g(A) = A$. Hence $A \subset I$.

By applying Lemma 3 to $f, g : I \rightarrow I$, we conclude that the orbit of each a_i has 4 elements. Then the set $A_{ext} = \bigcup_{k=1}^4 \{f^k(a_i) \mid i = 1, \dots, n\} \cup \{x_0\}$ contains all points of discontinuity of f and their orbits. By lemma 2 and $g(x_0) = x_0$, the cardinality of A_{ext} is $4p + 1$ for some $p \in \mathbb{N}$. The partition $I_1 = (a, b_1), I_2 = (b_1, b_2), \dots, I_{4p+1} = (b_{4p}, b_{4p+1}), I_{4p+2} = (b_{4p+1}, b)$, induced on I by A_{ext} , should then be made of $4p+2$ open, disjoint intervals (where we denote the b_i as being the elements of A_{ext} such that $b_i < b_j \Leftrightarrow i < j$). Now we can apply Lemma 1 to I with $M = A_{ext}$ and find that the orbit of each I_j has 4 elements, and hence the number of intervals should be divisible by 4. But this contradicts the fact that the number of elements in the partition is $4p + 2$. Hence we got a contradiction to the existence of f . ■

4 f◦f=g, g discontinuous

We now consider the equation $f \circ f = g$ in the case when $g : \mathbb{R} \rightarrow \mathbb{R}$ is *not* continuous, but both f and $g : \mathbb{R} \rightarrow \mathbb{R}$ are in the class of functions with finitely many points of discontinuity. Is it possible to find solutions of equation (1)?

Proposition 3. *Let $I \subset \mathbb{R}$ be an open interval. There exist functions $f, g : I \rightarrow I$ with finitely many points of discontinuity such that g is strictly decreasing and $f(f(x)) = g(x)$ for all $x \in I$.*

PROOF. Here we do not start by picking a function g and then construct f , but construct f such that f and $f \circ f$ respect the conditions of the theorem. To make calculations easy, we consider $I = (-16, 16)$, instead of $(-1, 1)$.

$$\text{Let } f : (-16, 16) \rightarrow \mathbb{R}, \quad f(x) = \begin{cases} \frac{x}{2} + 2 : x \in (-16, -8) \\ -\frac{x}{2} + 10 : x \in (-8, 0) \\ -\frac{x}{2} - 10 : x \in (0, 8) \\ \frac{x}{2} - 2 : x \in (8, 16) \\ -2 : x = -8 \\ -10 : x = 0 \\ 2 : x = 8 \end{cases}$$

It is trivial to check that f has 3 points of discontinuity and that $g := f \circ f$ is strictly decreasing with also 3 points of discontinuity. To get a better picture of what happens, see Figure 3 and Figure 4. Again we observe that the graph of f is symmetric (except for one point) under a plane rotation of 180° (also see Figure 1). ■

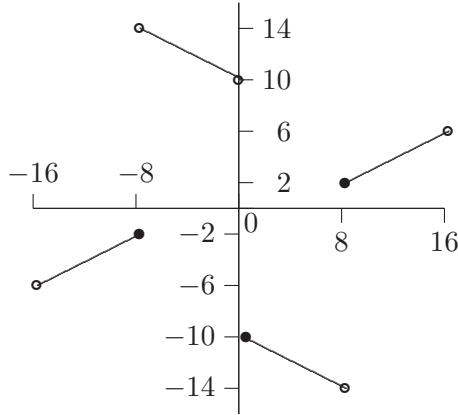


Figure 3: The graph of f

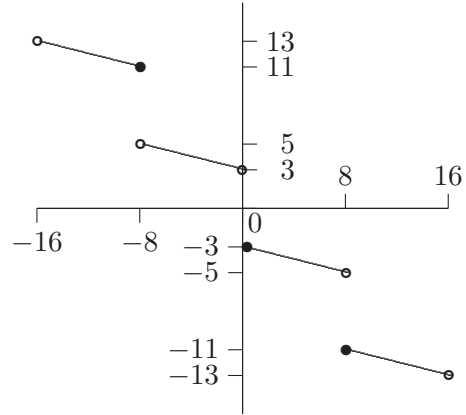


Figure 4: The graph of g

To sum up, we have seen that the aforementioned equation $f(f(x)) = g(x)$ has solutions in the class of *arbitrary* functions (e.g. when $g(x) = -x$). As we have illustrated in our main result, there exist no solutions of (1) when $g(x)$ belongs to the class of continuous, strictly decreasing functions. Surprisingly, when tempted to generalize further to the case when $g(x)$ has finitely many discontinuous points, we obtain an example which shows that (1) actually possesses a solution.

Some other types of functional equations and their relations to dynamical systems can be found in [1] and [2].

ACKNOWLEDGEMENTS: We would like to thank Alexei Belov and Götz Pfander who introduced us to the functional equation $f \circ f = -id$. We are in particular thankful to Alexei Belov who has encouraged us to seek generalizations of this well understood functional equation.

References

- [1] Katok, A., Hasselblatt, B.: *Introduction to the Modern Theory of Dynamical Systems*, Cambridge University Press 1995
- [2] Kuczma, M., Choczewski, B., Ger, R.: *Iterative Functional Equations*, Cambridge University Press 1990

Разбиение множеств на части меньшего диаметра

А.М. Райгородский, а также В. Буланкина и М. Прасолов

1 Определения и обозначения

Назовем *диаметром* множества Ω на плоскости величину

$$\text{diam } \Omega = \sup_{\mathbf{x}, \mathbf{y} \in \Omega} |\mathbf{x} - \mathbf{y}|.$$

Здесь

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}, \quad \mathbf{x} = (x_1, x_2), \quad \mathbf{y} = (y_1, y_2),$$

т.е. это обычное “евклидово” расстояние между точками на плоскости. Значок “sup” – это значок “супремума” (точной верхней грани), и при желании можно считать, что речь идет просто о максимуме. По сути, диаметр множества – это максимум расстояний между его точками. Почему мы все-таки пишем не всем понятный супремум? А потому, что бывают множества, в которых обычный максимум расстояний не достигается. Например, возьмем круг без границы (удалим из круга ограничивающую его окружность). Впрочем, все это детали. Будем предполагать, что все наши множества “замкнуты” (содержат свою границу), и тогда надобность в супремуме отпадет.

Рассмотрим произвольное ограниченное множество Ω . Можно считать, что $\text{diam } \Omega = 1$ (при необходимости сожмем или раздуюм множество с помощью гомотетии). Хотелось бы как можно экономнее разбить Ω на части строго меньшего диаметра. Иными словами, мы хотим представить Ω в виде

$$\Omega = \Omega_1 \cup \dots \cup \Omega_f$$

с условием $\text{diam } \Omega_i < \text{diam } \Omega$ для каждого i . При этом f мы стремимся минимизировать. Можно представлять себе Ω как некий неправильной формы торт, который целиком к нам в рот не лезет, но который по жадности своей мы желаем съесть за наименьшее количество “укусов”. Вот и нужно нам так разрезать торт на куски, чтобы этих кусков было мало и чтобы в рот они к нам все-таки лезли.

Основной вопрос: какой торт хуже всех с точки зрения описанной выше задачи о разрезании на куски? Иначе говоря, на сколько кусков мы заведомо любой торт разделим?

К. Борсук в 1933 году формализовал указанную задачу так: каково наименьшее число $f(2)$, такое, что любое ограниченное множество Ω на плоскости допускает разбиение на $f(2)$ частей меньшего диаметра? Разумеется, Борсук размышлял не в терминах скорейшего поедания “кривых” тортов, да и вообще, мотивировкой для него служила топологическая проблематика. Подробную и, кстати, весьма интригующую историю задачи можно найти в книге [1].

Еще вопрос: почему мы пишем $f(2)$? А дело в том, что плоскость у нас двумерная. На самом деле, Борсук ставил аналогичную задачу и на прямой (соответствующая величина – $f(1)$), и в пространстве любой размерности. Обычно пространство размерности n обозначают через $\mathbb{R}^n$. В частности, $\mathbb{R}^1 = \mathbb{R}$ – это прямая, $\mathbb{R}^2$ – плоскость, $\mathbb{R}^3$ – пространство в стандартном школьном смысле, т.е. трехмерное пространство, в котором мы живем. В общем случае $f(n)$ – это *число Борсука*, равное такому наименьшему f , что всякое ограниченное множество в $\mathbb{R}^n$ можно разбить на f частей меньшего диаметра, но существует ограниченное множество в $\mathbb{R}^n$, которое на $f - 1$ частей меньшего диаметра не разбивается. При этом расстояния в $\mathbb{R}^n$ меряются стандартно (“по Евклиду”):

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}, \quad \mathbf{x} = (x_1, \dots, x_n), \quad \mathbf{y} = (y_1, \dots, y_n).$$

Борсук предположил, что $f(n) = n + 1$. Это предположение называется *гипотезой Борсука*. Гипотезу с треском опровергли в 1993 году (см. [1], [2]), но осталась куча вопросов, на которые по-прежнему нет ответов.

В следующих разделах мы приведем задачи проекта. Постепенно мы выйдем и на интересные нерешенные проблемы, в которых, однако, вполне возможны серьезные продвижения и на школьном уровне.

2 Задачи до промежуточного финиша

Задача 1. Докажите, что $f(1) = 2$.

Задача 2. Докажите, что $f(2) \geq 3$. Иными словами, приведите пример множества на плоскости, которое на две части меньшего диаметра не разбивается.

Задача 3. Разбейте квадрат на части меньшего диаметра.

Задача 4. Разбейте круг радиуса $1/2$ на 3 части меньшего диаметра.

Задача 5. Разбейте круг радиуса $1/2$ на 3 части, диаметры которых не превосходят величины $\frac{\sqrt{3}}{2} = 0.866\dots$

Задача 6. Докажите, что константа $\frac{\sqrt{3}}{2}$ из задачи 5 неумлучшаема, т.е. при любом разбиении круга радиуса $1/2$ на 3 части найдется часть, диаметр которой не меньше $\frac{\sqrt{3}}{2}$.

Назовем *универсальной покрывшкой* в $\mathbb{R}^n$ такое множество Ω , что для любого множества Φ диаметра 1 в $\mathbb{R}^n$ существует движение пространства, переводящее Φ внутрь Ω . Иными словами, Φ можно так подвинуть, что Ω целиком его покроет. Например:

Задача 7. Докажите, что квадрат со стороной 1 является универсальной покрывшкой на плоскости.

Задача 8. Докажите, что куб со стороной 1 является универсальной покрывшкой в пространстве любой размерности. При этом n -мерным кубом со стороной 1 мы просто считаем множество точек $\mathbf{x} = (x_1, \dots, x_n)$, у которых $x_i \in [0, 1]$ для каждого i .

Известно, что правильный шестиугольник Ω_6 с расстоянием 1 между параллельными сторонами является универсальной покрывшкой. Подробное доказательство этого (не вполне тривиального) факта можно найти в книге [3]. Можете, однако, подумать над этим самостоятельно.

Задача 9. Разбейте правильный шестиугольник Ω_6 на 3 части диаметра $\frac{\sqrt{3}}{2}$. Выведите отсюда справедливость гипотезы Борсука на плоскости, а также, в определенном смысле, “неулучшаемость” константы $\frac{\sqrt{3}}{2}$ из задачи 6.

Задача 10. Что играет роль неулучшаемой константы из задачи 9 в случае прямой?

Задача 11. Докажите, что в любом множестве из n точек на плоскости есть не более n пар точек, расстояние между которыми равно диаметру.

Задача 12. Выведите из задачи 11 справедливость гипотезы Борсука для *конечных* множеств точек на плоскости (не прибегая к помощи покрывшек).

Задача 13*. Докажите, что круг радиуса $\frac{1}{\sqrt{3}}$ является универсальной покрывшкой на плоскости.

Задача 14. Объясните, почему круг радиуса $r < \frac{1}{\sqrt{3}}$ не может быть универсальной покрывшкой.

Задача 15. Объясните, почему результат задачи 13* не позволяет сходу доказать гипотезу Борсука на плоскости.

Задача 16. Возьмем на плоскости круг B_1 радиуса $\frac{1}{\sqrt{3}}$. Поставим произвольную точку на его границе и рассмотрим круг B_2 радиуса 1 с центром в этой точке. Докажите, что $B_1 \cap B_2$ – универсальная покрывшка на плоскости.

Задача 17. С помощью результата задачи 16 докажите гипотезу Борсука.

Задача 18* (исследовательская). Можно ли с помощью результата задачи 16 доказать, что каждое множество на плоскости разбивается на три части диаметра $\leq \frac{\sqrt{3}}{2}$? Какая наилучшая константа такого типа у Вас получается?

Назовем *универсальной покрывающей системой (упс)* в $\mathbb{R}^n$ любую совокупность множеств $\{S_\alpha\}$, обладающих тем свойством, что для всякого $\Omega \subset \mathbb{R}^n$, $\text{diam } \Omega = 1$, существует движение, переводящее Ω внутрь хотя бы одного из множеств S_α .

Задача 19. Рассмотрим правильный шестиугольник Ω_6 с расстоянием 1 между параллельными сторонами. Возьмем отрезок, соединяющий центр шестиугольника с одной из его вершин, и проведем прямую, перпендикулярную этому отрезку, на расстоянии $1/2$ от центра. Прямая отсечет от шестиугольника треугольник. Докажите, что шестиугольник без указанного треугольника также служит универсальной покрывашкой на плоскости. Этот усеченный шестиугольник обозначен Ω'_6 на рисунке 1.

Задача 20. Докажите, что средний и правый шестиугольники с рисунка 1 образуют унс. Треугольники, как и в задаче 19, отсекаются прямыми, которые перпендикулярны отрезкам, соединяющим центр шестиугольника с соответствующими вершинами, и проходят на расстоянии $1/2$ от центра.

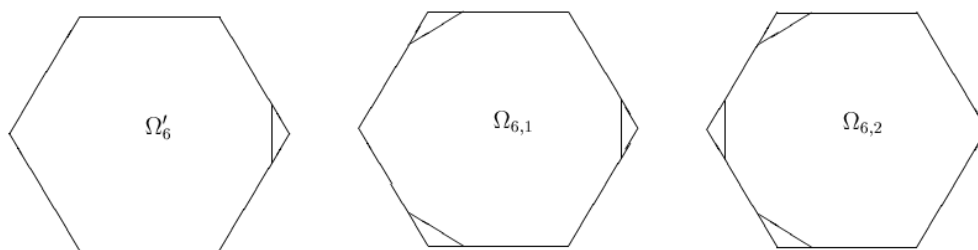


Рисунок 1: Примеры унс.

Задача 21. Докажите, что любое множество диаметра 1 на плоскости можно разбить на 5 частей, в каждой из которых нет пары точек, отстоящих друг от друга на расстояние $\frac{1}{\sqrt{3}}$. **Указание.** Используйте Ω_6 .

Задача 22* (исследовательская). Можно ли доказать, что при некотором $a < \frac{1}{\sqrt{3}}$ любое множество диаметра 1 на плоскости разбивается на 5 частей, в каждой из которых нет пары точек, отстоящих друг от друга на расстояние a ?

Задача 23. Укажите такое n , что любое множество на плоскости можно разбить на n частей, в каждой из которых нет пары точек, отстоящих друг от друга на расстояние 1. Какое наименьшее n Вы можете указать?

Задача 24*. Докажите, что всякое множество диаметра 1 на плоскости разбивается на 6 частей, диаметры которых не превосходят величины $\sqrt{\frac{13}{3}}(2 - \sqrt{3}) = 0.5577\dots$ **Указание.** Используйте унс $\{\Omega_{6,1}, \Omega_{6,2}\}$.

Задача 25.** А еще лучше, чем в задаче 24*?

Задача 26*. Докажите, что всякое множество диаметра 1 на плоскости разбивается на 5 частей, диаметры которых не превосходят величины 0.603. **Указание.** Используйте покрывашку Ω'_6 .

Задача 27.** А еще лучше, чем в задаче 26*?

Задача 28. Докажите, что всякое множество диаметра 1 на плоскости разбивается на 4 части, диаметры которых не превосходят величины $\frac{1}{\sqrt{2}}$.

Задача 29. Докажите неулучшаемость результата задачи 28.

Задача 30. Докажите, что всякое множество диаметра 1 на плоскости разбивается на 7 частей, диаметры которых не превосходят величины $\frac{1}{2}$.

Задача 31. Докажите неулучшаемость результата задачи 30.

3 Задачи после промежуточного финиша.

Задача 32. Докажите, что $f(3) \geq 4$.

Задача 33*. Докажите, что шар радиуса $\sqrt{\frac{3}{8}}$ является универсальной покрывкой в $\mathbb{R}^3$.

Задача 34. Объясните, почему шар радиуса $r < \sqrt{\frac{3}{8}}$ не является универсальной покрывкой в $\mathbb{R}^3$.

Задача 35. Разбейте шар радиуса $1/2$ в пространстве на 4 части меньшего диаметра (т.е. диаметры частей должны быть меньше 1).

Задача 36*. Впишем в шар радиуса $1/2$ правильный тетраэдр. Рассмотрим 4 трехгранных угла, которые получаются, если соединять центр шара с вершинами граней тетраэдра. Пересечем каждый из углов с шаром. Получится разбиение шара на 4 одинаковых части. Найдите диаметры этих частей.

Задача 37. Назовем *правильным симплексом* в $\mathbb{R}^n$ аналог правильного треугольника на плоскости и правильного тетраэдра в пространстве. А именно, рассмотрим $n + 1$ точек $\mathbf{x}_1, \dots, \mathbf{x}_{n+1}$ в $\mathbb{R}^n$, обладающих тем свойством, что $|\mathbf{x}_i - \mathbf{x}_j| = a$ для всех пар $i \neq j$ и некоторого $a > 0$. Докажите, что симплекс существует.

Задача 38*. Назовем n -мерным шаром множество

$$B = \{\mathbf{x} = (x_1, \dots, x_n) : x_1^2 + \dots + x_n^2 \leq 1\}.$$

Это шар радиуса 1 и диаметра 2. Впишем в этот шар правильный симплекс. Найдите длину его стороны.

Задача 39.** Осуществим разбиение шара из задачи 38*, аналогичное разбиению из задачи 36*. А именно, впишем в шар правильный симплекс с длиной стороны, найденной в задаче 38*, и рассмотрим многогранные углы с вершиной в центре шара, проходящие через грани симплекса (граней $n + 1$). Найдите диаметры полученных частей. В частности, убедитесь, что они меньше 2 и что их величины стремятся к 2 при $n \rightarrow \infty$.

Задача 40. Возьмем шар B_1 радиуса $\sqrt{\frac{3}{8}}$ и пересечем его с произвольным шаром B_2 радиуса 1, центр которого расположен на границе шара B_1 . Докажите, что $B_1 \cap B_2$ – универсальная покрывка в $\mathbb{R}^3$.

Задача 41*. Докажите, что $B_1 \cap B_2$ разбивается на 5 частей диаметра меньше 1.

Задача 42. Докажите, что $f(4) \geq 5$. Вообще, $f(n) \geq n + 1$.

Задача 43. Найдите какую-нибудь верхнюю оценку для $f(4)$.

Задача 44. Найдите какую-нибудь верхнюю оценку для $f(n)$.

Задача 45. Постройте покрывку в $\mathbb{R}^4$, аналогичную покрывкам из задач 40 и 16 из первого списка.

Задача 46*. Докажите, что покрывка из задачи 45 разбивается на 9 частей диаметра меньше 1 и что, стало быть, $f(4) \leq 9$.

4 Решения

При решении задач проекта школьниками был получен ряд ярких и неожиданных результатов. Прежде всего стоит отметить результат Егора Воронцовского, которому удалось улучшить ранее известные верхние оценки минимальной величины запрещенного расстояния между точками одного цвета в раскраске произвольного плоского множества диаметра 1 в четыре и пять цветов. Если раньше были оценки величинами $\frac{1}{\sqrt{2}}$ и $\frac{1}{\sqrt{3}}$, то теперь, благодаря Егору, мы имеем оценки величинами $\frac{1}{\sqrt{3}}$ и $\frac{1-\sqrt{3}+\sqrt{6\sqrt{3}}}{4\sqrt{3}-2}$. Конструкции Егора мы приводим ниже. Также хочется сказать о новой верхней оценке минимального диаметра в разбиении произвольного плоского множества диаметра 1 на шесть частей. Эту оценку независимо получили Дима Белов с Никитой Александровым и How Si Wei. Если прежняя оценка имела величину $0.557\dots$, то нынешняя равна $0.542\dots$. Эти конструкции мы также приводим ниже. В то же время некоторые школьники показали настолько высокую математическую культуру, что это позволило им аккуратно подсчитать диаметры частей в разбиении n -мерного шара на $n+1$ часть (задача 8** из второй части проекта), а также передоказать теорему М. Лассака, опубликованную в 1982 году и утверждающую, что каждое множество диаметра 1 в $\mathbb{R}^n$ можно разбить на $2^{n-1}+1$ часть диаметра < 1 . И разбиение шара, и доказательство теоремы Лассака выполнили Егор Воронцовский и Максим Дидин.

1. Очевидно $f(1) > 1$. Так как любое множество диаметра 1 на прямой можно поместить внутри отрезка длины 1, то достаточно разбить отрезок на части меньшего диаметра: например, пополам.
2. Например, равносторонний треугольник.
3. Это можно сделать, например, проведя один вертикальный разрез.
5. Можно разрезать круг тремя радиусами, углы между которыми равны 120° .
6. Пусть круг разрезан на три части. Возьмём точку на границе круга, которая принадлежит двум из этих множеств и построим равносторонний треугольник с одной вершиной в выбранной точке, а двумя другими — на границе круга. Тогда две вершины этого треугольника принадлежат одной части. Значит, диаметр этой части не меньше $\frac{\sqrt{3}}{2}$.
8. Очевидно, что множество Ω диаметра 1 лежит внутри полосы $\min_{x \in \Omega} x_i \leq x_i \leq \max_{x \in \Omega} x_i$, ширина которой меньше 1. Пересечение таких полос для всех i — это параллелепипед, который покрывается единичным кубом.
9. Разрежем шестиугольник на три части перпендикулярами из центра к трём несмежным сторонам шестиугольника. Диаметр каждой части равен $\frac{\sqrt{3}}{2}$. Теперь поместим множество диаметра 1 внутрь шестиугольника Ω_6 . Это множество также разобьётся на части диаметра не больше $\frac{\sqrt{3}}{2} < 1$. А как мы знаем из задачи 6, константа $\frac{\sqrt{3}}{2}$ неулучшаема в случае круга диаметра 1.
10. Любое множество диаметра 1 на прямой можно разбить на части диаметра $\leq \frac{1}{2}$, а отрезок длины 1 лучше разрезать нельзя.
11. Соединим ребром пары точек, расстояние между которыми равно 1. Если из каждой точки выходит не более двух рёбер, то всего не более n рёбер. Тогда рассмотрим тройку рёбер с общим концом. Так как расстояния между точками не более 1, то угол между рёбрами не превосходит 60° .
Из другого конца среднего ребра не может выходить ребро, иначе бы его конец был бы на расстоянии больше 1 от одного из концов рёбер. Потому можно выкинуть среднее ребро вместе с его концом (необщим) и продолжить доказательство по индукции.
12. Достаточно покрасить вершины графа из решения предыдущей задачи в три цвета так, чтобы вершины одного цвета не были соединены ребром. Сделаем это по индукции. Если есть висячая вершина, то выкинем её, оставшийся граф раскрасим по предположению индукции, а её — в цвет, отличный от цвета её соседа. Если нет висячей вершины, то из всех вершин выходит два ребра, а значит, мы имеем набор циклов, каждый из которых можно покрасить в три цвета требуемым образом.

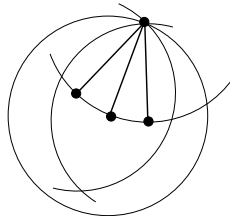


Рисунок 2: Три ребра с общим концом.

13. *Первое решение.* Поместим множество диаметра 1 внутрь некоторого большого круга, а потом будем уменьшать круг, так чтобы он содержал исходное множество. Как только на границу круга попадают точки из данного множества, будем уменьшать круг далее так, чтобы эти точки оставались на границе круга. Мы больше не сможем уменьшать круг в одном из двух случаев:

- 1) концы диаметра круга принадлежат исходному множеству, а значит, диаметр круга не больше 1;
- 2) круг описан вокруг некоторых трёх точек исходного множества, которые образуют остроугольный треугольник.

Как известно, среди остроугольных треугольников со сторонами не более 1 максимальный радиус описанной окружности у равностороннего. А значит, исходное множество можно поместить в круг радиуса $\frac{1}{\sqrt{3}}$.

Второе решение. Так как вписанный в круг правильный шестиугольник является универсальной покрывкой, то сам круг — также универсальная покрывка.

14. Пусть равносторонний треугольник со стороной 1 поместили в круг радиуса r , тогда будем уменьшать круг, как в решении прошлой задачи. В конце мы получим описанный вокруг треугольника круг. Значит, $r \geq \frac{1}{\sqrt{3}}$.

15. По задаче 6, если круг радиуса $\frac{1}{\sqrt{3}}$ разрезан на три части, то диаметр одной из частей не менее 1.

16. Пусть дано некоторое множество диаметра 1. По задаче 13 поместим его в круг B_1 радиуса $\frac{1}{\sqrt{3}}$. После этого сдвинем его немного, чтобы одна из его точек X попала на границу круга, но при этом само множество оставалось внутри B_1 . Проведём круг B_2 радиуса 1 с центром X . Так как множество имеет диаметр 1, то проведённый круг содержит наше множество. А значит, пересечение $B_1 \cap B_2$ также покрывает исходное множество.

17. Покрывку из задачи 16 можно разрезать на три части диаметра $c = \frac{\sqrt{3}}{2} + \frac{\sqrt{\frac{2}{\sqrt{3}}}-1}{2} < 1$. На рисунке O_1 — центр окружности радиуса $\frac{1}{\sqrt{3}}$, O_2 — центр окружности радиуса 1, B — середина дуги окружности радиуса 1, а точки A и C выбраны так, чтобы треугольник ABC был равносторонним. Нетрудно посчитать, что его сторона равняется $\frac{\sqrt{3}}{2} + \frac{\sqrt{\frac{2}{\sqrt{3}}}-1}{2}$.

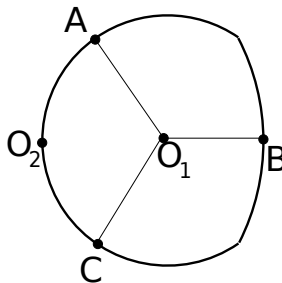


Рисунок 3: Разрезание покрывки из задачи 16.

Далее гипотеза Борсука доказывается аналогично решению задачи 9.

18. Докажем, что покрывку $B_1 \cap B_2$ нельзя разбить на три части диаметра меньше, чем c , где c определялось в решении прошлой задачи. Сначала докажем лемму.

Лемма. Для каждой точки X границы $B_1 \cap B_2$ найдётся равносторонний треугольник с вершиной в точке X , а другими двумя — на границе $B_1 \cap B_2$, причём сторона любого такого треугольника не меньше c .

Доказательство. Повернём границу $B_1 \cap B_2$ относительно X на 60° по часовой стрелке и против, и повернутое пересечём с границей $B_1 \cap B_2$. Полученные точки пересечения будут вершинами искомого треугольника. Ровно одна вершина этого треугольника попадёт на дугу окружности радиуса 1: если ни одна вершина не попала на эту дугу, то имеем вписанный угол $< 60^\circ$, если попали две — $< 60^\circ$. На рисунке O_1 — центр окружности радиуса $\frac{1}{\sqrt{3}}$, O_2 — центр окружности радиуса 1, ABC — равносторонний треугольник, причём вершина B лежит на дуге окружности радиуса 1, а остальные — нет.

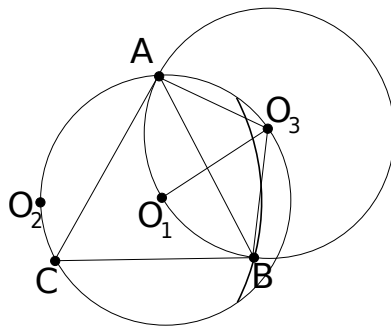


Рисунок 4: Равносторонний треугольник на границе покрывки из задачи 16.

O_3 — центр окружности, полученной поворотом на 60° относительно точки A из окружности с центром O_1 . Поэтому точки O_1 и B лежат на окружности с центром O_3 . То есть $O_3A = O_3B = \frac{1}{\sqrt{3}}$. Значит, AB тем меньше, чем меньше угол AO_3B . Но $BO_3O_1 = 60^\circ$. Значит, угол AO_3B тем меньше, чем меньше угол O_1O_3B . Также $O_3O_1 = O_3B = \frac{1}{\sqrt{3}}$. Значит, угол O_1O_3B тем меньше, чем меньше O_1B , которое в свою очередь минимально, если B — середина дуги окружности радиуса 1. Значит, $AB \geq c$.

Теперь вернёмся к решению задачи. Пусть $B_1 \cap B_2$ разбито на три части. Возьмём точку X на границе, которая принадлежит двум частям. Применим лемму для точки X . В найденном треугольнике какие-то две вершины принадлежат одной части, а расстояние между ними не меньше c . Значит, диаметр этой части не меньше c .

19. Рассмотрим два маленьких треугольника, которые находятся в противоположных вершинах шестиугольника. Между любыми двумя точками этих треугольников расстояние не меньше 1. Значит, если множество диаметра 1 лежит внутри шестиугольника, то один из этих треугольников можно отрезать, не задев множества.

20. Как было замечено в прошлой задаче один из двух противоположных маленьких треугольников можно отрезать, не задев множества диаметра 1 внутри шестиугольника. Сделаем так со всеми тремя парами треугольников. Получим один из шестиугольников на рисунке.

21. Решение предложил участник конференции Егор Воронцовский. Достаточно разрезать правильный шестиугольник со стороной $\frac{1}{\sqrt{3}}$. Однако, его можно разрезать даже на четыре части!

В центре рисунка расположен треугольник Рело диаметра $\frac{1}{\sqrt{3}}$. Нетрудно посчитать, что $AB = \frac{1}{\sqrt{3}}$. Дуге CD припишем зелёный цвет, но вершине C — голубой. Дугам AC и BC — голубой, но вершинам A и B — красный и жёлтый соответственно. Цвет остальных дуг и вершин определяется аналогично с помощью поворота на 120° .

22. Решение предложил участник конференции Егор Воронцовский. Разрежем шестиугольник аналогично предыдущему решению, только диаметр треугольника Рело выберем равным AB (см. рис.6).

На рисунке поменяли цвет лишь точки внутри синей части, цвет остальных точек остался прежним.

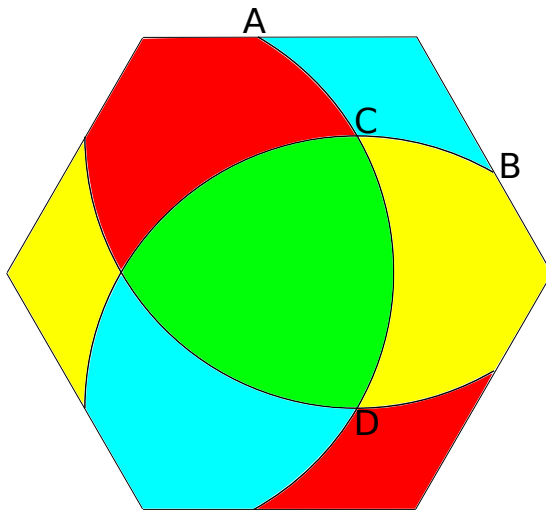


Рисунок 5: На расстоянии $\frac{1}{\sqrt{3}}$ нет точек одного цвета.

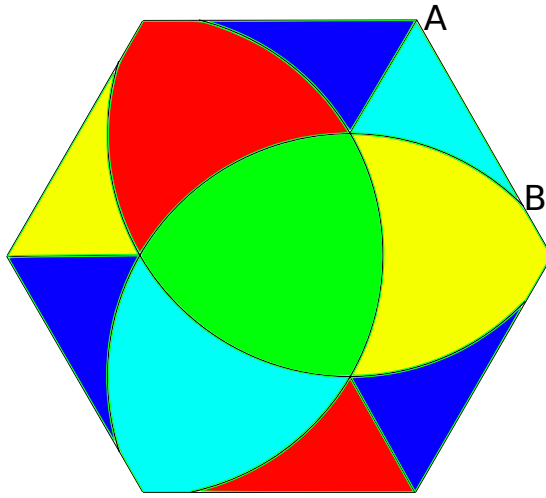


Рисунок 6: На расстоянии $\frac{1-\sqrt{3}+\sqrt{6\sqrt{3}}}{4\sqrt{3}-2}$ нет точек одного цвета.

23. Эта задача эквивалентна проблеме о хроматическом числе плоскости и до сих пор не решена. Пока неизвестно можно ли раскрасить плоскость меньше, чем в семь цветов: шестиугольники правильной шестиугольной решётки можно раскрасить в 7 цветов так, чтобы соседние шестиугольники были разного цвета.

24. Введём обозначение $\sigma = \sqrt{\frac{13}{3}} (2 - \sqrt{3})$ и убедимся, что шестиугольники $\Omega_{6,1}$ и $\Omega_{6,2}$ можно разрезать на части диаметра не более σ . По задаче 20 этого достаточно для доказательства.

Начнём с шестиугольника $\Omega_{6,1}$.

Пусть $\Omega_{6,1}$ получается из правильного шестиугольника $ABCDEF$ с серединами сторон $M_1, \dots, M_6$ и центром O отсечением треугольников BB_1B_2 , DD_1D_2 и FF_1F_2 (см. рис. 7). Отложим на лучах AO, CO, EO отрезки AX, CY, EZ длины $1/2$ и проведём отрезки OX, OY, OZ . Далее, соединим каждую из точек X, Y, Z с двумя серединами сторон шестиугольника, как на рисунке. Тем самым, задано покрытие $\Omega_{6,1}$ шестью многоугольниками $OXM_1B_2B_1M_2Y$, AM_1XM_6 и т.д.

Убедимся, что их диаметры не превосходят σ .

Действительно, $AX = M_1M_6 = \frac{1}{2}$, а значит, диаметр четырёхугольника AM_1XM_6 равен $\frac{1}{2}$. Диаметр семиугольника $OXM_1B_1B_2M_2Y$, как легко проверить, равен $OB_1 = \frac{1}{2 \cos \frac{\pi}{12}} \approx 0.5176$. Остальные множества покрытия получаются из этих двух поворотами и поэтому имеют такие же диаметры.

Теперь разрежем шестиугольник $\Omega_{6,2}$.

Пусть $\Omega_{6,2}$ получается из правильного шестиугольника $ABCDEF$ с центром O отсечением треугольников AA_1A_2 , BB_1B_2 и FF_1F_2 (см. рис. 8). Пусть точка M — середина отрезка A_1A_2 , а серединный перпендикуляр к отрезку A_1C пересекает отрезок AD в точке J . Очевидно, $JA_1 = JC$.

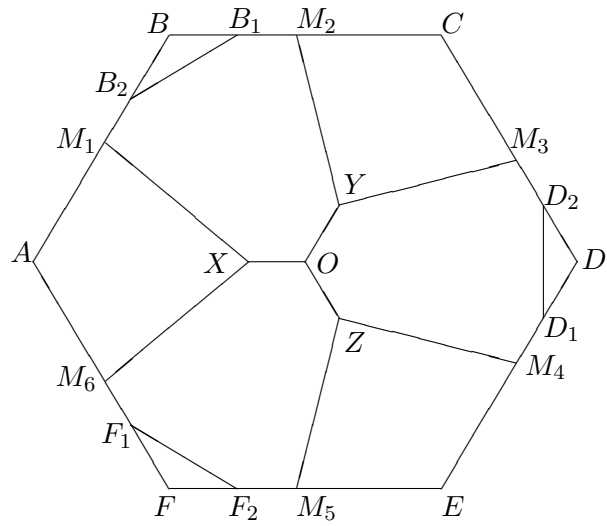


Рисунок 7:

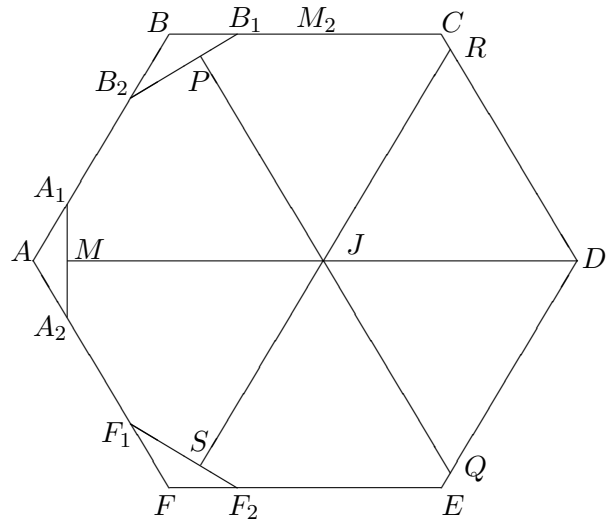


Рисунок 8:

Проведём через точку J прямые, параллельные диагоналям BE и CF шестиугольника. Пусть они высекают на $\Omega_{6,2}$ отрезки PQ и RS (см. рис. 8). Итак, мы получили разбиение $\Omega_{6,2}$ на шесть многоугольников.

Проверим, что диаметр каждого из них не превосходит σ .

Заметим сначала, что $JA_1 = JC = \sigma$.

Действительно, равенство $JA_1^2 = JC^2$ в силу теоремы Пифагора для треугольников JMA_1 и JM_2C (точка M_2 — середина BC) равносильно

$$\left(OJ + \frac{1}{2}\right)^2 + \left(\frac{\operatorname{tg} \frac{\pi}{12}}{2}\right)^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2\sqrt{3}} - OJ\right)^2,$$

откуда находим

$$OJ = \frac{1 - 3 \operatorname{tg}^2 \frac{\pi}{12}}{4(3 + \sqrt{3})}.$$

Теперь длину отрезка JA_1 можно найти по теореме Пифагора из треугольника JMA_1 .

Несложные вычисления показывают, что диаметры пятиугольников JMA_1B_2P и JPB_1CR равны $JA_2 = JC = \sigma$, а диаметр равностороннего треугольника JRD меньше σ . Множества покрытия разбиваются на пары симметричных относительно прямой MD , что завершает доказательство.

25. Решение предложили две команды: Александров Никита с Беловым Димой и How Si Wei. Разрежем элементы упс. Сначала разрежем многоугольник на рисунке 9. Рисунок симметричен относительно поворота

на 120° и $BT = \sqrt{2 - \sqrt{3}}$. В этом случае диаметры всех частей равны $\sqrt{2 - \sqrt{3}}$.

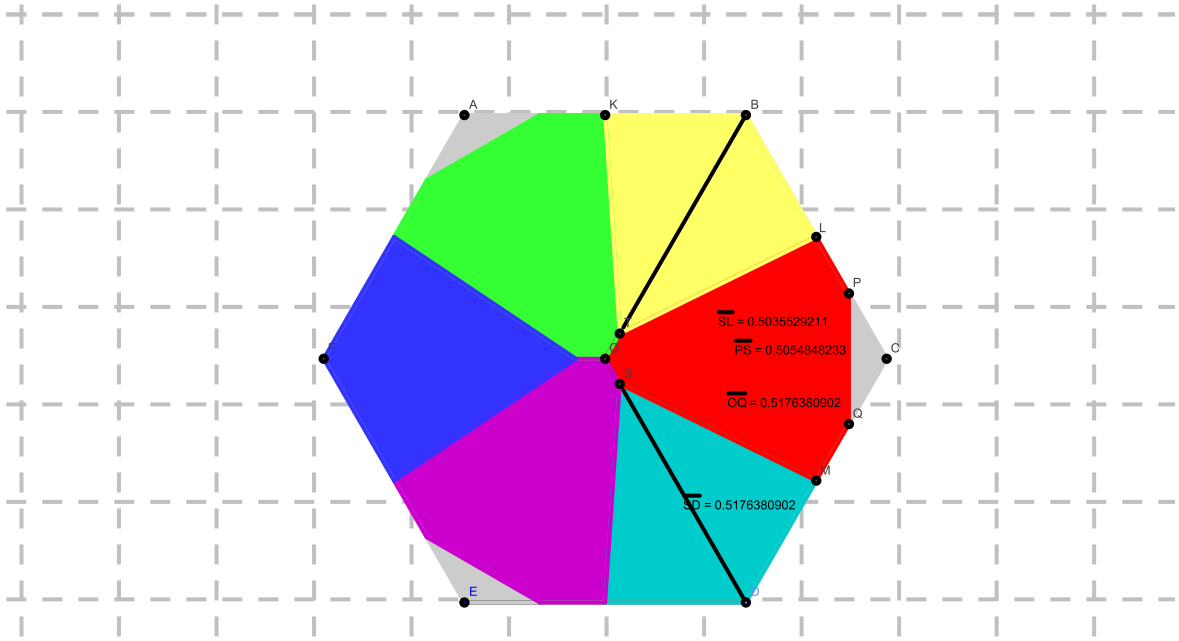


Рисунок 9: Диаметры всех частей равны $\sqrt{2 - \sqrt{3}}$.

Перейдём к рисунку 10. Точка T лежит на диагонали AD и $ST = TD$. Также $AA_1 = EV = CU' = \sqrt{2 - \sqrt{3}}$. Точка W выбрана на отрезке VD так, чтобы TW было параллельно CD . Точка Z определяется аналогично. Точки M', N, P', Q', K и L' — основания перпендикуляров, опущенных из точки T . Вычисления показывают, что диаметр частей не превосходит $TD = \frac{10-4\sqrt{3}}{5\sqrt{3}-3} \approx 0,5427$.

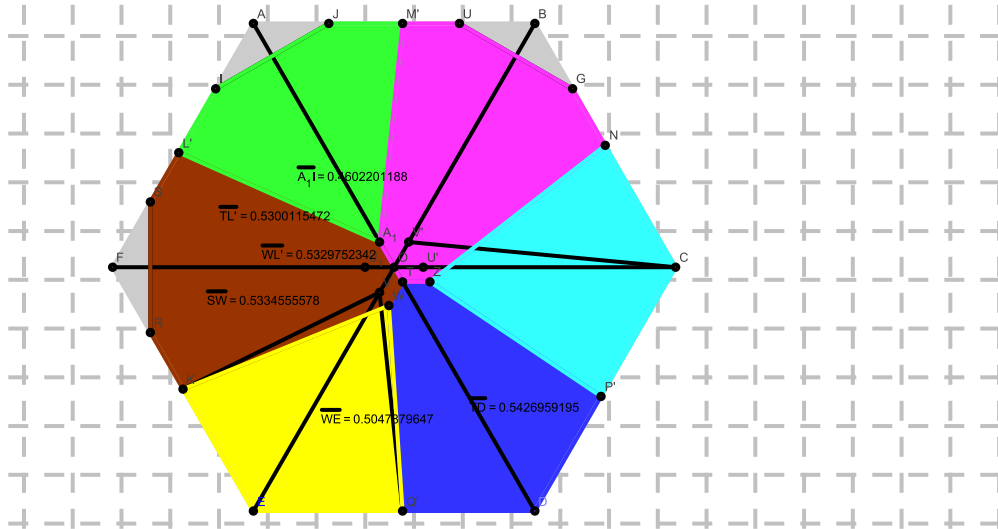


Рисунок 10: Диаметры частей не превосходят TD .

26. Опишем необходимое разрезание Ω'_6 на пять множеств.

Рассмотрим на сторонах BC , CD , DE и EF точки X , Y , Z и T соответственно такие, что все стороны пятиугольника $MXYZT$ равны (см. рис. 11).

Это можно сделать единственным образом очевидно.

Обозначим длину отрезка MX через ρ'_5 . Можно убедиться, что $\rho'_5 = 0.6020 \dots$

Соединим точку O с каждой из вершин $MXYZT$. Этим задано покрытие Ω'_6 пятью многоугольниками.

Очевидно, что расстояние от точки O до произвольной точки границы Ω'_6 не превосходит $\frac{1}{\sqrt{3}} < \rho'_5$, а значит, диаметры всех многоугольников покрытия равны ρ'_5 .

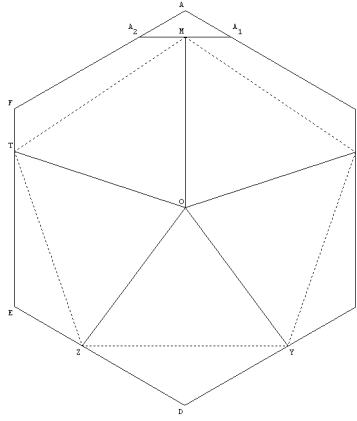


Рисунок 11:

27. ?

28. По задаче 7 достаточно разрезать квадрат со стороной 1 на четыре части диаметра $\frac{1}{\sqrt{2}}$. Это можно сделать, проведя диагонали.

29. Докажем, что круг диаметра 1 нельзя разрезать на четыре части диаметра не более $\frac{1}{\sqrt{2}}$. Допустим можно. Возьмём точку на границе, которая принадлежит сразу двум частям. Отстроим от неё квадрат с вершинами на окружности круга. Его сторона равна $\frac{1}{\sqrt{2}}$. Некоторые две вершины этого квадрата принадлежат одной части, противоречие.

30. Так как шестиугольник со стороной $\frac{1}{\sqrt{3}}$ является универсальной покрывшкой, то достаточно его разрезать на семь частей диаметра $\frac{1}{2}$:

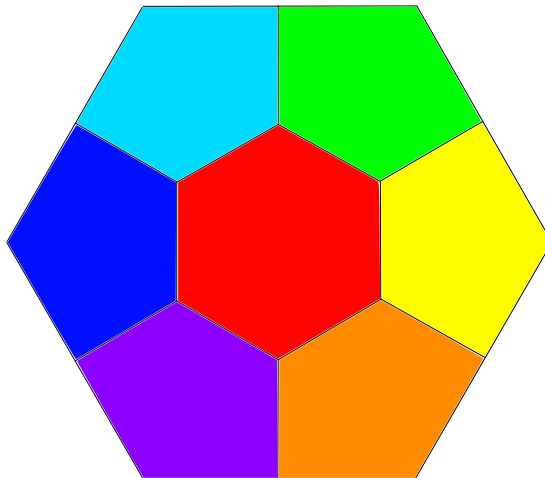


Рисунок 12: Наибольшие диагонали шестиугольника и пятиугольников равны $\frac{1}{2}$.

31. Докажем, что круг диаметра 1 нельзя разрезать на семь частей диаметра не более $\frac{1}{2}$. Допустим можно. Возьмём точку на границе, которая принадлежит сразу двум частям. Отстроим от неё правильный шестиугольник с вершинами на окружности круга. Его сторона равна $\frac{1}{2}$. Рассмотрим семь точек: вершины шестиугольника и его центр. Некоторые две из них принадлежат одной части, противоречие.

32. Правильный тетраэдр нельзя разрезать на три части меньшего диаметра, потому что его вершины должны принадлежать разным частям.

33. Решение аналогично первому решению задачи 13. Поместим множество диаметра 1 внутрь некоторого большого шара, а потом будем уменьшать этот шар, так чтобы он содержал исходное множество. Как только на границу шара попадают точки из данного множества, будем уменьшать шар далее так, чтобы эти точки оставались на границе шара. Мы больше не сможем уменьшать шар в одном из трёх случаев:

1) концы некоторого диаметра шара принадлежат исходному множеству, а значит, диаметр шара не больше 1;

2) некоторые три точки исходного множества лежат на экваторе шара и образуют остроугольный треугольник, в этом случае радиус шара не превосходит $\frac{1}{\sqrt{3}}$;

3) некоторые четыре точки исходного множества лежат на границе шара и образуют тетраэдр, который содержит центр шара.

Осталось доказать, что в четвёртом случае радиус шара не превосходит $\sqrt{\frac{3}{8}}$. Это следует из леммы.

Лемма. У тетраэдра, вписанного в сферу радиуса 1 и содержащего её центр, наибольшая сторона не короче $\sqrt{\frac{8}{3}}$. Если при этом тетраэдр правильный, то его стороны равны $\sqrt{\frac{8}{3}}$.

Доказательство. Пусть O — центр сферы, а $ABCD$ — некоторый тетраэдр, вписанный в неё. Так как O лежит внутри тетраэдра, то

$$a \cdot \overrightarrow{OA} + b \cdot \overrightarrow{OB} + c \cdot \overrightarrow{OC} + d \cdot \overrightarrow{OD} = \vec{0}$$

для некоторых положительных чисел a, b, c, d . Пусть a — наибольшее из них. Тогда умножим обе части этого векторного равенства скалярно на вектор $\overrightarrow{OA}$. Получим

$$a \cdot \overrightarrow{OA} \cdot \overrightarrow{OA} + b \cdot \overrightarrow{OB} \cdot \overrightarrow{OA} + c \cdot \overrightarrow{OC} \cdot \overrightarrow{OA} + d \cdot \overrightarrow{OD} \cdot \overrightarrow{OA} = 0.$$

Так как a максимально, то $\overrightarrow{OA} \cdot \overrightarrow{OX} < -\frac{1}{3} \overrightarrow{OA} \cdot \overrightarrow{OA}$, где $X = B, C$ или D . Можно считать, что $X = B$. Так как $OA = OB = 1$, то по теореме косинусов $AB \geq \sqrt{\frac{8}{3}}$. А в случае правильного тетраэдра равенство достигается.

34. Пусть правильный тетраэдр со стороной 1 поместили в шар радиуса r , тогда будем уменьшать шар, как в решении прошлой задачи. В конце мы получим описанный вокруг тетраэдра шар. Значит, $r \geq \sqrt{\frac{3}{8}}$.

36. Пусть вершины тетраэдра — это A_1, A_2, A_3, A_4 , а его центр — это O . Для определенности рассмотрим множество, порожденное трехгранным углом $OA_1A_2A_3$. Пусть B — середина стороны A_2A_3 . Проведем радиус OB . Обозначим через C его конец, лежащий на сфере. Утверждение состоит в том, что диаметр — это длина отрезка A_1C . Мы не станем доказывать этот несложный факт, оставляя читателю хорошую пищу для размышлений.

По прошлой задаче сторона тетраэдра равна $\sqrt{\frac{2}{3}}$. По теореме Пифагора для треугольников A_1BA_2 и $OB A_2$ находим $|A_1B| = \sqrt{\frac{1}{2}}$, и $|OB| = \sqrt{\frac{1}{12}}$. По теореме косинусов косинус угла A_1OB равен $-\sqrt{\frac{1}{3}}$.

Берем треугольник A_1OC , и по теореме косинусов находим

$$|A_1C| = \sqrt{\frac{3 + \sqrt{3}}{6}} \approx 0.888... < 1.$$

37. Докажем по индукции по n . Пусть в плоскости $x_{n+1} = 0$ построен правильный n -мерный симплекс T . Пусть его центр находится в начале координат. Тогда ось x_{n+1} равноудалена от вершин симплекса T . Значит, на ней найдётся точка X , от которой расстояния до вершин T равны a . Симплекс, построенный на T , как на основании, с вершиной X является правильным. Его центр находится на оси x_{n+1} , который можно найти по теореме Пифагора.

39. Сперва напомним ряд сведений из геометрии. Скалярным произведением векторов $\mathbf{x} = (x_1, x_2)$ и $\mathbf{y} = (y_1, y_2)$ называется число $(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2$. Расстояние $|\mathbf{x} - \mathbf{y}|$ между точками $\mathbf{x}, \mathbf{y}$ можно измерить по формуле

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Запись $(\mathbf{x}, \mathbf{x})$ называется скалярным квадратом вектора $\mathbf{x}$. Она выражает квадрат длины $|\mathbf{x}|$ этого вектора. Косинус угла между векторами $\mathbf{x}, \mathbf{y}$ можно вычислить по формуле $\frac{(\mathbf{x}, \mathbf{y})}{|\mathbf{x}| \cdot |\mathbf{y}|}$. Таким образом, соотношение (2) — это просто теорема косинусов:

$$|\mathbf{x} - \mathbf{y}|^2 = |\mathbf{x}|^2 + |\mathbf{y}|^2 - 2|\mathbf{x}| \cdot |\mathbf{y}| \cdot \cos(\hat{\mathbf{x}}, \mathbf{y}). \quad (1')$$

Абсолютно то же самое можно сказать и про $\mathbb{R}^d$, где скалярное произведение векторов $\mathbf{x} = (x_1, \dots, x_d)$, $\mathbf{y} = (y_1, \dots, y_d)$ задается выражением

$$(\mathbf{x}, \mathbf{y}) = x_1 y_1 + \dots + x_d y_d.$$

Что ж, вычислим диаметр одной из частей D , порожденной вершинами $\mathbf{x}_1, \dots, \mathbf{x}_d$ симплекса T . Нетрудно заметить, что $\mathbf{x}_1 + \dots + \mathbf{x}_{d+1} = \mathbf{0}$ (ср. двумерный и трехмерный случаи). Значит,

$$(\mathbf{x}_1, \mathbf{x}_i) + \dots + (\mathbf{x}_{d+1}, \mathbf{x}_i) = (\mathbf{0}, \mathbf{x}_i) = 0$$

для любого i . Поскольку, далее, $|\mathbf{x}_1| = \dots = |\mathbf{x}_{d+1}| = 1$ (все вершины симплекса лежат на нашей сфере радиуса 1), имеем $(\mathbf{x}_i, \mathbf{x}_i) = 1$. Наконец, из соображений симметрии следует, что все углы $(\mathbf{x}_j, \mathbf{x}_i)$ при $i \neq j$ равны между собой. Стало быть, при $i \neq j$ получаем

$$0 = (\mathbf{x}_1, \mathbf{x}_i) + \dots + (\mathbf{x}_{d+1}, \mathbf{x}_i) = 1 + d(\mathbf{x}_j, \mathbf{x}_i),$$

т.е. для всех $i \neq j$ выполнено $(\mathbf{x}_j, \mathbf{x}_i) = -\frac{1}{d}$.

Заметим, что последнее наблюдение сразу же позволяет нам найти длину стороны симплекса T (расстояние между любыми двумя его вершинами). По теореме косинусов (соотношение (1')) имеем

$$|\mathbf{x}_i - \mathbf{x}_j|^2 = 1 + 1 - 2 \cdot 1 \cdot 1 \cdot \left(-\frac{1}{d}\right) = 2 + \frac{2}{d}, \quad |\mathbf{x}_i - \mathbf{x}_j| = \sqrt{\frac{2d+2}{d}}.$$

В частности, при $d = 2$ получается $\sqrt{3}$, а при $d = 3$ выходит $2\sqrt{\frac{2}{3}}$.

Вернемся к поиску диаметра. Здесь есть два случая: $d = 2k$ и $d = 2k - 1$. Рассмотрим их по отдельности.

Случай 1. Возьмем точки $\xi = \mathbf{x}_1 + \dots + \mathbf{x}_k$ и $\eta = \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k}$. Эти точки при $k > 1$ не принадлежат интересующему нас множеству D , но сперва мы поработаем с ними. Итак,

$$\cos(\hat{\xi}, \eta) = \frac{(\mathbf{x}_1 + \dots + \mathbf{x}_k, \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k})}{|\mathbf{x}_1 + \dots + \mathbf{x}_k| \cdot |\mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k}|} = \frac{(\mathbf{x}_1 + \dots + \mathbf{x}_k, \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k})}{|\mathbf{x}_1 + \dots + \mathbf{x}_k|^2}.$$

Числитель в последнем выражении представляет собой (после раскрытия скобок) сумму k^2 слагаемых, каждое из которых есть $(\mathbf{x}_i, \mathbf{x}_j)$ с разными i и j . Значит, числитель равен $k^2 \cdot \left(-\frac{1}{2k}\right) = -\frac{k}{2}$. Перепишем знаменатель:

$$|\mathbf{x}_1 + \dots + \mathbf{x}_k|^2 = |\mathbf{x}_1|^2 + \dots + |\mathbf{x}_k|^2 + \sum_{i \neq j} (\mathbf{x}_i, \mathbf{x}_j) = k + k \cdot (k-1) \cdot \left(-\frac{1}{2k}\right) = k - \frac{k-1}{2} = \frac{k+1}{2}.$$

В итоге

$$\cos(\hat{\xi}, \eta) = -\frac{k}{k+1}.$$

Положим теперь $\xi' = \frac{\xi}{|\xi|}$, $\eta' = \frac{\eta}{|\eta|}$. Эти точки уже лежат на сфере, и, более того, обе они находятся в множестве D . По теореме косинусов расстояние между ними равно величине

$$|\xi' - \eta'| = \sqrt{|\xi'|^2 + |\eta'|^2 - 2 \cdot |\xi'| \cdot |\eta'| \cdot \cos(\hat{\xi}, \eta)} = \sqrt{2 - 2 \cos(\hat{\xi}, \eta)} = \sqrt{2 + \frac{2k}{k+1}}.$$

В случае 1 диаметр мы нашли. Отметим, что при $k = 1$ (т.е. в размерности 2) $\xi' = \mathbf{x}_1$, $\eta' = \mathbf{x}_2$, т.е., действительно, диаметр достигается на стороне. Однако при $k > 1$ длина стороны равна

$$\sqrt{\frac{4k+2}{2k}} = \sqrt{2 + \frac{1}{k}} < \sqrt{2 + \frac{2k}{k+1}}.$$

Более того, длина стороны стремится с ростом k к корню из двух, а диаметр множества D стремится к двум, т.е. к диаметру всей сферы (оставаясь всегда чуть меньше двойки).

Случай 2. Возьмем точки $\xi = \mathbf{x}_1 + \dots + \mathbf{x}_k$ и $\eta = \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k-1}$. Опуская выкладки, которые полностью аналогичны выкладкам из случая 1, получаем

$$\cos(\hat{\xi}, \eta) = -\sqrt{\frac{k-1}{k+1}}.$$

Снова полагая $\xi' = \frac{\xi}{|\xi|} \in D$, $\eta' = \frac{\eta}{|\eta|} \in D$, имеем окончательно

$$|\xi' - \eta'| = \sqrt{2 + 2\sqrt{\frac{k-1}{k+1}}}.$$

В случае $k = 2$ (т.е. при $d = 3$) выполнено

$$\sqrt{2 + 2\sqrt{\frac{k-1}{k+1}}} = \sqrt{2 + 2\sqrt{\frac{1}{3}}} = \sqrt{2 + \frac{2\sqrt{3}}{3}} = \sqrt{2 \cdot \frac{3 + \sqrt{3}}{3}} = 2\sqrt{\frac{3 + \sqrt{3}}{6}}.$$

В точности то же, что и в задаче 36! Нетрудно заодно осознать и тот факт, что точки ξ' и η' суть, в обозначениях решения задачи 36, точки C и A_1 соответственно. Такая вот (вполне ожидаемая) аналогия.

40. Пусть дано некоторое множество диаметра 1. По задаче 33 поместим его в шар радиуса $\sqrt{\frac{3}{8}}$. После этого сдвинем его немного, чтобы одна из его точек X попала на границу шара, но при этом само множество оставалось внутри круга. Проведём круг радиуса 1 с центром X . Так как множество имеет диаметр 1, то проведённый круг содержит наше множество. А значит, пересечение $B_1 \cap B_2$ также покрывает исходное множество.

41. Пусть центр шара B_2 — самая высокая точка шара B_1 . Отсечём от $B_1 \cap B_2$ сверху небольшую шапку горизонтальной плоскостью. Остальную часть $B_1 \cap B_2$ разрежем на четыре части плоскостями, параллельными двум другим координатным плоскостям. Диаметр каждой части в этом случае меньше 1.

42. Правильный симплекс нельзя разбить на $n+1$ частей меньшего диаметра.

44. Множество диаметра 1 можно поместить в единичный куб, потому достаточно разбить куб на части диаметра меньше 1. Покроем единичный куб $([\sqrt{n}] + 1)^n$ кубиками, сторона которых чуть меньше $\frac{1}{\sqrt{n}}$. Главная диагональ каждого кубика чуть меньше 1. Поэтому $f(n) \leq ([\sqrt{n}] + 1)^n$.

45. По решению задачи 39 радиус описанной сферы единичного симплекса в $\mathbb{R}^4$ равен $\sqrt{\frac{2}{5}}$. Аналогично решению задачи 33 шар радиуса $\sqrt{\frac{2}{5}}$ — универсальная покрывка в $\mathbb{R}^4$. Аналогично задаче 40 пересечение шара B_1 радиуса $\sqrt{\frac{2}{5}}$ с единичным шаром B_2 с центром на границе B_1 — универсальная покрывка в $\mathbb{R}^4$.

46. Аналогично решению задачи 41 отсечём небольшую шапку горизонтальной плоскостью, а остальное разрежем тремя плоскостями, параллельными координатным, на восемь частей.

Список цитированной литературы

- [1] А.М. Райгородский, *Проблема Борсука*, Москва, МЦНМО, 2006.
- [2] А.М. Райгородский, *Линейно-алгебраический метод в комбинаторике*, Москва, МЦНМО, 2007.
- [3] В.Г. Болтянский и И.Ц. Гохберг, *Теоремы и задачи комбинаторной геометрии*, Москва, “Наука”, 1965.
- [4] А.М. Райгородский, *Хроматические числа*, Москва, МЦНМО, 2003.

Partitioning of a set into pieces of smaller diameter

A.M. Raigorodskii with V. Bulankina and M. Prasolov

1 Definitions and notations

Let the *diameter* of a set Ω on the plane be the quantity

$$\text{diam } \Omega = \sup_{\mathbf{x}, \mathbf{y} \in \Omega} |\mathbf{x} - \mathbf{y}|.$$

Here

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + (x_2 - y_2)^2}, \quad \mathbf{x} = (x_1, x_2), \quad \mathbf{y} = (y_1, y_2),$$

i.e. this is ordinary “Euclidian” distance between points on the plane. The symbol “sup” means “supremum” (least upper bound), and it is convenient to suppose that “sup” means maximum. Essentially, diameter of a set is a maximal distance between its points. Why do we write not well known supremum nevertheless? Because there exist sets without a pair of points with maximal distance between them. For example, a disc without its boundary (remove its bounding circle). Never mind though. We consider only “closed” sets (which contain their boundary), so supremum is not necessary.

Consider an arbitrary bounded set Ω . We can suppose that $\text{diam } \Omega = 1$ (zoom in or zoom out the set using homothetic transformation to obtain the desired diameter). We aim to sparingly dissect Ω into pieces of smaller diameter. In other words, we aim to represent Ω in the form

$$\Omega = \Omega_1 \cup \dots \cup \Omega_f$$

under the condition $\text{diam } \Omega_i < \text{diam } \Omega$ for all i and we aim to minimize f . You can imagine Ω as some crooked cake which does not go through our mouth as a whole but which we desire to eat greedily, to bite the least number of times. And so we should dissect a cake into pieces such that number of these pieces is the least and each piece fits in the mouth still.

The main question: which cake is the worse in the sense of the above-described problem about dissecting? In other words, into how much pieces can we dissect any cake deliberately?

K.Borsuk in 1933 formalized the problem described above: what is the least number $f(2)$ such that any bounded set Ω on the plane admits a partition into $f(2)$ parts of smaller diameter? Of course, Borsuk was not reflecting about crooked cakes and even topology served as the motivation for his research. More detailed and, by the way, more intriguing history of the problem can be found in [1].

One more question: why do we write $f(2)$? The answer is that the plane is two-dimensional. In the truth, Borsuk raised a similar problem on the real axis too (corresponding quantity is $f(1)$), and in space of any dimension also. Usually the space of dimension n is denoted by $\mathbb{R}^n$. In particular, $\mathbb{R}^1 = \mathbb{R}$ is the real axis, $\mathbb{R}^2$ is the plane, $\mathbb{R}^3$ is the space in common sense, i.e. 3-dimensional space in which we live. In general case $f(n)$ is a *Borsuk number*, which is the least f , such that any bounded set in $\mathbb{R}^n$ can be dissected into f pieces of smaller diameter, but there exists a bounded set in $\mathbb{R}^n$, which cannot be dissected into $f - 1$ pieces of smaller diameter. Here the distance between points in $\mathbb{R}^n$ is standard (is measured “by Euclid”):

$$|\mathbf{x} - \mathbf{y}| = \sqrt{(x_1 - y_1)^2 + \dots + (x_n - y_n)^2}, \quad \mathbf{x} = (x_1, \dots, x_n), \quad \mathbf{y} = (y_1, \dots, y_n).$$

Borsuk supposed that $f(n) = n + 1$. This supposition is called *the Borsuk conjecture*. This conjecture was disproved in 1993 (see [1], [2]), but it remains a great amount of questions without answers still.

In the following section we introduce the problems. Step by step you approach the interesting problems in which an advance can be done by elementary methods.

2 Problems before intermediate finish

Problem 1. Prove that $f(1) = 2$.

Problem 2. Prove that $f(2) \geq 3$. In other words, give an example of a set on the plane which cannot be dissected into two pieces of smaller diameter.

Problem 3. Dissect a square into pieces of smaller diameter.

Problem 4. Dissect a disc of radius $1/2$ into three pieces of smaller diameter.

Problem 5. Dissect a disc of radius $1/2$ into three pieces of diameter not greater than $\frac{\sqrt{3}}{2} = 0.866\dots$

Problem 6. Prove that the constant $\frac{\sqrt{3}}{2}$ from the problem 5 is unimprovable, i.e. for any partition of a disc of radius $1/2$ into 3 pieces at least one of those pieces has diameter not smaller than $\frac{\sqrt{3}}{2}$.

Call by *universal cover* in $\mathbb{R}^n$ such set Ω that any set Φ of unit diameter can be moved into Ω , i.e. it is possible to cover Φ by Ω . For instance:

Problem 7. Prove that a unit square is a universal cover on the plane.

Problem 8. Prove that a unit cube is a universal cover in the space of any dimension. Here we call by unit cube a set of points $\mathbf{x} = (x_1, \dots, x_n)$, such that $x_i \in [0, 1]$ for all i .

It is known that a regular hexagon Ω_6 with distance 1 between its parallel sides is a universal cover on the plane. For detailed proof see [3]. However, you may reflect on it.

Problem 9. Dissect the regular hexagon Ω_6 into three parts of diameter $\frac{\sqrt{3}}{2}$. Deduce from this problem the validity of the Borsuk conjecture on the plane and, in some sense, “unimprovability” of the constant $\frac{\sqrt{3}}{2}$ from the problem 6.

Problem 10. What number plays the role of unimprovable constant from the problem 9 on the real axis?

Problem 11. Prove that in any set of n points on the plane there are at most n pairs of points such that the distance between them equals the diameter of the set.

Problem 12. Deduce from the problem 11 the validity of the Borsuk conjecture for *finite* sets on the plane (not involving universal covers).

Problem 13*. Prove that a disc of radius $\frac{1}{\sqrt{3}}$ is a universal cover on the plane.

Problem 14. Explain why a disc of radius $r < \frac{1}{\sqrt{3}}$ cannot be a universal cover.

Problem 15. Explain why the result of the problem 13* does not allow to prove the Borsuk conjecture on the plane.

Problem 16. A disc B_1 of radius $\frac{1}{\sqrt{3}}$ is given on the plane. Choose an arbitrary point on its boundary and consider the disc B_2 of radius 1 with center in chosen point. Prove that $B_1 \cap B_2$ is a universal cover on the plane.

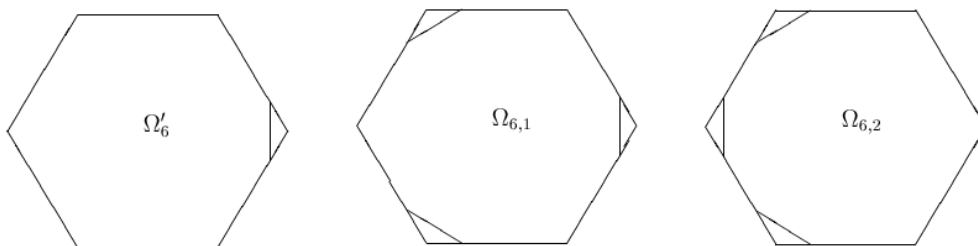
Problem 17. Using the result of the problem 16 prove the Borsuk conjecture.

Problem 18* (research). Is it possible to prove using the result of the problem 16 that any set of diameter 1 can be dissected into three pieces of diameter $\leq \frac{\sqrt{3}}{2}$? What is the least such constant that you obtained?

Call by *universal covering system (ucs)* in $\mathbb{R}^n$ such collection of sets $\{S_\alpha\}$, that any $\Omega \subset \mathbb{R}^n$, $\text{diam } \Omega = 1$, can be moved into at least one of the sets S_α .

Problem 19. Consider the regular hexagon Ω_6 with distance 1 between parallel sides. Consider a segment connecting the center of hexagon with one of its vertices and draw a line perpendicular to this segment at the distance $1/2$ from the center. This line cuts off a triangle from the hexagon. Prove that the hexagon without mentioned triangle also is a universal cover on the plane. This truncated hexagon is denoted by Ω'_6 on the picture 1.

Problem 20. Prove that the middle and the regular hexagons form ucs. Triangles, as in the problem 19, are cut off by the lines at the distance $1/2$ from the hexagon center and perpendicular to the segments connecting the center with corresponding vertices.



Picture 1: Examples of ucs.

Problem 21. Prove that any set of diameter 1 on the plane can be dissected into 5 pieces without a pair of points at the distance $\frac{1}{\sqrt{3}}$. **Hint.** Use Ω_6 .

Problem 22* (research). Is it possible to prove that for some $a < \frac{1}{\sqrt{3}}$ any set of diameter 1 on the plane can be dissected into 5 pieces without a pair of points at the distance a ?

Problem 23. Find such n , that any set on the plane can be dissected into n pieces without a pair of points at the distance 1. What is the least n that you found?

Problem 24*. Prove that any set of diameter 1 on the plane can be dissected into 6 pieces of diameter not greater than $\sqrt{\frac{13}{3}}(2 - \sqrt{3}) = 0.5577\dots$ **Hint.** Use ucs $\{\Omega_{6,1}, \Omega_{6,2}\}$.

Problem 25.** Even better than in the problem 24*?

Problem 26*. Prove that any set of diameter 1 on the plane can be dissected into 5 pieces of diameter not greater than 0.603. **Hint.** Use the universal cover Ω'_6 .

Problem 27.** And even better than in the problem 26*?

Problem 28. Prove that any set of diameter 1 on the plane can be dissected into 4 pieces of diameter not greater than $\frac{1}{\sqrt{2}}$.

Problem 29. Prove the unimprovability of the result of the problem 28.

Problem 30. Prove that any set of diameter 1 on the plane can be dissected into 7 pieces of diameter not greater than $\frac{1}{2}$.

Problem 31. Prove the unimprovability of the result of the problem 30.

3 Problems after intermediate finish

Problem 32. Prove that $f(3) \geq 4$.

Problem 33*. Prove that a ball with radius $\sqrt{\frac{3}{8}}$ is a universal cover in $\mathbb{R}^3$.

Problem 34. Explain why a ball of radius $r < \sqrt{\frac{3}{8}}$ cannot be a universal cover in $\mathbb{R}^3$.

Problem 35. Split a ball of radius $1/2$ into four pieces of smaller diameter in the space (i.e. diameter of each piece must be smaller than 1).

Problem 36*. Let regular tetrahedron be inscribed in the ball of radius $1/2$. Let us consider 4 trihedral angles which we can get if we connect the center of the ball with vertices of tetrahedron's faces. Let us intersect each of these angles with the ball. So we will have a partitioning of our ball into 4 equal pieces. Find diameters of these pieces.

Problem 37. Let us define *regular simplex* in $\mathbb{R}^n$ as an analog of regular triangle on the plane and regular tetrahedron in the space. Notably let us consider $n+1$ points $\mathbf{x}_1, \dots, \mathbf{x}_{n+1}$ in $\mathbb{R}^n$ such that $|\mathbf{x}_i - \mathbf{x}_j| = a$ for every pairs $i \neq j$ and some $a > 0$. Prove the existence of the simplex.

Problem 38*. Let us define *n-dimensional ball* as a set

$$B = \{\mathbf{x} = (x_1, \dots, x_n) : x_1^2 + \dots + x_n^2 \leq 1\}.$$

It is a ball with radius 1 and with diameter 2 . Let us inscribe the regular simplex in this ball. Find the length of the side of this simplex.

Problem 39.** Let us realize partitioning of the ball from the problem 38* like partitioning from the problem 36*. Notably let us inscribe a regular simplex whose sides' length was found in problem 38* in our ball and let us consider such polyhedral angles which have a vertex in the center of our ball and pass through the simplex faces (there are $n+1$ faces of simplex). Find diameters of obtained pieces. In particular ascertain that they are smaller than 2 and also that their values tend to 2 with $n \rightarrow \infty$.

Problem 40. Let us intersect the ball B_1 of radius $\sqrt{\frac{3}{8}}$ with any ball B_2 of radius 1 whose center lies on the border of the ball B_1 . Prove that $B_1 \cap B_2$ is a universal cover in $\mathbb{R}^3$.

Problem 41*. Prove that $B_1 \cap B_2$ can be split into 5 pieces of diameter smaller than 1 .

Problem 42. Prove that $f(4) \geq 5$. Also in the general case $f(n) \geq n+1$.

Problem 43. Find any upper bound for $f(4)$.

Problem 44. Find any upper bound for $f(n)$.

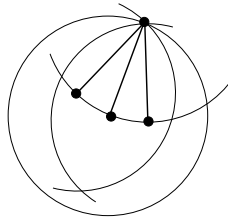
Problem 45. Construct a cover in $\mathbb{R}^4$, like covers from the problem 40 of this list and also the problem 16 from the list of problems before the intermediate finish.

Problem 46*. Prove that the cover from the problem 45 can be split into 9 pieces of diameter smaller than 1 and so $f(4) \leq 9$.

4 Solutions

When solving the problems of the project, some of the school participants have obtained brilliant and unexpected results. First of all, it is worth making special mention of a result by Egor Voronetskiy who succeeded in improving all the previously known upper bounds for the minimum value of a forbidden distance between any two monochromatic points in a colouring of an arbitrary planar set of diameter 1 with four and five colours. If the previous bounds were by the values $\frac{1}{\sqrt{2}}$ and $\frac{1}{\sqrt{3}}$, then now, due to Egor, we have bounds by the values $\frac{1}{\sqrt{3}}$ and $\frac{1-\sqrt{3}+\sqrt{6\sqrt{3}}}{4\sqrt{3}-2}$. Egor's constructions are given below. Also we want to say about a new upper bound for the minimum diameter in a partitioning of an arbitrary planar set of diameter 1 into six parts. This bound was independently obtained by Dima Belov with Nikita Aleksandrov and by How Si Wei. If the previous bound had a value $0.557\dots$, then the current bound equals $0.542\dots$. Below, we also present these constructions. At the same time, some school participants have shown a very high mathematical culture: they managed to carefully calculate the diameters of parts in a dissection of the n -dimensional unit ball into $n+1$ parts (problem 8** from the second part of the project); they also managed to give a proof of a theorem by M. Lassak, which was published in 1982 and which asserts that any set of diameter 1 in $\mathbb{R}^n$ can be partitioned into $2^{n-1}+1$ pieces of diameter < 1 . Both the dissection of the unit ball and the proof of Lassak's theorem were done by Egor Voronetskiy and Maksim Didin.

1. It is obvious that $f(1) > 1$. It is sufficient to dissect the segment into 2 pieces with smaller diameter as long as for any set with diameter 1 on the line we can put it in the segment with length 1. For example we can dissect our segment in halves.
2. It is equilateral triangle for example.
3. We can do it with one vertical section for example.
5. We can cut our circle by three radii, with angles of 120° between them.
6. Let our circle be dissected into three pieces. Let us take a point on the boundary of our circle so that it lies in two of these pieces. And let us construct an equilateral triangle with one vertex at our point and other vertices on the boundary of our circle. Then two vertices of this triangle are in the same piece. So the diameter of this piece is not less than $\frac{\sqrt{3}}{2}$.
8. It is obvious that the set Ω with diameter 1 is in stripe $\min_{x \in \Omega} x_i \leq x_i \leq \max_{x \in \Omega} x_i$ with width at most 1. Intersection of such stripes for all i is a parallelepiped. We can cover it by the unit cube.
9. Dissect the regular hexagon into three pieces by perpendiculars from the center to not adjacent sides. The diameter of each piece equals $\frac{\sqrt{3}}{2}$. Then place the set Ω of diameter 1 into Ω_6 . The partition of Ω_6 provides the partition of Ω into the pieces of diameter at most $\frac{\sqrt{3}}{2} < 1$. And as we know from the problem 6, the constant $\frac{\sqrt{3}}{2}$ is unimprovable in the case of the circle of diameter 1.
10. Any set of diameter 1 on the line can be dissected into two pieces of diameter $\frac{1}{2}$ but the unit segment cannot be dissected into two parts of diameter smaller than $\frac{1}{2}$.
11. Connect by edges all pairs of points at the distance 1. If every point is incident to at most two edges then we have at most n edges. So consider a triple of edges with common end. Since the distance between points is at most 1, the angle between edges is at most 60° .
Another end of the middle edge is incident only to this edge, since any two points are at the distance at most 1 (see pic.2). So erase the middle edge with its not common end and continue the proof by induction.
12. It is sufficient to paint in three colours the vertices of the graph from the previous problem. Do it by induction. Suppose you have a vertex v with only one edge incident to it. Erase v , colour the rest graph by induction and then paint v not in the colour of its neighbour. In other cases the graph is a collection of cycles. Paint them in three colours.



Picture 2: Three edges with common end.

13. *The first solution.* Place the set Ω of diameter 1 into a large disc B . Then reduce this disc in such a way that it always contains Ω and once some points appear on the boundary of B they continue to lie there. We cannot reduce the disc if one of two cases occurs:

- 1) ends of some diameter of B belong to Ω , so the diameter of B is not greater than 1;
- 2) some three points of Ω lie on the boundary of B and form an acute-angled triangle, it is well-known that in this case the diameter of B is not greater than $\frac{1}{\sqrt{3}}$.

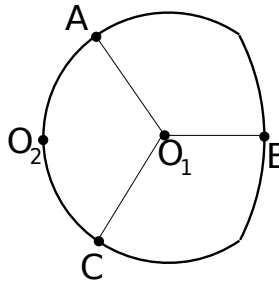
The second solution. Since the regular hexagon inscribed in the circle is a universal cover, this is a universal cover also.

14. Suppose that the equilateral triangle with the side 1 is contained in a disc with radius r , then reduce this disc as in the solution of the previous problem. In the end we obtain the circumscribed disc about the triangle. So $r \geq \sqrt{\frac{1}{3}}$.

15. By the problem 6 if the disc with radius $\frac{1}{\sqrt{3}}$ is dissected into three parts then the diameter of some part is at least 1.

16. By the problem 13 we can place any set Ω of diameter 1 into the circle B_1 with radius $\frac{1}{\sqrt{3}}$. Then translate this set so that the point $X \in \Omega$ appears on the boundary of the circle but Ω continues to lie in B_1 . Draw a circle B_2 with radius 1 and center X . Since the diameter of Ω equals 1, B_2 covers Ω also. So the intersection $B_1 \cap B_2$ covers Ω .

17. The universal cover from the problem 16 can be dissected into three parts of diameter $c = \frac{\sqrt{3}}{2} + \frac{\sqrt{\frac{2}{\sqrt{3}}-1}}{2} < 1$. We see on the picture that O_1 is the center of circle with radius $\frac{1}{\sqrt{3}}$, O_2 is the center of the circle with radius 1, B is the middle of the arc with unit radius and points A and C are chosen in such a way that the triangle ABC is equilateral. It is easy to compute that its side equals $\frac{\sqrt{3}}{2} + \frac{\sqrt{\frac{2}{\sqrt{3}}-1}}{2}$.



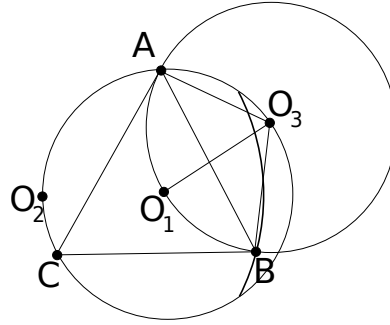
Picture 3: The partition of the universal cover from the problem 16.

After that the Borsuk conjecture can be proved in a similar way as in the problem 9.

18. Let us prove that $B_1 \cap B_2$ cannot be dissected into three parts of diameter smaller than c which is defined in the solution of the previous problem.

Lemma. For every point X on the boundary of $B_1 \cap B_2$ there exists an equilateral triangle whose vertices belong to the boundary of $B_1 \cap B_2$ and one of them is X . Also the side of such triangle is not shorter than c .

Proof. Rotate the boundary of $B_1 \cap B_2$ about X by 60 degree clockwise and counter-clockwise. Intersect the image under rotation with boundary of $B_1 \cap B_2$. Intersection points are the vertices of the equilateral triangle. Exactly one of them lies on the arc with radius 1: if no points lie on this arc then we have an inscribed angle $< 60^\circ$, and if two points lie on this arc — $< 60^\circ$. On the picture there are O_1 — the center of the circle with radius $\frac{1}{\sqrt{3}}$, O_2 — the center of the circle with radius 1, ABC — the equilateral triangle, where vertex B lies on the arc with radius 1.



Picture 4: A equilateral triangle on the boundary of the universal cover from the problem 16.

Rotate the circle with center O_1 about A by 60° . Denote by O_3 its center. Clearly points O_1 and B lie on the circle with center O_3 , i.e. $O_3A = O_3B = \frac{1}{\sqrt{3}}$. Therefore, AB decreases if the angle AO_3B decreases. But $BO_3O_1 = 60^\circ$. So the angle AO_3B decreases as the angle O_1O_3B decreases. Also $O_3O_1 = O_3B = \frac{1}{\sqrt{3}}$. So the angle O_1O_3B decreases as O_1B decreases. O_1B is minimal if B is the middle of the arc with radius 1. Therefore, $AB \geq c$.

Return to the proof of the initial problem. Suppose $B_1 \cap B_2$ is dissected into three parts. Consider the point X on the boundary which belongs to 2 parts. Apply lemma to point X . In the triangle from lemma some two vertices belong to the same part, i.e. the distance between them is at least c . Therefore the diameter of this part is at least c .

19. Consider two small triangles that lie in the opposite vertices of the hexagon. The distance between any two points of these triangles is at least 1. So, if a set of diameter 1 lies within the hexagon then one of these triangles can be cut off without touching the set.

20. Continuing the proof of the previous problem we can cut off a triangle in every pair of opposite triangles without touching the set. So we obtain one of the hexagons on the picture.

21. *Solution is given by the participant of the conference Egor Voronetskii.* It is sufficient to dissect the regular hexagon with the length of the side $\frac{1}{\sqrt{3}}$. However it can be dissected into 4 parts!

In the center of the picture the Reuleaux triangle of diameter $\frac{1}{\sqrt{3}}$ is placed. It is easy to compute that $AB = \frac{1}{\sqrt{3}}$. Colour the arc CD in green, but the vertex C — in blue. Colour arcs AC and BC in blue, but vertices A and B — in red and yellow respectively. Colours of other arcs and vertices are defined using the rotation by 120° .

22. *Solution is given by the participant of the conference Egor Voronetskii.*

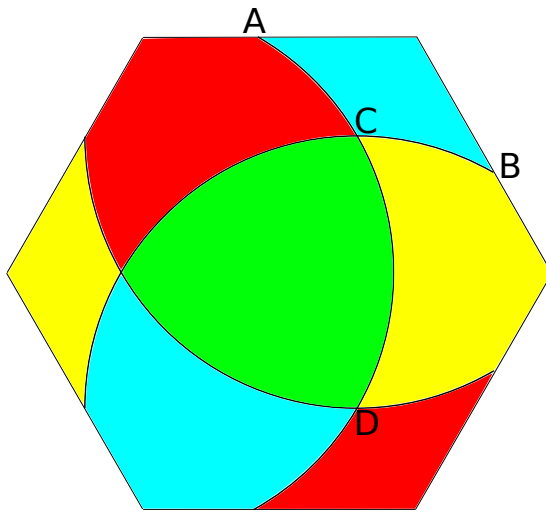
Dissect the hexagon similarly to the previous problem, but the diameter of the Reuleaux triangle equals AB in this case (see pic.6).

We change color only in the interior of the blue part. Other points keep their color.

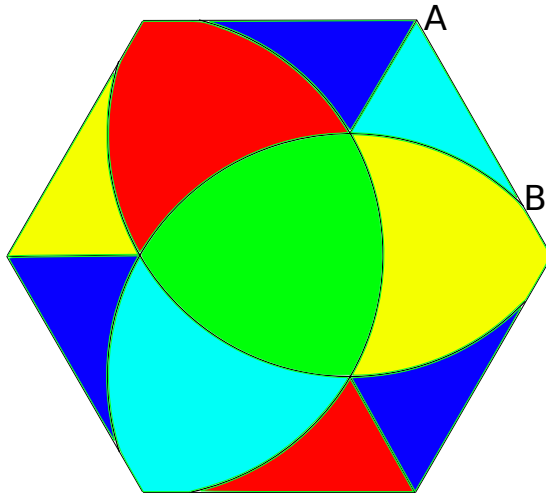
23. This problem is equivalent to the problem about the chromatic number of the plane which is unsolved. It is known only how to paint the plane in 7 colours: hexagons of regular hexagonal lattice can be painted in 7 colours in such a way that adjacent hexagons are of different colour.

24. Let $\sigma = \sqrt{\frac{13}{3}} (2 - \sqrt{3})$. We will dissect hexagons $\Omega_{6,1}$ and $\Omega_{6,2}$ into 6 pieces of diameter not greater than σ . By the problem 20 it is sufficient for the proof.

Let us start with hexagon $\Omega_{6,1}$.



Picture 5: There are no points of the same colour at the distance $\frac{1}{\sqrt{3}}$



Picture 6: There are no points of the same colour at the distance $\frac{1-\sqrt{3}+\sqrt{6\sqrt{3}}}{4\sqrt{3}-2}$.

Suppose that $\Omega_{6,1}$ is obtained from the regular hexagon $ABCDEF$ by cutting triangles BB_1B_2 , DD_1D_2 and FF_1F_2 . Let $M_1, \dots, M_6$ be the middle points of the sides and O be the center (see pic. 7). Consider segments AX, CY, EZ of length $1/2$ on rays AO, CO, EO and draw segments OX, OY, OZ . Then connect all points X, Y, Z with two sides of the hexagon (see pic.7). So we obtain a partition of $\Omega_{6,1}$ into six polygons $OXM_1B_2B_1M_2Y$, AM_1XM_6 etc.

Their diameters are not greater than σ .

Indeed, $AX = M_1M_6 = \frac{1}{2}$. Therefore the diameter of quadrilateral AM_1XM_6 equals $\frac{1}{2}$. The diameter of 7-gon $OXM_1B_1B_2M_2Y$ equals $OB_1 = \frac{1}{2\cos\frac{\pi}{12}} \approx 0.5176$. Other diameters can be obtained from these two ones by rotation of the picture.

Now dissect the hexagon $\Omega_{6,2}$ in the following way.

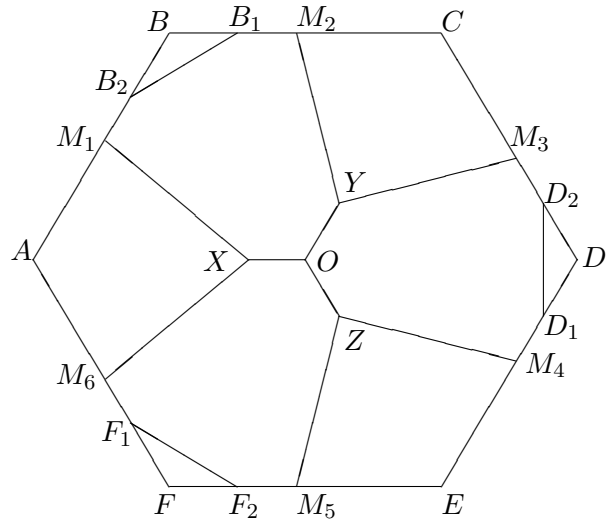
Suppose that $\Omega_{6,2}$ is obtained from the hexagon $ABCDEF$ by cutting triangles AA_1A_2 , BB_1B_2 and FF_1F_2 (see pic. 8). Let M be the middle of A_1A_2 , and J be the intersection of a midperpendicular to the segment A_1C with segment AD . Clearly $JA_1 = JC$.

Draw lines parallel to diagonals BE and CF through the point J . Suppose these lines intersect $\Omega_{6,2}$ by segments PQ and RS (see pic. 8). So we have $\Omega_{6,2}$ dissected into six polygons.

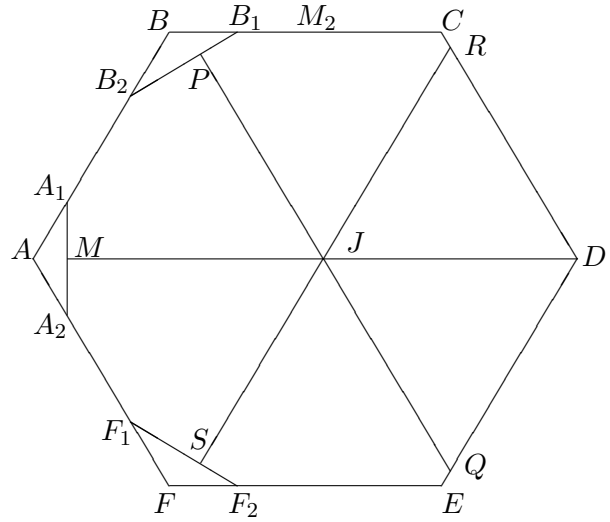
Let us check that their diameter is not greater than σ .

Note that $JA_1 = JC = \sigma$.

Indeed, by Pythagorean theorem for triangles JMA_1 and JM_2C (the point M_2 is the middle of BC) the



Picture 7:



Picture 8:

equality $JA_1^2 = JC^2$ is equivalent to

$$\left(OJ + \frac{1}{2}\right)^2 + \left(\frac{\operatorname{tg} \frac{\pi}{12}}{2}\right)^2 = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2\sqrt{3}} - OJ\right)^2,$$

so we obtain

$$OJ = \frac{1 - 3 \operatorname{tg}^2 \frac{\pi}{12}}{4(3 + \sqrt{3})}.$$

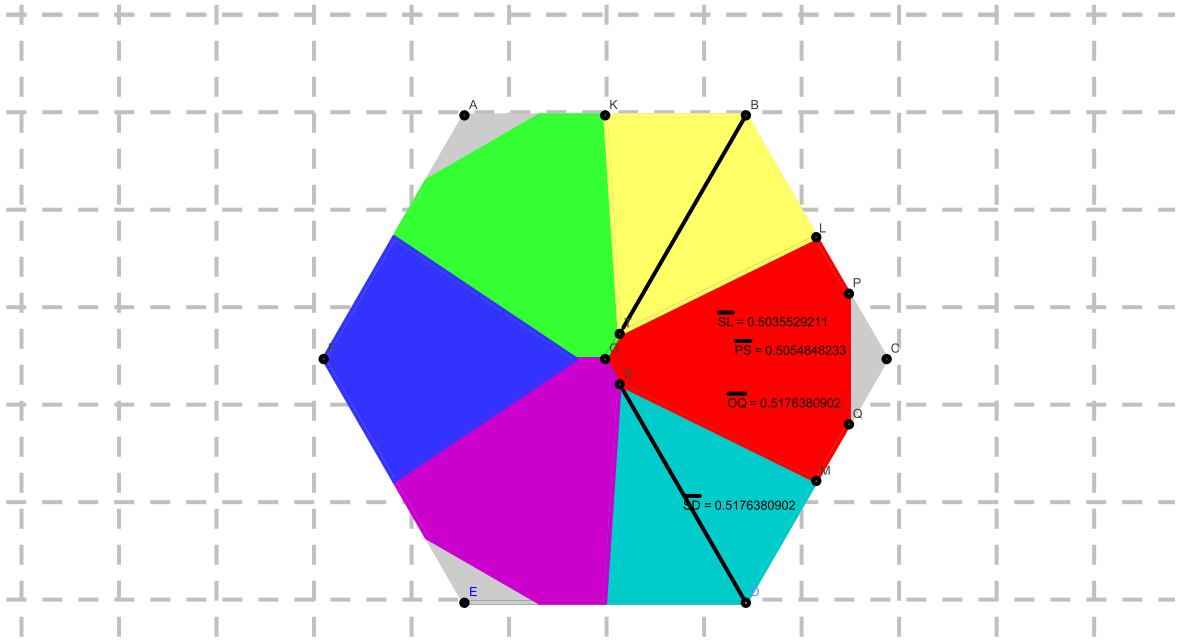
Now the length of the segment JA_1 can be computed by Pythagorean theorem for the triangle JMA_1 .

It is not so difficult to compute that diameters of pentagons JMA_1B_2P and JPB_1CR equal $JA_2 = JC = \sigma$, and diameter of the equilateral triangle JRD is less than σ . The partition is symmetric with respect to the line MD . This finishes the proof.

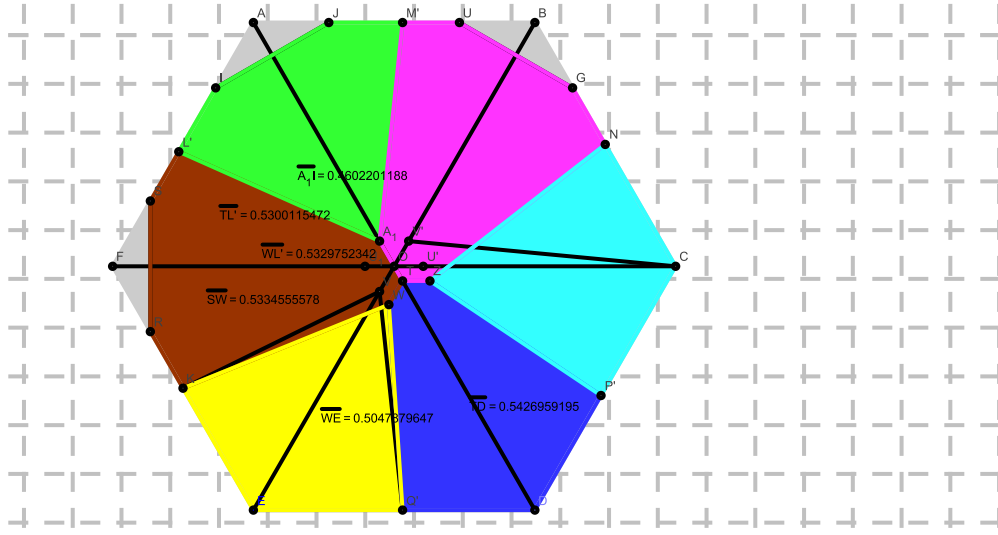
25. *Solution is given independently by two teams: Aleksandrov Nikita and Belov Dima, and How Si Wei.*

Dissect elements of ucs. At first dissect the polygon on the picture 9. It is symmetric with respect to rotation by 120° and $BT = \sqrt{2 - \sqrt{3}}$. We have diameters of all parts equal $\sqrt{2 - \sqrt{3}}$.

Then consider the picture 10. The point T lie on the diagonal AD and $ST = TD$. Also $AA_1 = EV = CU' = \sqrt{2 - \sqrt{3}}$. The point W is chosen in such a way that W lies on VD and TW is parallel to CD . The point Z can be defined in similar way. Points M', N, P', Q', K and L' are bases of perpendiculars dropped from the point T . After some computations we see that diameters of all parts are at most $TD = \frac{10 - 4\sqrt{3}}{5\sqrt{3} - 3} \approx 0,5427$.



Picture 9: Diameters of all parts equal $\sqrt{2 - \sqrt{3}}$.



Picture 10: Diameters of all parts are at most TD .

26. Dissect Ω'_6 into five sets in the following way.

Consider points X, Y, Z and T on the sides BC, CD, DE, EF respectively such that all sides of the pentagon $MYXZT$ are equal (see pic. 11).

Clearly this can be done in the unique way.

Denote the length of the segment MX by ρ'_5 . It is easy to compute that $\rho'_5 = 0.6020\dots$

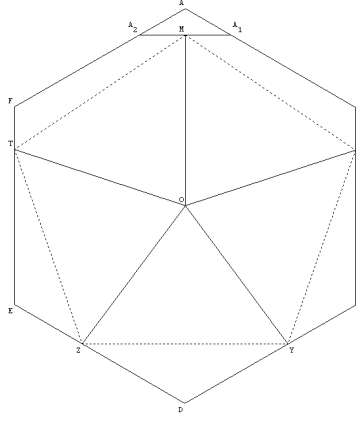
Connect the point O with all vertices of $MYXZT$. So Ω'_6 is dissected.

Obviously the distance between the point O and arbitrary point on the boundary of Ω'_6 is not greater than $\frac{1}{\sqrt{3}} < \rho'_5$. Therefore parts of the partition have diameter ρ'_5 .

27. ?

28. By the problem 7 the partition of the unit square into 4 parts of diameter $\frac{1}{\sqrt{2}}$ is sufficient. Draw the diagonals.

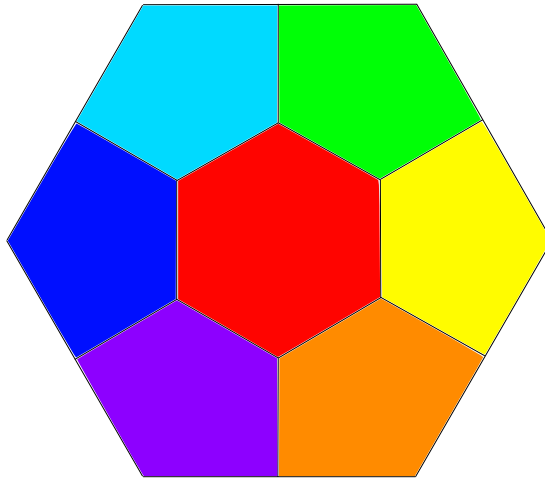
29. Let us prove that the circle of diameter 1 cannot be dissected into four pieces. Suppose the contrary. Let us take a point on the boundary of our circle so that it lies in two of these pieces. And let us construct a square



Picture 11:

with one vertex at our point and other vertices on the boundary of our circle. Then two vertices of this square are in the same piece. So the diameter of this piece is not less than $\sqrt{\frac{1}{2}}$.

30. Since the regular hexagon with side $\frac{1}{\sqrt{3}}$ is a universal cover, its partition into 7 parts of diameter $\frac{1}{2}$ is sufficient (see pic.12)



Picture 12: the maximal diagonals of the hexagon and pentagons equal $\frac{1}{2}$.

31. Let us prove that the circle of diameter 1 cannot be dissected into seven pieces. Suppose the contrary. Let us take a point on the boundary of our circle so that it lies in two of these pieces. And let us construct a regular hexagon with one vertex at our point and other vertices on the boundary of our circle. Then two vertices of this hexagon are in the same piece. So the diameter of this piece is not less than $\frac{1}{2}$.

32. The regular tetrahedron cannot be dissected into three pieces of smaller diameter, because its vertices must lie in different pieces.

33. The solution is similar to the first solution of the problem 13. Place the set Ω of diameter 1 into a large ball B . Then reduce this ball in such a way that it always contains Ω and once some points appear on the boundary of B they continue to lie there. We cannot reduce the ball if one of three cases occurs:

- 1) ends of some diameter of B belong to Ω , so the diameter of B is not greater than 1;
- 2) some three points of Ω lie on the equator of B and form an acute-angled triangle, in this case the diameter of B is not greater than $\frac{1}{\sqrt{3}}$;
- 3) some four points of Ω lie on the boundary of B and form tetrahedron which contains the center of B .

It is sufficient to prove that in the third case the radius of the ball is not greater than $\sqrt{\frac{3}{8}}$. This follows from the lemma.

Lemma. Suppose a tetrahedron T is inscribed into a unit sphere and contains the center of the sphere. Then some side of T is not shorter than $\sqrt{\frac{8}{3}}$. Suppose additionally that T is regular. Then its sides equal $\sqrt{\frac{8}{3}}$.

Proof. Let O be the center of the sphere and A, B, C, D be vertices of T . T contains O , therefore

$$a \cdot \overrightarrow{OA} + b \cdot \overrightarrow{OB} + c \cdot \overrightarrow{OC} + d \cdot \overrightarrow{OD} = \vec{0}$$

for some positive numbers a, b, c, d . Let a be the maximal number among them. Consider the inner product of vector $\overrightarrow{OA}$ with both parts of this equality:

$$a \cdot \overrightarrow{OA} \cdot \overrightarrow{OA} + b \cdot \overrightarrow{OB} \cdot \overrightarrow{OA} + c \cdot \overrightarrow{OC} \cdot \overrightarrow{OA} + d \cdot \overrightarrow{OD} \cdot \overrightarrow{OA} = 0.$$

Number a is maximal, so $\overrightarrow{OA} \cdot \overrightarrow{OX} < -\frac{1}{3}\overrightarrow{OA} \cdot \overrightarrow{OA}$ where $X = B, C$ or D . Without loss of generality $X = B$. By cosine law $AB \geq \sqrt{\frac{8}{3}}$ since $OA = OB = 1$. The inequality is exact in the case of the regular tetrahedron.

34. Suppose that the regular tetrahedron with the side 1 is contained in a ball with radius r , then reduce this ball as in the solution of the previous problem. In the end we obtain the circumscribed ball about the tetrahedron. So $r \geq \sqrt{\frac{3}{8}}$.

36. Let A_1, A_2, A_3, A_4 be the vertices of the tetrahedron and O be its center. Consider the piece associated to the trihedral angle $OA_1A_2A_3$. Let B be the middle of A_2A_3 . Draw the radius OB . Denote by C its end lying on the sphere. The statement is that the diameter equals the length of A_1C . We leave the proof of this fact to the reader.

By the previous problem a side of the tetrahedron equals $\sqrt{\frac{2}{3}}$. By the Pythagorean theorem for triangles A_1BA_2 and OBA_2 obtain that $|A_1B| = \sqrt{\frac{1}{2}}$ and $|OB| = \sqrt{\frac{1}{12}}$. By the cosine law a cosine of the angle A_1OB equals $-\sqrt{\frac{1}{3}}$.

By the cosine law for triangle A_1OC , obtain that

$$|A_1C| = \sqrt{\frac{3 + \sqrt{3}}{6}} \approx 0.888... < 1.$$

37. n points which have one unit coordinate and whose all other coordinates are zero form a regular simplex in the plane $x_1 + x_2 + \dots + x_n = 1$.

39. Recall some geometric notions. The inner product of vectors $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ is a number $(\mathbf{x}, \mathbf{y}) = x_1y_1 + x_2y_2$. The distance $|\mathbf{x} - \mathbf{y}|$ between points $\mathbf{x}, \mathbf{y}$ is measured by formula

$$|\mathbf{x} - \mathbf{y}|^2 = (\mathbf{x}, \mathbf{x}) + (\mathbf{y}, \mathbf{y}) - 2(\mathbf{x}, \mathbf{y}). \quad (1)$$

Notation $(\mathbf{x}, \mathbf{x})$ is called the inner square of the vector $\mathbf{x}$. It represents a square of the length $|\mathbf{x}|$ of this vector. The cosine of the angle between the vectors $\mathbf{x}, \mathbf{y}$ can be computed by formula $\frac{(\mathbf{x}, \mathbf{y})}{|\mathbf{x}||\mathbf{y}|}$. So the equality (1) is just the cosine law:

$$|\mathbf{x} - \mathbf{y}|^2 = |\mathbf{x}|^2 + |\mathbf{y}|^2 - 2|\mathbf{x}| \cdot |\mathbf{y}| \cdot \cos(\hat{\mathbf{x}}, \hat{\mathbf{y}}). \quad (1')$$

Say the same about $\mathbb{R}^d$. The inner product of vectors $\mathbf{x} = (x_1, \dots, x_d)$, $\mathbf{y} = (y_1, \dots, y_d)$ equals

$$(\mathbf{x}, \mathbf{y}) = x_1y_1 + \dots + x_dy_d.$$

Let us compute the diameter of the part D associated to the vertices $\mathbf{x}_1, \dots, \mathbf{x}_d$ of the simplex T . Clearly $\mathbf{x}_1 + \dots + \mathbf{x}_{d+1} = \mathbf{0}$ (see two- and three-dimensional cases). Therefore

$$(\mathbf{x}_1, \mathbf{x}_i) + \dots + (\mathbf{x}_{d+1}, \mathbf{x}_i) = (\mathbf{0}, \mathbf{x}_i) = 0$$

for each i . Since $|\mathbf{x}_1| = \dots = |\mathbf{x}_{d+1}| = 1$ (all vertices of T lie on the unit sphere), we obtain that $(\mathbf{x}_i, \mathbf{x}_i) = 1$. Finally by symmetry all angles $(\mathbf{x}_j, \mathbf{x}_i)$ for $i \neq j$ are the same. Hence for $i \neq j$ we obtain that

$$0 = (\mathbf{x}_1, \mathbf{x}_i) + \dots + (\mathbf{x}_{d+1}, \mathbf{x}_i) = 1 + d(\mathbf{x}_j, \mathbf{x}_i),$$

i.e. $(\mathbf{x}_j, \mathbf{x}_i) = -\frac{1}{d}$. for all $i \neq j$

By the last observation and the cosine law (the equality (1'))

$$|\mathbf{x}_i - \mathbf{x}_j|^2 = 1 + 1 - 2 \cdot 1 \cdot 1 \cdot \left(-\frac{1}{d}\right) = 2 + \frac{2}{d}, \quad |\mathbf{x}_i - \mathbf{x}_j| = \sqrt{\frac{2d+2}{d}}.$$

In particular, substituting $d = 2$ or $d = 3$ we get $\sqrt{3}$ or $2\sqrt{\frac{2}{3}}$

Return to the diameter computing. We have two cases: $d = 2k$ and $d = 2k - 1$.

Case 1. Consider the points $\xi = \mathbf{x}_1 + \dots + \mathbf{x}_k$ and $\eta = \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k}$. These points do not belong to D if $k > 1$ but have some interest. So

$$\cos(\hat{\xi}, \hat{\eta}) = \frac{(\mathbf{x}_1 + \dots + \mathbf{x}_k, \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k})}{|\mathbf{x}_1 + \dots + \mathbf{x}_k| \cdot |\mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k}|} = \frac{(\mathbf{x}_1 + \dots + \mathbf{x}_k, \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k})}{|\mathbf{x}_1 + \dots + \mathbf{x}_k|^2}.$$

The numerator in the last expression (after expansion) is a sum of k^2 summands of the form $(\mathbf{x}_i, \mathbf{x}_j)$ for all i and j . Therefore, numerator equals $k^2 \cdot (-\frac{1}{2k}) = -\frac{k}{2}$. Rewrite the denominator:

$$|\mathbf{x}_1 + \dots + \mathbf{x}_k|^2 = |\mathbf{x}_1|^2 + \dots + |\mathbf{x}_k|^2 + \sum_{i \neq j} (\mathbf{x}_i, \mathbf{x}_j) = k + k \cdot (k-1) \cdot \left(-\frac{1}{2k}\right) = k - \frac{k-1}{2} = \frac{k+1}{2}.$$

Finally

$$\cos(\hat{\xi}, \hat{\eta}) = -\frac{k}{k+1}.$$

Now consider $\xi' = \frac{\xi}{|\xi|}$, $\eta' = \frac{\eta}{|\eta|}$. These points lie on the sphere and belong to the set D . By the cosine law the distance between them equals the quantity

$$|\xi' - \eta'| = \sqrt{|\xi'|^2 + |\eta'|^2 - 2 \cdot |\xi'| \cdot |\eta'| \cdot \cos(\hat{\xi}, \hat{\eta})} = \sqrt{2 - 2 \cos(\hat{\xi}, \hat{\eta})} = \sqrt{2 + \frac{2k}{k+1}}.$$

In the case 1 we found the diameter. Note that if $k = 1$ (i.e. in the second dimension) then $\xi' = \mathbf{x}_1$, $\eta' = \mathbf{x}_2$, i.e. in fact the diameter equals the side of T . However, if $k > 1$ the length of the side equals

$$\sqrt{\frac{4k+2}{2k}} = \sqrt{2 + \frac{1}{k}} < \sqrt{2 + \frac{2k}{k+1}}.$$

The length of the side tends to $\sqrt{2}$ with growth of k but the diameter of D tends even to 2, i.e. the diameter of the sphere.

Case 2. Consider the points $\xi = \mathbf{x}_1 + \dots + \mathbf{x}_k$ $\eta = \mathbf{x}_{k+1} + \dots + \mathbf{x}_{2k-1}$. Similarly to the case 1 we obtain that

$$\cos(\hat{\xi}, \hat{\eta}) = -\sqrt{\frac{k-1}{k+1}}.$$

Again consider $\xi' = \frac{\xi}{|\xi|} \in D$, $\eta' = \frac{\eta}{|\eta|} \in D$, and finally

$$|\xi' - \eta'| = \sqrt{2 + 2\sqrt{\frac{k-1}{k+1}}}.$$

In the case $k = 2$ (i.e. if $d = 3$) we get

$$\sqrt{2 + 2\sqrt{\frac{k-1}{k+1}}} = \sqrt{2 + 2\sqrt{\frac{1}{3}}} = \sqrt{2 + \frac{2\sqrt{3}}{3}} = \sqrt{2 \cdot \frac{3 + \sqrt{3}}{3}} = 2\sqrt{\frac{3 + \sqrt{3}}{6}}.$$

It is the same as in the problem 36! Clearly, points ξ' and η' are points C and A_1 respectively in the notations of the problem 36. Here we have such (expected) analogy.

40. By the problem 33 we can place any set Ω of diameter 1 into the ball B_1 with radius $\sqrt{\frac{3}{8}}$. Then translate this set so that the point $X \in \Omega$ appears on the boundary of the circle but Ω continues to lie in B_1 . Draw a ball B_2 with radius 1 and center X . Since the diameter of Ω equals 1, B_2 covers Ω also. So the intersection $B_1 \cap B_2$ covers Ω .

41. Suppose that the center of B_2 is the highest point of B_1 . Cut off the little hat from $B_1 \cap B_2$ from above by horizontal plane. Dissect the rest of $B_1 \cap B_2$ into 4 parts by the planes parallel to other coordinate planes. The diameter of each part is less than 1.

42. The regular simplex cannot be dissected into $n+1$ parts of smaller diameter.

44. A set of unit diameter can be placed into the unit cube. So it is sufficient to dissect the cube into parts of diameter less than 1. Cover the unit cube by $([\sqrt{n}] + 1)^n$ small cubes whose sides are quite smaller than $\frac{1}{\sqrt{n}}$. The main diagonal of each small cube is quite smaller than 1. Therefore $f(n) \leq ([\sqrt{n}] + 1)^n$.

45. By the solution of the problem 37 the radius of the subscribed sphere about a unit simplex in $\mathbb{R}^4$ equals $\sqrt{\frac{2}{5}}$. Similarly to the solution of the problem 33 the ball B_1 of radius $\sqrt{\frac{2}{5}}$ is a universal cover in $\mathbb{R}^4$. Similarly to the problem 40 the intersection of the ball B_1 with the unit ball (whose center lies on the boundary of B_1) is a universal cover in $\mathbb{R}^4$ also.

46. Similarly to the solution of the problem 41 cut off the small hat by horizontal plane, and dissect the rest by three other coordinate plans into 8 parts.

References

- [1] A.M. Raigorodskii, *Borsuk's problem*, Moscow, MCCME, 2006.
- [2] A.M. Raigorodskii, *A linear-algebraic method in combinatorics*, Moscow, MCCME, 2007.
- [3] V.G. Boltyanskii and I.Ts. Gohberg, *Theorems and problems in combinatorial geometry*, Moscow, "Nauka", 1965.
- [4] A.M. Raigorodskii, *Chromatic numbers*, Moscow, MCCME, 2003.

Наборы прямых на плоскости

К. Кулумжиян, Е. Молчанов, И. Шнурников

Пусть набор из n различных прямых делит плоскость на f частей. Цель следующей серии задач — найти все возможные числа f частей плоскости для фиксированного числа прямых n . В 1993 г. Н. Мартинов нашел все такие числа, а в 2007 г. В.И. Арнольд предложил новую схему доказательства, которой мы будем следовать.

Задачи до промежуточного финиша

Число прямых в наборе всегда будет обозначаться через n ($n \geq 1$), а число частей (многоугольных или неограниченных областей) плоскости, разделённой этим набором, через f .

Задача 1. Для произвольного n найдите минимальное и максимальное возможные значения f .

Задача 2. Для каждого отдельного значения n найдите все возможные числа f , где

(a) $1 \leq n \leq 5$,

(b) $n = 6, 7$.

Максимальное число параллельных прямых в наборе обозначим через p . Максимальное число проходящих через одну точку прямых в наборе обозначим через q . Число точек пересечения, каждая из которых принадлежит i прямым набора, обозначим через r_i , где $2 \leq i \leq q$.

Задача 3. Докажите, что

(a) $f \geq (p+1)(n-p+1)$,

(b) $f \geq q(n-q+2)$,

(c) оценки пунктов (a) и (b) реализуются,

(d) $f = n + 1 + \sum_{i=2}^q (i-1)r_i$.

Задача 4. Докажите, что число областей f не может принадлежать интервалам

(a) $(n+1; 2n)$ для $n \geq 3$,

(b) $(2n; 3n-3)$ для $n \geq 5$,

(c) $(3n-2; 4n-8)$ для $n \geq 8$.

Задача 5. Найдите максимальные возможные значения f для фиксированных чисел

(a) n и p ,

(b) n и q .

Для фиксированных n и p , $1 \leq p \leq n$, обозначим через $a(n, p)$ и $b(n, p)$ следующие числа:

$$b(n, p) = (p+1)(n-p+1) + C_{n-p}^2, \quad a(n, p) = b(n, p) - \min \{p, C_{n-p}^2\}.$$

Задача 6. Для любого целого числа p , $1 \leq p \leq n$, и любого целого числа f , где $a(n, p) \leq f \leq b(n, p)$, приведите пример набора из n прямых, делящего плоскость на f областей и имеющего максимум p параллельных прямых.

Основная теорема. Для фиксированного n множество всех возможных чисел f есть объединение натуральных чисел отрезков $[a(n, p); b(n, p)]$ по всем p , где $1 \leq p \leq n$.

Другими словами, все возможные числа областей f реализуются примерами задачи 6. Однако пока не очевидно, почему числа, не попадающие в отрезки $[a(n, p); b(n, p)]$, не могут быть числами областей. Дело в том, что для фиксированных чисел n и p соответствующие наборы могут делить плоскость менее чем на $a(n, p)$ частей.

Задача 7. Найдите все пары чисел n и p , для которых существует набор из n прямых, делящий плоскость на менее чем $a(n, p)$ частей.

Для данного n лакуной назовём интервал $(b(n, p+1); a(n, p))$, содержащий не менее одного целого числа. Число лакун для данного n обозначим через $L(n)$. Занумеруем лакуны числами от 1 до $L(n)$ по убыванию p (т.е. слева направо).

Задача 8. (а) Выразите число лакун $L(n)$ явной формулой через n для $n \geq 3$.

(б) Сколько целых чисел содержит лакуна номер j для $1 \leq j \leq L(n)$?

Задача 9. Предположим, что существуют n прямых, делящих плоскость на f частей, где число f принадлежит лакуне номер j . Докажите, что $p \leq j - 1$ и $q \leq j$.

Задача 10. Докажите, что

$$\sum_{i=2}^q i(i-1)r_i \geq n(n-p).$$

Задача 11. (а) Докажите, что $f \geq n + 1 + \frac{n(n-p)}{q}$.

(б) Докажите, что число f не может принадлежать лакуне номер j для $1 \leq j \leq \sqrt{n}$.

Задача 12. Докажите, что если $p < n$, то

$$r_2 + n \geq 3 + r_4 + 2r_5 + 3r_6 + \dots + (q-3)r_q.$$

Задача 13. (а) Докажите, что

$$f \geq 2 \frac{n(n-p)}{q+3}.$$

(б) Докажите, что число f не может принадлежать лакуне номер j для $1 \leq j \leq L(n) - 2$.

Задача 14. В выпуклом n -угольнике ($n \geq 4$) проведены все диагонали, причём никакие три из них не пересекаются в одной точке.

(а) Сколько получилось точек пересечения диагоналей? (Вершины не считаются точками пересечения диагоналей.)

(б) На сколько частей диагонали разбивают внутренность n -угольника?

Задача 15*. Докажите, что число f областей плоскости, разделённой n прямыми, не может принадлежать последним двум лакунам (номер $L(n) - 1$ и $L(n)$).

Задача 16*. На плоскости даны n точек, не лежащие на одной прямой. Рассмотрим прямые, проходящие ровно через две из данных точек, и обозначим число таких прямых через m . Докажите, что $C_{m+2}^2 \geq n$.

Наборы прямых на плоскости

К. Кулумжиян, Е. Молчанов, И. Шнурников

Задачи после промежуточного финиша

Рассмотрим плоскости α_1 и α_2 в трёхмерном пространстве и точку O , не лежащую ни на одной из них. *Центральным проектированием* называется преобразование, при котором точке X плоскости α_1 ставится в соответствие точка пересечения прямой OX с плоскостью α_2 .

Задача 17. Пусть на плоскости α_1 дан набор прямых. Найдите образы прямых и областей плоскости α_1 при центральном проектировании на плоскость α_2 относительно точки O . Можно считать, что в наборе есть две пересекающиеся прямые.

Будем считать, что прямые, параллельные данной прямой l , проходят через *бесконечно удалённую точку*, соответствующую направлению l . Центральное проектирование бесконечно удалённой точки, соответствующей направлению l , есть точка пересечения плоскости α_2 с прямой, проходящей через точку O параллельно l (если l параллельна α_2 , то образом будет бесконечно удалённая точка плоскости α_2 , соответствующая направлению l).

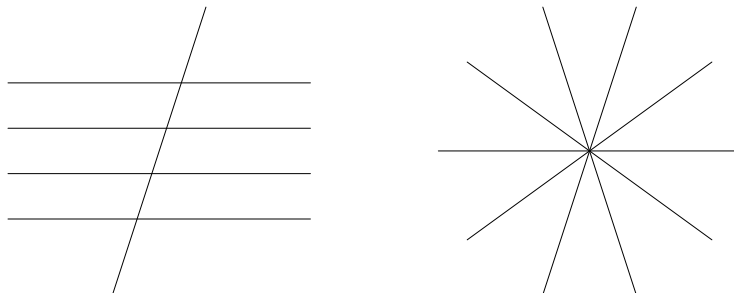
Задача 18. Докажите, что центральное проектирование есть взаимно однозначное отображение плоскостей вместе с их бесконечно удалёнными точками. Найдите образ и прообраз бесконечно удалённых точек плоскостей α_1 и α_2 , соответственно.

Назовём *проективной плоскостью* плоскость вместе с её бесконечно удалёнными точками, а *набором прямых* на проективной плоскости — набор прямых вместе с соответствующими им бесконечно удалёнными точками. При этом одна из прямых набора может быть бесконечно удалённой. Для набора n прямых на проективной плоскости обозначим через t_i число точек проективной плоскости, принадлежащих i прямой, где $2 \leq i \leq n$.

Задача 19. Докажите, что для n прямых на проективной плоскости

$$\sum_{i \geq 2} i(i-1)t_i = n(n-1).$$

Заметим, что проективная плоскость позволяет объяснить следующее сходство между параллельными прямыми и прямыми, проходящими через одну точку. Возьмём два набора из $k+1$ прямых на плоскости: первый состоит из k параллельных прямых и одной секущей, а второй из $k+1$ проходящих через одну точку прямых:



Оба набора делят плоскость на $2k + 2$ области, и это не случайное совпадение. Если к обоим наборам добавить бесконечно удалённую прямую, то получатся наборы из $k + 2$ прямых, которые переводятся друг в друга центральным проектированием и поэтому имеют одинаковое число областей. В этой связи можно ожидать, что решить задачу 15 будет проще на проективной плоскости.

Задача 20. Дано n прямых на проективной плоскости. Определите области проективной плоскости так, чтобы при центральном проектировании области переходили в области взаимно однозначно. Как по двум данным точкам и набору прямых узнать, принадлежат ли точки одной области?

В дальнейшем число областей проективной плоскости будем обозначать через f , а максимальное число прямых набора, проходящих через одну точку, через m .

Задача 21. Докажите следующие аналоги задач 3, 12 и 13.

(a)

$$f = 1 + t_2 + 2t_3 + \dots + (n - 1)t_n,$$

(b)

$$m(n - m + 1) \leq f \leq m(n - m + 1) + C_{n-m}^2.$$

(c) Если $m < n$, то

$$t_2 \geq 3 + t_4 + 2t_5 + 3t_6 + \dots + (m - 3)t_m.$$

(d) Если $m < n$, то для любого целого числа M , $M \geq m$, верно

$$f \geq 2 \left(\frac{n^2 - n + 2M}{M + 3} \right).$$

Задача 22*. Пусть $n \geq 2m + 2$ и $t_m \geq 2$. Докажите, что $f \geq (m + 1)(n - m)$. Верно ли это для $n = 2m + 1$?

Задача 23*. Сформулируйте и докажите основную теорему для наборов n прямых на проективной плоскости. Завершите доказательство основной теоремы для обычной плоскости.

Задача 24. (a) На сколько областей могут разделить плоскость n окружностей, проходящих через одну точку?

(b) Рассмотрим на сфере окружности, получаемые как сечения сферы плоскостями, проходящими через её центр. На сколько частей могут разделить сферу n таких окружностей?

Дальнейшая цель — доказать теорему Сильвестра и её обобщения.

Задача 25. (Теорема Сильвестра) (a) На плоскости даны n точек, не лежащих на одной прямой. Докажите, что найдётся прямая, на которой лежат только две данные точки.

(b) На плоскости проведены n прямых, причём не все они параллельны и не все пересекаются в одной точке. Докажите, что найдётся точка, принадлежащая ровно двум прямым.

Оказывается, что в условиях задачи 25(b) найдётся несколько таких точек. Чтобы оценить их число, удобнее рассматривать наборы прямых на проективной плоскости.

Обозначим через p_j число j -угольных областей проективной плоскости, образованных этим набором прямых.

Задача 26. Докажите, что если $t_n = 0$, то

$$\sum_{i \geq 2} (3-i)t_i + \sum_{j \geq 3} (3-j)p_j = 3.$$

Задача 27. Дан набор n прямых на проективной плоскости такой, что $t_n = 0$. Найдите минимальные возможные значения t_2 отдельно для каждого $n \leq 9$.

Задача 28. (а) Приведите примеры наборов n прямых с $t_2 = \frac{n}{2}$ для чётных $n \geq 6$.

(б) Приведите примеры наборов n прямых с $t_2 = 3 \left\lfloor \frac{n}{4} \right\rfloor$ для нечётных $n \geq 7$.

Задача 29★. Докажите, что если $t_n = 0$, то $t_2 \geq \frac{3}{7}n$.

Задача 30★. (Гипотеза Дирака 1951-го года). Если $t_n = 0$, то $t_2 \geq \left\lfloor \frac{n}{2} \right\rfloor$.

Очередная цель — доказать ряд неравенств, в которых участвуют сразу несколько чисел t_i .

Задача 31*. Если $t_n = t_{n-1} = t_{n-2} = 0$, то

$$t_2 + \frac{3}{2}t_3 \geq 8 + \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i.$$

Задача 32. Дано n прямых на проективной плоскости. Отметим красным цветом точки пересечения, принадлежащие ровно двум прямым. Синим цветом отметим точки пересечения, принадлежащие не менее чем трём прямым. Отрезки прямых с одноцветными концами, не содержащие внутри себя цветных точек, покрасим в цвет своих концов. Обозначим через x и y числа красных и синих отрезков соответственно. Покрасим зелёным цветом области, ограниченные не менее чем четырьмя отрезками данных прямых и содержащие на своей границе хотя бы одну красную точку. Число пар, состоящих из зелёной области и лежащей на её границе синей точки, обозначим через z . Докажите, что

(а)

$$x - y = 2t_2 - \sum_{i \geq 3} it_i.$$

(б) Если не существует таких двух точек, что любая данная прямая проходит хотя бы через одну из них, то

$$y + z \geq \frac{3}{2} \sum_{i \geq 3} t_i.$$

(с) Если $t_n = t_{n-1} = t_{n-2} = 0$, то

$$x + z \leq 3p_4 + \sum_{j \geq 5} jp_j.$$

Задача 33*. Найдите новые соотношения между t_i и p_j (не выводимые тривиально из задач 26 и 31, но, возможно, использующие задачу 32).

Наборы прямых на плоскости

Решения задач до промежуточного финиша

Задача 1. Ответ: $n + 1 \leq f \leq \frac{n(n+1)}{2} + 1$. Оба неравенства доказываются индукцией по n , база $n = 1$, $f = 2$. Если добавляемая прямая пересекает предыдущие в x точках, то при её добавлении число областей увеличивается на $x + 1$. Следовательно, при добавлении n -й прямой число областей увеличивается не менее, чем на 1, и не более, чем на n .

Задача 2. Ответ:

$n=1$, $f = 2$,

$n=2$, $f \in \{3, 4\}$,

$n=3$, $f \in \{4, 6, 7\}$,

$n=4$, $f \in \{5, 8, \dots, 11\}$,

$n=5$, $f \in \{6, 10, 12, \dots, 16\}$,

$n=6$, $f \in \{7, 12, 15, \dots, 22\}$,

$n=7$, $f \in \{8, 14, 18, \dots, 29\}$.

Невозможность остальных чисел следует из задач 1 и 3(a)(b).

Задача 3. (a) Рассмотрим p параллельных прямых набора и будем добавлять остальные прямые набора по очереди. Очередная прямая имеет не менее p точек пересечения с предыдущими прямыми, поэтому при её добавлении число областей увеличится на не менее, чем $p + 1$. Добавив $n - p$ прямых, получим $f \geq (p + 1)(n - p + 1)$.

(b) Рассмотрим q пересекающихся в одной точке прямых набора и будем добавлять остальные прямые набора по очереди. Очередная прямая имеет не менее $q - 1$ точек пересечения с предыдущими прямыми, поэтому при её добавлении число областей увеличится на не менее, чем q . Добавив $n - q$ прямых, получим $f \geq q(n - q + 2)$.

(c) Рассмотрим p параллельных прямых, через некоторую точку на одной из них поведем остальные $n - p$ прямых поочерёдно. При добавлении каждой прямой число областей увеличивается на p и в итоге будет равно $(p + 1)(n - p)$.

Рассмотрим q прямых, проходящих через одну точку. Будем проводить остальные $(n - q)$ прямых параллельно одной из первых q прямых по очереди. Тогда при добавлении очередной прямой число областей увеличивается на q и в итоге будет равно $q(n - q + 2)$.

(d) *Решение 1.* Будем добавлять прямые поочерёдно. Если очередная прямая пересекает предыдущие в x точках, то её добавление увеличивает число областей на $x + 1$. С другой стороны, каждая из этих x точек пересечения или имеет кратность два, или до добавления прямой имела кратность на единицу меньше. Следовательно, сумма $\sum_{i \geq 2} (i - 1)r_i$ при добавлении этой прямой увеличивается на x .

Решение 2. Пересечём набор прямых с кругом достаточно большого радиуса, содержащим внутри себя все точки пересечения прямых набора. Рассмотрим граф, вершины которого — точки пересечения прямых друг с другом и с окружностью круга, рёбра —

отрезки прямых и дуги окружности, не содержащие отличных от своих концов вершин графа. Число вершин v и рёбер e этого графа равны $2n + \sum_{i \geq 2} r_i$ и $3n + \sum_{i \geq 2} i r_i$ соответственно. Число f частей плоскости, разделённой набором прямых, на единицу меньше числа областей, образованных графом. Следовательно, по формуле Эйлера для графов имеем

$$f = n + 1 + \sum_{i \geq 2} (i - 1) r_i.$$

Задача 4. (а) Если все прямые параллельны, то $f = p + 1$. Если не все прямые параллельны, то $1 \leq p \leq n - 1$. По задаче 3 имеем $f \geq (p + 1)(n - p + 1)$. Выражение $(p + 1)(n - p + 1)$ есть квадратный трёхчлен относительно p с отрицательным старшим коэффициентом. При $p = 1$ и $p = n - 1$ трёхчлен $(p + 1)(n - p + 1)$ принимает значение $2n$. Следовательно, при $1 \leq p \leq n - 1$ трёхчлен $(p + 1)(n - p + 1)$ принимает значения, не меньшие $2n$.

(б) Если все или все кроме одной прямой параллельны, то $f = n + 1$ или $f = 2n$. По задаче 3(а) имеем $f \geq (p + 1)(n - p + 1)$. Выражение $(p + 1)(n - p + 1)$ есть квадратный трёхчлен относительно p с отрицательным старшим коэффициентом. При $p = 2$ и $p = n - 2$ трёхчлен $(p + 1)(n - p + 1)$ принимает значение $3n - 3$. Следовательно, при $2 \leq p \leq n - 2$ трёхчлен $(p + 1)(n - p + 1)$ принимает значения, не меньшие $3n - 3$. Поэтому при $2 \leq p \leq n - 2$ имеем $f \geq 3n - 3$. Если $p = 1$, то по задаче 3(б) имеем $f \geq q(n - q + 2)$. Если $q = n$, то $f = 2n$. Рассмотрим квадратный трёхчлен $q(n - q + 2)$. При $3 \leq q \leq n - 1$ имеем $f \geq q(n - q + 2) \geq 3n - 3$. Остался случай $p = 1$ и $q = 2$, в котором число областей равно

$$1 + \frac{n(n + 1)}{2} \geq 3n - 3 \quad \Leftrightarrow \quad n^2 - 5n + 8 \geq 0.$$

(с) Если $p \geq n - 2$ или $q \geq n - 1$, то $f \leq 3n - 2$. Если $3 \leq p \leq n - 3$ или $4 \leq q \leq n - 2$, то по задаче 3 получим $f \geq 4n - 8$. Остался случай $p \leq 2$ и $q \leq 3$. По задаче 3 имеем $f = n + 1 + r_2 + 2r_3$. Каждая прямая набора пересекается не менее, чем с $n - 2$ другими. Поэтому число пар пересекающихся прямых равно $r_2 + 3r_3$ и не меньше, чем $\frac{n(n-2)}{2}$. Следовательно,

$$f \geq n + 1 + \frac{2}{3}(r_2 + 3r_3) \geq n + 1 + \frac{n^2 - 2n}{3} \geq 4n - 8$$

при $n \geq 8$.

Задача 5. (а) Рассмотрим p параллельных прямых набора из n прямых и будем добавлять остальные прямые по очереди. Очередная прямая номер i , $1 \leq i \leq n - p$ пересекает предыдущие прямые в не более, чем $p + i - 1$ точках и поэтому её добавление увеличивает число областей на не более, чем $p + i$. Добавив $n - p$ прямых, получим

$$f \leq (p + 1)(n - p + 1) + C_{n-p}^2.$$

Оценка достигается для наборов p параллельных прямых и $n - p$ прямых общего положения (т.е. никакие две не параллельны и никакие три не проходят через одну точку), находящихся также в общем положении с p параллельными прямыми.

(б) Рассмотрим q пересекающихся в одной точке прямых набора из n прямых и будем добавлять остальные прямые по очереди. Очередная прямая номер i , $1 \leq i \leq n - q$, пересекает предыдущие прямые в не более, чем $q + i - 1$ точках, и поэтому её добавление увеличивает число областей на не более, чем $q + i$. Добавив $n - q$ прямых, получим

$$f \leq q(n - p + 2) + C_{n-q+1}^2 = 1 + C_{n+1}^2 - C_{q-1}^2.$$

Оценка достигается для наборов q пересекающихся в одной точке прямых и $n - q$ прямых общего положения, находящихся также в общем положении с q пересекающимися прямыми.

Задача 6. Возьмем $n - p$ прямых в общем положении. Выберем t точек из их точек пересечения для некоторого $t \leq \min\{p, C_{n-p}^2\}$. Проведем p параллельных прямых так, чтобы они проходили через выбранные точки пересечения и не проходили бы через другие точки пересечения $n - p$ прямых между собой. При этом выберем направление для p параллельных прямых отличным от любой из первых $n - p$ прямых. Тогда предъявленный набор имеет максимум p параллельных прямых и делит плоскость на

$$f = (p + 1)(n - p + 1) + C_{n-p}^2 - t$$

частей.

Задача 7. Минимальное число областей для наборов прямых с данными числами n, p равно $(p + 1)(n - p + 1)$. Достигается, например, если $n - p + 1$ прямых проходят через одну точку, а все остальные $p - 1$ прямых параллельны одной из $n - p + 1$ прямых. Осталось заметить, что

$$(p + 1)(n - p + 1) < a(n, p) \Leftrightarrow C_{n-p}^2 > p \Leftrightarrow n > p + \frac{1}{2} + \sqrt{2p + \frac{1}{4}}.$$

В последнем равносильном переходе можно было прийти к $n \geq p + \frac{1}{2} + \sqrt{2p + \frac{9}{4}}$.

Задача 8. (а) $L(n) = \max\{k \geq 1 \mid b(n, n - k + 1) \leq a(n, n - k) - 2\}$ при $n \geq 3$,

$$\begin{aligned} b(n, n - k + 1) \leq a(n, n - k) - 2 &\Leftrightarrow \min\left\{n - k, \frac{k(k - 1)}{2}\right\} \leq n - k - 2 \Leftrightarrow \\ &\Leftrightarrow n \geq \frac{k^2 + k}{2} + 2 \Leftrightarrow k \leq \sqrt{2n - \frac{15}{4}} - \frac{1}{2}. \end{aligned}$$

Откуда $L(n) = \left\lfloor \sqrt{2n - \frac{15}{4}} - \frac{1}{2} \right\rfloor$.

(б) Так как

$$n \geq \frac{L^2(n) + L(n)}{2} + 2, \text{ то } \min\left\{n - j, \frac{j(j - 1)}{2}\right\} = \frac{j(j - 1)}{2} \text{ при } 1 \leq j \leq L(n).$$

Поэтому $a(n, n - j) = (n - j + 1)(j + 1)$, и лакуна номер j содержит $n - \frac{j(j+1)}{2} - 1$ целое число.

Задача 9. Если $j \leq p \leq n - j$ или $j + 1 \leq q \leq n - j + 1$, то по задаче 3 получаем $f \geq (n - j + 1)(j + 1) = a(n, n - j)$. Если $p \geq n - j + 1$, то вследствие задачи 5 получаем

$$f \leq (p + 1)(n - p + 1) + C_{n-p}^2 \leq b(n, n - j + 1).$$

Если $q \geq n - j + 2$, то вследствие задачи 5 имеем

$$f \leq q(n - q + 2) + C_{n-q}^2 + 1 \leq b(n, n - j + 1).$$

Задача 10. Число пар пересекающихся прямых равно $\sum_{i=2}^q \frac{i(i-1)}{2} r_i$ и не меньше, чем $\frac{n(n-p)}{2}$, поскольку каждая прямая пересекается с не менее, чем $n - p$ прямыми.

Задача 11. (а) По задачам 3 и 10 имеем

$$f - (n + 1) = \sum_{i \geq 2} (i - 1)r_i \geq \sum_{i \geq 2}^q \frac{i(i - 1)}{q} r_i \geq \frac{n(n - p)}{q}.$$

(б) Предположим противное, тогда по задаче 9 имеем $p \leq j - 1$ и $q \leq j$, где j — номер лакуны. Используя $n - p \geq n - j + 1$, получаем противоречие с предыдущим пунктом:

$$f \geq n + 1 + \frac{n(n - p)}{q} \geq (n - j + 1)\left(\frac{n}{q} + 1\right) \geq (n - j + 1)(j + 1) = a(n, n - j).$$

Задача 12. Пересечём набор прямых с кругом достаточно большого радиуса, содержащим внутри себя все точки пересечения прямых набора. Получим граф, вершины которого — точки пересечения прямых друг с другом и с окружностью круга, рёбра — отрезки прямых и дуги окружности, не содержащие отличных от своих концов вершин графа. Число вершин v и рёбер e этого графа равны $2n + \sum_{i \geq 2} r_i$ и $3n + \sum_{i \geq 2} ir_i$ соответственно. Внутри круга находится f областей, где

$$f = n + 1 + \sum_{i \geq 2} (i - 1)r_i.$$

Сумма по всем областям внутри круга числа ограничивающих их рёбер равна

$$2e - 2n = 4n + 2 \sum_{i \geq 2} ir_i.$$

Так как $p < n$, то каждая область внутри круга ограничена не менее, чем тремя рёбрами графа. Следовательно, $2e - 2n \geq 3f$, откуда получаем требуемое неравенство.

Задача 13. (а) Положим $a = \frac{2}{q+3}$, $b = \frac{q-1}{q+3}$. Рассмотрим квадратный трёхчлен относительно переменной i

$$a(i^2 - i) + b(3 - i) - (i - 1) = a(i - 2)(i - q) \leq 0 \quad \text{при} \quad 2 \leq i \leq q.$$

Умножим соответствующие значения многочлена на r_i и сложим по всем $2 \leq i \leq q$:

$$0 \geq a \sum_{i=2}^q i(i - 1)r_i + b \sum_{i=2}^q (3 - i)r_i - \sum_{i=2}^q (i - 1)r_i \geq an(n - p) + b(3 - n) - (f - n - 1),$$

где последнее неравенство получено из задач 10, 12 и 3. Следовательно,

$$f \geq 2\frac{n(n - p)}{q + 3} + (n + 1 + \frac{q - 1}{q + 3}(3 - n)) \geq 2\frac{n(n - p)}{q + 3}.$$

(б) Предположим противное, тогда по задаче 9 имеем $p \leq j - 1$ и $q \leq j$. Используя $n - p \geq n - j + 1$, получаем противоречие с предыдущим пунктом:

$$f \geq 2\frac{n(n - p)}{q + 3} \geq (n - j + 1)\frac{2n}{q + 3} \geq (n - j + 1)(j + 1) = a(n, n - j),$$

т.к.

$$\frac{(q + 3)(j + 1)}{2} \leq \frac{j^2 + 4j + 3}{2} \leq \frac{1}{2}L^2(n) < n.$$

Задача 14. (а) Точка пересечения определяет две проходящие через неё диагонали и их концы, т.е. четвёрку вершин n -угольника. Обратно, каждая четвёрка различных вершин n -угольника определяет одну точку пересечения диагоналей. Следовательно, число точек пересечения равно C_n^4 .

(б) *Решение 1.* Будем проводить диагонали по очереди. Если добавленная диагональ имеет x точек пересечения с предыдущими диагоналями, то она увеличивает число частей внутренности n -угольника на $x + 1$. Значит, каждая точка пересечения и каждая диагональ увеличивает число частей на единицу. Тогда искомое число частей равно $1 + C_n^4 + \frac{n(n-3)}{2}$, т.к. число точек пересечения известно из предыдущего пункта, а число диагоналей равно $\frac{n(n-3)}{2}$.

Решение 2. Рассмотрим граф с вершинами в точках пересечения диагоналей и вершинах n -угольника, рёбра которого суть отрезки диагоналей и стороны n -угольника. В таком графе $v = n + C_n^4$ вершин и $e = 2C_n^4 + \frac{n(n-1)}{2}$ рёбер. Откуда по формуле Эйлера число частей равно $1 + e - v = 1 + C_n^4 + \frac{n(n-3)}{2}$.

Задача 15. См. задачу 23.

Задача 16. Нарисуем на плоскости прямые, каждая из которых проходит через две из данных точек. Эти m прямых разобьют плоскость на не более, чем $1 + m + C_m^2$ областей. Рассмотрим все точки данного множества, через которые не проходит ни одной прямой, проходящей ровно через две точки данного множества. Оказывается, что в каждой области, образованной набором m прямых, находится не более одной такой точки (это остаётся вам доказать). Также остаётся найти m областей, внутри которых таких точек нет. На m прямых находится не более $2m$ точек данного множества. Поэтому $n \leq 2m + 1 + C_m^2 = C_{m+2}^2$.

Решения задач после промежуточного финиша

Задача 17. Для параллельных плоскостей α_1 и α_2 центральное проектирование есть преобразование подобия, переводящее прямые в прямые и области в области. Пусть плоскости α_1 и α_2 пересекаются и пусть l_1 и l_2 — прямые пересечения плоскостей α_1 и α_2 с плоскостями, проходящими через точку O параллельно плоскостям α_2 и α_1 соответственно. Образ отличной от l_1 прямой l есть прямая, если $l \parallel l_1$, и есть прямая с выколотой точкой (точкой пересечения с l_2), если $l \not\parallel l_1$. Если область пересекает l_1 , то её образ состоит из двух неограниченных областей. Если неограниченная область примыкает к двум непараллельным лучам, то её образ примыкает к l_2 .

Задача 18. Взаимная однозначность вытекает из определений. Образом и прообразом будут соответственно прямые l_2 и l_1 вместе со своими бесконечно удалёнными точками. Прямые l_1 и l_2 — прямые пересечения плоскостей α_1 и α_2 с плоскостями, проходящими через точку O параллельно плоскостям α_2 и α_1 соответственно.

Задача 19. Любые две прямые имеют ровно одну общую точку на плоскости с бесконечно удалёнными точками (если прямые параллельны или одна из них бесконечно удалена, то эта общая точка бесконечно удалена). Количество пар прямых равно C_n^2 . В точке, принадлежащей i прямым, пересекается C_i^2 пар прямых, откуда и получаем требуемое.

Задача 20. Определим, что такое «область» проективной плоскости, разделённой набором n прямых, предположив сначала, что не все прямые проходят через одну точку. Если одна из прямых набора бесконечно удалена, то областями будем называть

части обычной плоскости, разделённой остальными $n - 1$ прямыми. Если в наборе нет бесконечно удалённой прямой, тогда областью будет называться:

- ограниченная область плоскости,
- неограниченная область плоскости, примыкающая к двум параллельным лучам,
- пара неограниченных областей плоскости, одна из которых примыкает к непараллельным лучам l_1 и l_2 , а другая к непараллельным лучам l_3 и l_4 при условии $l_1 \parallel l_3$ и $l_2 \parallel l_4$. При этом считается, что бесконечно удалённые точки, соответствующие направлениям от l_1 до l_2 , соединяют неограниченные области пары и вместе с ними входят в одну область на проективной плоскости.

Если же все прямые набора проходят через одну точку проективной плоскости, то «области» определяются аналогично. Две точки принадлежат одной области тогда и только тогда, когда их можно соединить ломаной, не пересекающей прямые. При этом концы ломаной совпадают с данными точками, а промежуточные вершины могут быть бесконечно удалёнными точками. Звеньями ломаной, выходящими из бесконечно удалённой точки, считаются лучи, параллельные направлению этой бесконечно удалённой точки. При центральном проектировании так доопределённая ломаная переходит в ломаную. Следовательно, две точки находятся в одной области тогда и только тогда, когда их образы при центральном проектировании находятся в одной области. Это означает взаимно однозначное соответствие областей.

Задача 21. (а) *Решение 1.* Переведем одну из прямых набора центральным проектированием в бесконечно удалённую. Число областей и числа t_i при этом не изменятся. Теперь число областей проективной плоскости совпадает с числом f областей обычной плоскости, разделённой набором из $n - 1$ прямыми. По задаче 3 имеем $f = n + \sum_{i \geq 2} (i - 1)r_i$. Осталось заметить, что

$$n - 1 = \sum_{i \geq 2} (i - 1)(t_i - r_i),$$

т.к. на бесконечно удалённой прямой находятся $t_i - r_i$ точек пересечения, принадлежащих $i - 1$ прямым набора, на считая бесконечно удалённой.

Решение 2. Индукция по числу прямых, база $n = 1$. Для перехода заметим, что добавляемая прямая увеличивает число областей на количество своих точек пересечения с предыдущими прямыми.

(б) Индукция по n , база $n = m, f = m$. Добавляемая прямая номер j , $1 \leq j \leq n - m$, имеет не менее m и не более $m + j - 1$ точек пересечения с предыдущими прямыми, т.к. на проективной плоскости любые две прямые пересекаются. Осталось заметить, что добавляемая прямая увеличивает число областей на количество своих точек пересечения с предыдущими прямыми.

(в) Рассмотрим граф на проективной плоскости, вершины которого — точки пересечения прямых друг с другом, рёбра — отрезки прямых. При этом допускается прохождение ребра через бесконечно удалённую точку, в этом случае ребро состоит из двух лучей, лежащих на одной прямой, и бесконечно удалённой точки соответствующего направления, соединяющей два луча. Число вершин v и рёбер e этого графа равны $\sum_{i \geq 2} r_i$ и $\sum_{i \geq 2} i r_i$ соответственно. Если $m < n$, то каждая область проективной плоскости ограничена не менее чем тремя рёбрами графа, поэтому

$$3f \leq 2e \Leftrightarrow 3 + 3 \sum_{i \geq 2} (i - 1)t_i \leq 2 \sum_{i \geq 2} i r_i \Leftrightarrow \sum_{i \geq 2} (3 - i)t_i \geq 3.$$

(d) Положим $a = \frac{2}{M+3}$ и $b = \frac{M-1}{M+3}$. Рассмотрим квадратный трёхчлен относительно переменной i

$$a(i^2 - i) + b(3 - i) - (i - 1) = a(i - 2)(i - M) \leq 0 \quad \text{при} \quad 2 \leq i \leq m.$$

Умножим соответствующие значения многочлена на t_i и сложим по всем $2 \leq i \leq m$:

$$0 \geq a \sum_{i=2}^m i(i-1)t_i + b \sum_{i=2}^m (3-i)t_i - \sum_{i=2}^m (i-1)t_i \geq an(n-1) + 3b - (f-1),$$

где последнее неравенство получено из задач 19, 21(a) и (c). Следовательно,

$$f \geq 2 \frac{n(n-1)}{M+3} + \left(1 + \frac{3(M-1)}{M+3}\right) = 2 \frac{n(n-1) + 2M}{M+3}.$$

Задача 22*. Выберем две точки P и Q , через каждую из которых проходит m прямых. Обозначим через N множество прямых исходного набора, проходящих через хотя бы одну из точек P и Q . Возможны два случая:

(i) прямая PQ не принадлежит набору. В этом случае N содержит $2m$ прямых и делит проективную плоскость (без учёта остальных прямых) на $m^2 + 2m - 1$ область.

(ii) прямая PQ принадлежит набору. В этом случае N содержит $2m - 1$ прямых и делит проективную плоскость (без учёта остальных прямых) на m^2 область.

В обоих случаях каждая из оставшихся прямых набора (не принадлежащая N) пересекает прямые из N не менее чем в m точках, причём существует не более двух прямых, пересекающих прямые из N ровно в m точках. Тем самым случай (i) разобран, поскольку

$$f \geq m^2 + 2m - 1 + (m+1)(n-2m) - 2 \geq (m+1)(n-m).$$

Рассмотрим случай (ii). Если набор прямых содержит не более одной прямой, пересекающей N в m точках, то тогда оцениваем число областей через число точек пересечения остальных прямых:

$$f \geq m^2 + (m+1)(n-2m+1) - 1 = (m+1)(n-m).$$

Если набор прямых содержит две прямые, пересекающие N в m точках каждая, и их точка пересечения не лежит на прямых N , то аналогично получим $f \geq (m+1)(n-m)$.

Остался случай, когда набор содержит две прямые, пересекающие N в m точках каждая, и их точка пересечения лежит на прямых N . Обозначим эти прямые через l_{2m} и l_{2m+1} , а их точку пересечения через R . Докажем в этом случае, что любая другая прямая набора пересекает $N \cup l_{2m} \cup l_{2m+1}$ не менее, чем в $m+2$ точках. Из этого вытекает, что

$$f \geq m^2 + 2m + (m+2)(n-2m-1) \geq (m+1)(n-m),$$

и тем самым доказательство случая (ii) будет завершено.

Обозначим прямые, проходящие через точку P , по порядку их следования, считая от прямой PQ , $l_1, \dots, l_{m-1}$. Аналогично обозначим прямые, проходящие через точку Q , по порядку их следования, считая от прямой PQ , $l_m, \dots, l_{2m-2}$. Обозначим через $A_{i,j}$ точку пересечения прямых l_i и l_{m-1+j} для $1 \leq i, j \leq m-1$. Не ограничивая общности, будем считать прямую PQ бесконечно удалённой, прямую l_{2m} проходящей через точки $A_{i,i}$ для $1 \leq i \leq m-1$, прямую l_{2m+1} проходящей через точки $A_{i,m-i}$ для $1 \leq i \leq m-1$. Тогда

прямые l_{2m} и l_{2m+1} пересекаются в точке $A_{\frac{m}{2}, \frac{m}{2}}$ и m чётно. Рассмотрим произвольную оставшуюся прямую l из набора. Она пересекает N не менее, чем в $m + 1$ точке. Если хотя бы одна точка пересечения l с l_{2m} или с l_{2m+1} не лежит на прямых из N , то тогда l пересекает $N \cup l_{2m} \cup l_{2m+1}$ не менее, чем в $m + 2$ точках.

Заметим, что если прямая l проходит через точку $A_{\frac{m}{2}, \frac{m}{2}}$, то точки пересечения прямой l с прямыми $l_{\frac{m}{2}-1}$ и $l_{\frac{m}{2}+1}$ или с прямыми $l_{m-1+\frac{m}{2}-1}$ и $l_{m-1+\frac{m}{2}+1}$ отличны от точек A_{ij} . Следовательно, прямая l пересекает N не менее, чем в $m + 2$ точках.

Не ограничивая общности, будем считать, что точка пересечения прямых l и PQ и точка пересечения прямых l_{2m} и PQ лежат на одном отрезке прямой PQ , образованном точками P и Q . Тогда прямая l пересекает l_{2m+1} в точке $A_{a,b}$ с $|a-b| \geq 2$. Следовательно, прямая l проходит через не более чем $\min\{a, b\} + \min\{m-1-a, m-1-b\} \leq m-3$ точек из точек $A_{i,j}$. Значит, прямая l пересекает N не менее, чем в $m + 2$ точках.

Для $n = 2m + 1$ утверждение неверно, пример строится для чётного $m \geq 4$ следующим образом. Через точки P и Q проходят по m прямых, причём прямая PQ общая. Ещё две прямые пересекают эти $2m - 1$ прямые в m точках каждая. В итоге $f = m^2 + 2m < (m + 1)^2$.

Задача 23*. При добавлении к набору бесконечно удалённой прямой число областей не меняется, число прямых n увеличивается на 1, а вместо p параллельных прямых получается $p + 1$ прямых, проходящих через одну точку. Соответственно получаем:

Число f областей может быть числом областей проективной плоскости, разделённой n прямыми, тогда и только тогда, когда f принадлежит хотя бы одному из отрезков $[a(n, m), b(n, m)]$ для $n \geq m \geq 2$, где

$$b(n, m) = m(n - m + 1) + C_{n-m}^2, \quad a(n, m) = b(n, m) - \min\{m - 1, C_{n-m}^2\}.$$

Лакуной будет также называться интервал $(b(n, m), a(n, m - 1))$, содержащий не менее одного целого числа. Из задачи 8 получаем, что $L(n) = \left\lceil \sqrt{2n - 5\frac{3}{4} - \frac{1}{2}} \right\rceil$. В дальнейшем зависимость $L = L(n)$ от n будем опускать. После задачи 13 осталось доказать, что число областей не может принадлежать последним двум лакунам номер $L - 1$ и L .

Предположим, что существует набор прямых, для которого число f принадлежит предпоследней лакуне — интервалу

$$((n - L + 2)(L - 1) + C_{L-2}^2, L(n - L + 1)).$$

Из задачи 9 следует, что $m = \max\{p + 1, q\} \leq L - 1$. Применим задачу 21 для $M = L - 1$:

$$f \geq \frac{2(n^2 - n)}{L + 2} \geq L(n - L + 1).$$

В последнем неравенстве использовалось $n \geq \frac{L^2 + L}{2} + 3$ следующим образом:

$$n^2 - n \geq (n + \frac{L}{2} - 3)(n - L + 1) \geq \left(\frac{L^2 + 2L}{2}\right)(n - L + 1).$$

Тем самым получено противоречие с тем, что число f принадлежит предпоследней лакуне.

Предположим, что существует набор прямых на проективной плоскости, для которого число областей попадает в последнюю лакуну номер L :

$$f \in (L(n - L + 1) + C_{L-1}^2, (L + 1)(n - L)).$$

По задаче 4 можно считать, что $L \geq 4$. В силу задачи 9 имеем $m \leq L$. Рассмотрим 3 случая.

(1) Если $m < L$, то по задаче 21(d) для $M = L - 1$ получаем

$$f > \frac{2(n^2 - n)}{L + 2} \geq (L + 1)(n - L),$$

т.к. из $n \geq \frac{n^2 + n}{2} + 3$ следует, что

$$\frac{(L + 2)(L + 1)}{2}(n - L) \leq (n + L - 2)(n - L) \leq n^2 - 2n.$$

(2) Если $m = L$ и $t_m = 1$, то удалим из набора одну прямую, проходящую через точку, принадлежащую m прямым. Число областей при этом только уменьшится. Применим к полученному набору из $n - 1$ прямой неравенство задачи 21(d) для $M = L - 1$ и получим

$$f \geq 2 \left(\frac{n^2 - 3n + 2L}{L + 2} \right) \geq (L + 1)(n - L).$$

Обоснуем последнее неравенство. Если $n \geq \frac{L^2 + L}{2} + 4$, то

$$n^2 - 3n + 2L \geq (n - L)(n + L - 3) \geq (n - L) \left(\frac{L^2 + 3L + 2}{2} \right).$$

Случай $n = \frac{L^2 + L}{2} + 3$ проверяется непосредственной проверкой.

(3) Если $m = L$ и $t_m \geq 2$, то $n \geq 2m + 2$ и из предыдущего пункта получаем $f \geq (L + 1)(n - L)$.

Задача 24. (а) Ответ: это множество чисел из основной теоремы для наборов n прямых на плоскости. Сделаем инверсию относительно некоторой окружности с центром в точке, принадлежащей всем окружностям набора. Получится набор прямых, число областей при этом не изменится. Обратно, если дан набор прямых, то можно сделать инверсию относительно окружности, чей центр не принадлежит прямым. Получится набор окружностей, число областей при этом не изменится.

(б) Ответ: это множество удвоенных чисел областей из основной теоремы для проективной плоскости. Рассмотрим проекцию сферы из её центра O на плоскость α , касающуюся сферы в южном полюсе. При этой проекции точка X сферы переходит в точку пересечения прямой OX с плоскостью α . Если прямая OX параллельна плоскости α , то точка X переходит в бесконечно удалённую точку по направлению OX . При этой проекции большие круги на сфере перейдут в прямые на проективной плоскости. А пара противоположных областей сферы перейдёт в одну область проективной плоскости. Следовательно, число областей сферы в два раза больше числа областей проективной плоскости, разделённой соответствующим набором прямых. Наоборот, по любому набору прямых на проективной плоскости можно при помощи обратной проекции на сферу получить набор больших кругов и удвоенное число областей.

Задача 25. (а) Рассмотрим пару «прямая AB , не лежащая на ней точка C » такую, что точки A, B, C принадлежат заданному множеству, и расстояние от точки C до прямой AB минимально среди всех таких пар. Предположим, что на прямой AB находится точка D из исходного множества. Не ограничивая общности, будем считать, что точка D находится между точками A и B и что угол $ADC \geq 90^\circ$. Тогда расстояние

от точки D до прямой AC будет меньше расстояния от точки C до прямой AB , что противоречит выбору точек A, B, C . Следовательно, на прямой AB нет отличных от A и B точек данного множества.

(b) *Решение 1.* Предположим противное. Случай, когда все прямые параллельны одной из двух данных прямых, разбирается отдельно. Далее считаем, что среди прямых набора найдутся три попарно не параллельные и не пересекающиеся в одной точке. Рассмотрим все треугольники, образованные тройками исходных прямых, и выберем треугольник ABC минимальной (ненулевой) площади. Поскольку через его вершины A, B и C проходит не менее трёх данных прямых и его площадь минимальная, то прямые, проходящие через вершины A, B и C параллельно BC, CA и AB соответственно, принадлежат данному набору. Обозначим точки пересечения этих прямых через A_1, B_1 и C_1 . Треугольник ABC — серединный треугольник для треугольника $A_1B_1C_1$. Следовательно, площади треугольников A_1BC, B_1CA и C_1AB равны площади ABC . Аналогично рассмотрим треугольники A_1BC, B_1CA и C_1AB вместо ABC и т.д. В итоге получим неограниченное число прямых. Противоречие.

Решение 2. Сведём задачу к предыдущей при помощи полярной (или проективной) двойственности. Рассмотрим окружность, чей центр не принадлежит данным прямым. Сделаем полярное преобразование относительно этой окружности, т.е. каждой точке поставим в соответствие её поляр, а каждой поляре поставим в соответствие её полюс. Набор из n прямых перейдёт в набор из n точек, не лежащих на одной прямой. По предыдущему пункту найдётся прямая l , на которой лежат ровно два полюса, A и B . Сделаем обратное полярное преобразование и получим, что через полюс L прямой l проходит ровно две прямые из набора — поляры a и b точек A и B . Здесь использовался факт, что поляра точки пересечения двух прямых совпадает с прямой, проходящей через их полюса.

Задача 26. Рассмотрим граф на проективной плоскости, вершины которого — точки пересечения прямых, рёбра — отрезки прямых, не содержащие внутри себя точек пересечения. Обозначим через v и e число вершин и рёбер графа соответственно. Через f обозначим, как обычно, число областей проективной плоскости. Не умаляя общности, будем считать, что одна из прямых набора бесконечно удалена. Если это не так, подберём центральное проектирование так, чтобы некоторая прямая набора стала бесконечно удалённой, числа v, e, f, t_i и p_j при этом не изменятся. Заметим, что если связный граф на проективной плоскости содержит все бесконечно удалённые точки, то верна формула Эйлера $v - e + f = 1$. Поскольку $t_n = 0$, то все области проективной плоскости, образованные графом, ограничены не менее, чем тремя рёбрами. Следовательно, $p_2 = 0$. Заметим, что тогда

$$v = \sum_{i \geq 2} t_i, \quad e = \sum_{i \geq 2} i t_i = \frac{1}{2} \sum_{j \geq 3} j p_j, \quad f = \sum_{j \geq 3} p_j.$$

Следовательно,

$$3 = 3f - (2e + e) + 3v = 3 \sum_{j \geq 3} p_j - \left(\sum_{j \geq 3} j p_j + \sum_{i \geq 2} i t_i \right) + 3 \sum_{i \geq 2} t_i = \sum_{j \geq 3} (3 - j) p_j + \sum_{i \geq 2} (3 - i) t_i.$$

Задача 27. Ответ: $\frac{n : \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9}{t_2 : \quad 3 \quad 3 \quad 4 \quad 3 \quad 3 \quad 4 \quad 6}$. Пример для $n \geq 6$ см. в задаче 28.

Из задачи 26 следует, что $t_2 \geq 3$.

(i) Докажем, что для 5 прямых $t_2 \geq 4$. Из задачи 19 следует, что $10 = t_2 + 3t_3 + 6t_4$. Следовательно, t_2 не может делиться на 3.

(ii) Докажем, что для 8 прямых $t_2 \geq 4$. Если $t_5 + t_6 + t_7 = 1$, то $t_2 \geq 4$. В противном случае из задачи 19 следует, что $28 = t_2 + 3t_3 + 6t_4$. Поэтому t_2 не может делиться на 3.

(iii) Докажем, что для 9 прямых $t_2 \geq 6$. Если $t_6 + t_7 + t_8 = 1$, то из задачи 26 следует, что $t_2 \geq 6$. Если $t_5 = 1$, то пять прямых, проходящих через одну точку, пересекают остальные 4 прямые не менее чем в $5 \cdot 4 - 2C_4^2 = 8$ точках кратности 2, т.е. $t_2 \geq 8$. Если $t_5 + t_6 + t_7 + t_8 = 0$, то $36 = t_2 + 3t_3 + 6t_4$ и $t_2 \geq 3 + t_4$. Отсюда при условии $t_2 < 6$ из задачи 26 получаем, что $t_2 = 3$, $t_3 = 11$, $t_4 = 0$, и все области треугольные, $p_3 = 26 = f$. Осталось доказать невозможность такой конфигурации.

Задача 28. (а) Возьмём все стороны правильного $\frac{n}{2}$ -угольника и $\frac{n}{2}$ его осей симметрии. Для этих n прямых $t_2 = \frac{n}{2}$.

(б) Если $n = 4k + 1$, то добавим к примеру для $4k$ прямых бесконечно удалённую прямую. Если $n = 4k + 3$, то возьмём предыдущий пример для $4k + 4$ прямых и удалим прямую, не проходящую через вершины $2k + 2$ -угольника. В обоих случаях получим n прямых и $t_2 = 3k$.

Задача 29★. Доказательство см. в статье «On the number of ordinary lines determined by n points», опубликованной L. M. Kelly и W. O. J. Moser в журнале «Canadian Journal of Mathematics» в 1958 г. на стр. 210-219.

Задача 30★. Наилучший известный результат: $t_2 \geq \frac{6}{13}n$ для $n \geq 8$. Доказательство см. в статье «There exist $\frac{6n}{13}$ ordinary points», опубликованной J. Csima и E. T. Sawyer в журнале «Discrete and Computational Geometry» в 1993 г. в выпуске 9 на стр. 187-202.

Задача 31*. Если существуют такие две точки, что любая данная прямая проходит через хотя бы одну из них, то требуемое неравенство проверяется непосредственно следующим образом. Пусть через одну из этих точек проходит a прямых, через другую — b прямых. Тогда, если $a + b = n$, то

$$a \geq 3, b \geq 3, \quad t_2 = ab, \quad \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i \leq 2a + 2b - 15.$$

Если $a + b = n + 1$, то

$$a \geq 4, b \geq 4, \quad t_2 = (a - 1)(b - 1), \quad \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i = 2a + 2b - 15.$$

Теперь считаем, что не существует таких двух точек, что любая прямая набора проходит через по крайней мере одну из них. Воспользуемся всеми тремя пунктами задачи 32:

$$3p_4 + \sum_{j \geq 5} jp_j \geq z + x = z + \left(y + 2t_2 - \sum_{i \geq 3} it_i\right) \geq \frac{3}{2} \sum_{i \geq 3} t_i + 2t_2 - \sum_{i \geq 3} it_i = 2t_2 - \sum_{i \geq 3} \left(i - \frac{3}{2}\right) t_i.$$

Вследствие задачи 26 имеем:

$$\sum_{i \geq 2} (9 - 3i)t_i = 9 + 3p_4 + \sum_{j \geq 5} (3j - 9)p_j.$$

Заметим, что $3j - 9 \geq j$ для $j \geq 5$ и что $p_j \geq 0$. Следовательно, получаем

$$\sum_{i \geq 2} (9 - 3i)t_i = 9 + 3p_4 + \sum_{j \geq 5} (3j - 9)p_j \geq 3p_4 + \sum_{j \geq 5} jp_j \geq 2t_2 - \sum_{i \geq 3} \left(i - \frac{3}{2}\right) t_i,$$

откуда вытекает требуемое неравенство на числа t_i .

Задача 32. Рассмотрим соответствующий граф, вершины которого — точки пересечения (покращенные в один из двух цветов), рёбра — отрезки прямых, не содержащие внутри себя других точек пересечения.

(а) Каждая красная вершина является красным концом четырех рёбер. При этом у красных рёбер по два красных конца, у бесцветных рёбер по одному, а у синих рёбер красных концов нет. Число красных вершин равно t_2 . Поэтому

$$4t_2 = 2x + \sum_{i \geq 2} it_i - x - y,$$

откуда получаем требуемое.

(б) Рассмотрим произвольную синюю вершину O и удалим все проходящие через неё прямые набора. Оставшиеся прямые не будут проходить через одну точку и поэтому разделят проективную плоскость на области, каждая из которых ограничена не менее чем тремя рёбрами. Точка O принадлежит одной из таких областей. Перебором можно убедиться в том, что для вершины O всегда выполняется одно из следующих трёх условий.

(1) Из точки O выходит не менее трёх синих рёбер (в исходном графе).

(2) Из точки O выходит не менее двух синих рёбер и точка O является вершиной границы хотя бы одной зелёной области.

(3) Точка O является вершиной границы не менее чем двух зелёных областей.

Тем самым для каждой синей вершины сумма числа исходящих из неё синих рёбер с удвоенным числом граничащих с ней зелёных областей не меньше трёх. Сложим эти суммы по всем синим вершинам и получим $2y + 2s \geq \sum_{i \geq 3} t_i$.

(с) Для зелёной области u обозначим через $x(u)$ и $s(u)$ число красных рёбер и число синих вершин на границе u , соответственно. Для зелёной области u положим

$$d(u) = \begin{cases} 0, & \text{если } s(u) \geq 1; \\ 1, & \text{если } s(u) = 0. \end{cases}$$

Нетрудно доказать, что если зелёная область u ограничена j рёбрами, то

$$s(u) \leq (j - 1) - x(u) + d(u).$$

Обозначим через X и через D суммы $x(u)$ и $d(u)$ по всем зелёным областям соответственно. Тогда, складывая предыдущее неравенство по всем зелёным областям, получим

$$s \leq \sum_{j \geq 4} (j - 1)p_j - X + D.$$

Заметим, что к любому красному ребру примыкает не менее одной зелёной области (это следует из $t_n = t_{n-1} = 0$). Назовём красное ребро тёмно-красным, если к нему примыкают две зелёные области. Обозначим через x_1 число тёмно-красных рёбер. Тогда $X = x + x_1$. Выделим четырехугольные области, все вершины которых красные (все выделенные области зелёные). Нетрудно доказать, что каждая выделенная область ограничена не менее чем двумя тёмно-красными рёбрами. Следовательно, число выделенных областей не превосходит x_1 . Отсюда следует, что $D \leq x_1 + \sum_{j \geq 5} p_j$. Осталось соединить все полученные неравенства.

Planar arrangements of lines

K. Kuyumzhiyan, E. Molchanov, I. Shnurnikov

By an arrangement of lines we mean a finite family of n distinct lines in the plane. Suppose that these n lines cut the plane into f regions. The aim of the series of problems below is to determine all possible values of f for a fixed n . In 1993, N. Martinov indicated all possible numbers f and in 2007 V.I. Arnold suggested a new sketch of proof that we are going to follow.

Before intermediate finish

We always denote by n ($n \geq 1$) and by f the number of lines in an arrangement and the number of regions in the plane partition, respectively. Let us note that regions in the plane partition are polygonal or unbounded.

Problem 1. For every n , find the minimal and the maximal possible values of f .

Problem 2. For every n , find all possible numbers f , if

- (a) $1 \leq n \leq 5$,
- (b) $n = 6, 7$.

Let us denote by p the maximal number of parallel lines in an arrangement, and by q the maximal number of concurrent (i.e. passing through one point) lines in an arrangement. Let us denote by r_i ($2 \leq i \leq q$) the number of points which are incident to exactly i lines of an arrangement.

Problem 3. Prove the following.

- (a) $f \geq (p+1)(n-p+1)$,
- (b) $f \geq q(n-q+2)$,
- (c) There exist arrangements such that the bounds (a) and (b) are reached.
- (d) $f = n+1 + \sum_{i=2}^q (i-1)r_i$.

Problem 4. Prove that the number of regions f cannot belong to intervals

- (a) $(n+1; 2n)$ for $n \geq 3$,
- (b) $(2n; 3n-3)$ for $n \geq 5$,
- (c) $(3n-2; 4n-8)$ for $n \geq 8$.

Problem 5. Find maximal possible values of f if the values

- (a) n and p ,
 - (b) n and q
- are given.

For p and n , where $1 \leq p \leq n$, denote by $a(n, p)$ and $b(n, p)$ the following numbers:

$$b(n, p) = (p+1)(n-p+1) + C_{n-p}^2, \quad a(n, p) = b(n, p) - \min \{p, C_{n-p}^2\}.$$

Problem 6. For any integer p , $1 \leq p \leq n$, and any integer f , $a(n, p) \leq f \leq b(n, p)$, construct a configuration of n lines splitting the plane into f regions and having at most p parallel lines.

Main Theorem. For a given n , the set of all possible values of f is formed by the union of integers in the intervals $[a(n, p); b(n, p)]$ for all p , where $1 \leq p \leq n$.

In other words, all the possibilities for f appear in Problem 6. However, it is not clear why the number of regions cannot be an integer from none of the intervals $[a(n, p); b(n, p)]$. In fact, one of the difficulties is that for fixed n and p , there exist arrangements splitting the plane into less than $a(n, p)$ regions.

Problem 7. Find all the pairs (n, p) such that there exists a configuration of lines splitting the plane into less than $a(n, p)$ regions.

For a given n , by a *gap* we mean the interval $(b(n, p + 1); a(n, p))$ if it contains at least one integer. The number of gaps for a given n is denoted by $L(n)$. We enumerate the gaps from left to right with integers from 1 to $L(n)$.

Problem 8. (a) Give an explicit formula for $L(n)$ (expressing it in n) for $n \geq 3$.
(b) How many integers does a gap number j contain, where $1 \leq j \leq L(n)$?

Problem 9. Suppose that there exists a configuration of n lines splitting the plane into f regions, where f belongs to the gap number j . Prove that $p \leq j - 1$ and $q \leq j$.

Problem 10. Prove that

$$\sum_{i=2}^q i(i-1)r_i \geq n(n-p).$$

Problem 11. (a) Prove that $f \geq n + 1 + \frac{n(n-p)}{q}$.

(b) Prove that f cannot belong to the gap number j if $1 \leq j \leq \sqrt{n}$.

Problem 12. Prove that if $p < n$, then

$$r_2 + n \geq 3 + r_4 + 2r_5 + 3r_6 + \cdots + (q-3)r_q.$$

Problem 13. (a) Prove that

$$f \geq 2 \frac{n(n-p)}{q+3}.$$

(b) Prove that f cannot belong to the gap number j if $1 \leq j \leq L(n) - 2$.

Problem 14. In a convex n -gon ($n \geq 4$) all the diagonals are drawn, and suppose that no three of them are concurrent.

(a) How many intersection points of diagonals are there? (Vertices are not considered as intersection points.)

(b) Into how many parts do the diagonals split the interior of the n -gon?

Problem 15*. Consider an arrangement of n lines in the plane. Prove that the number f of regions cannot belong to the two last gaps (enumerated as $L(n) - 1$ and $L(n)$).

Problem 16*. Consider n points on the plane, not all of them being collinear. Take all the lines containing exactly two of these points. Let m be the number of such lines. Prove that $C_{m+2}^2 \geq n$.

Planar arrangements of lines

K. Kuyumzhiyan, E. Molchanov, I. Shnurnikov

After intermediate finish

Consider two planes α_1 and α_2 in the 3-dimensional space and a point O , $O \notin \alpha_1 \cup \alpha_2$. By a *central projection* we mean a transformation which maps a point X of the plane α_1 to the point of intersection of the line OX with the plane α_2 .

Problem 17. Consider an arrangement of lines in α_1 . Find the images of lines and of regions of the plane α_1 after the central projection with center O to the plane α_2 . You can suppose that the arrangement has two intersecting lines.

We suppose that all the lines which are parallel to a given line l , contain the *infinite point* corresponding to the direction l . The result of the central projection of the infinite point corresponding to the direction l is the intersection point of the plane α_2 with the line passing through O parallel to l (if l is parallel to α_2 , then the image is the infinite point of α_2 corresponding to the direction l).

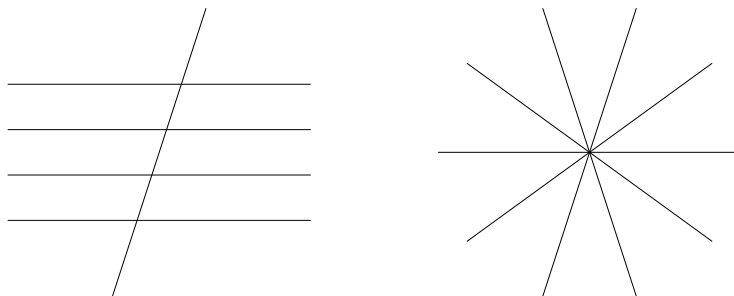
Problem 18. Prove that central projection is a one-to-one correspondence between planes considered with their infinite points. Find the image and the preimage of infinite points of the planes α_1 and α_2 respectively.

Let us call by the *projective plane* the usual plane with its infinite points, and by an *arrangement of lines* in a projective plane an arrangement of lines with their corresponding infinite points. Here one of the lines can be infinite. For an arrangement of n lines in the projective plane, we denote by t_i the number of intersection points incident to exactly i lines, where $2 \leq i \leq n$.

Problem 19. Prove that for n lines in the projective plane

$$\sum_{i \geq 2} i(i-1)t_i = n(n-1).$$

The notion of the projective plane helps to explain the following similarity between parallel and concurrent lines. Let us consider two arrangements of $k+1$ lines in the usual plane: in the first one k parallel lines intersect the $(k+1)$ th line, in the second there are $k+1$ concurrent lines, see the picture.



Each of these arrangements cuts the plane into $2k+2$ regions, and this fact has the following explanation. We can add the infinite lines to the both arrangements. We will obtain two

arrangements of $k + 2$ lines in the projective planes, and there exists a central projection mapping one arrangement to another. Hence, they cut the plane into the same number of regions. That's why it seems more convenient to solve the problem 15 in the projective plane instead of the usual one.

Problem 20. For an arrangement of n lines in the projective plane, define the notion of *region* so that any central projection gives a one-to-one correspondence between the regions of different projective planes. How can one verify whether two given points belong to one region (for a fixed arrangement)?

Below, we denote the number of regions of the projective plane by f , and the maximal number of concurrent lines in the arrangement by m .

Problem 21. Prove the following analogues of problems 3, 12, and 13.

(a)

$$f = 1 + t_2 + 2t_3 + \dots + (n - 1)t_n,$$

(b)

$$m(n - m + 1) \leq f \leq m(n - m + 1) + C_{n-m}^2.$$

(c) If $m < n$, then

$$t_2 \geq 3 + t_4 + 2t_5 + 3t_6 + \dots + (m - 3)t_m.$$

(d) If $m < n$, then for every integer M , $M \geq m$, it is true that

$$f \geq 2 \left(\frac{n^2 - n + 2M}{M + 3} \right).$$

Problem 22*. Let $n \geq 2m + 2$, and let $t_m \geq 2$. Prove that $f \geq (m + 1)(n - m)$. Is it true for $n = 2m + 1$?

Problem 23*. Formulate and prove the main theorem for the arrangements of n lines in the projective plane. Complete the proof of the main theorem for the usual plane.

Problem 24. (a) Into how many regions can the plane be divided by n circles passing through a fixed point?

(b) For the usual sphere, let the big circles (intersections of the sphere with planes passing through the center of the sphere) play the role of lines. Into how many regions can n big circles cut the sphere?

The next aim is to prove the Sylvester theorem and its generalizations.

Problem 25. (The Sylvester theorem) (a) Given n non collinear points in a plane, prove that there exists a line containing exactly two of these points.

(b) Consider an arrangement of n lines such that not all the lines are parallel and not all are concurrent. Prove that there exists an intersection point incident to exactly two lines.

It turns out that under the assumptions of problem 25(b), there exist several points incident to exactly two lines. To estimate their number, it is more convenient to consider the arrangements of lines in the projective plane. For a given arrangement of lines in the projective plane, let us denote by p_j the number of regions bounded by j segments of lines.

Note that a region bounded by j segments of lines is a polygon with j sides whenever it has an empty intersection with the infinite line.

Problem 26. Prove that if $t_n = 0$, then

$$\sum_{i \geq 2} (3 - i)t_i + \sum_{j \geq 3} (3 - j)p_j = 3.$$

Problem 27. Consider an arrangement of n lines in the projective plane such that $t_n = 0$. For every $n \leq 9$, determine the minimal possible value of t_2 in such arrangement.

Problem 28. (a) For every even $n \geq 6$, construct an arrangement of n lines with $t_2 = \frac{n}{2}$.

(b) For every odd $n \geq 7$, construct an arrangement of n lines with $t_2 = 3 \left\lfloor \frac{n}{4} \right\rfloor$.

Problem 29*. Prove that if $t_n = 0$, then $t_2 \geq \frac{3}{7}n$.

Problem 30*. (Dirak conjecture, 1951). If $t_n = 0$, then $t_2 \geq \left\lfloor \frac{n}{2} \right\rfloor$.

The next aim is to prove inequalities involving the numbers t_i for different i .

Problem 31*. If $t_n = t_{n-1} = t_{n-2} = 0$, then

$$t_2 + \frac{3}{2}t_3 \geq 8 + \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i.$$

Problem 32. Consider n points in the projective plane. Let us mark with red color the intersection points which are incident to exactly two lines, and with blue color the intersection points which are incident to at least three lines. If the endpoints of a line segment are of one color, we mark this segment with the same color (if its interior does not contain other colored points). We denote by x and y the numbers of red and blue segments, respectively. Let us mark with green color the regions bounded by at least four segments of the given lines and containing at least one red point on its boundary. We denote by z the number of pairs (a green region, a blue point on its boundary). Prove that

(a)

$$x - y = 2t_2 - \sum_{i \geq 3} it_i.$$

(b) If the arrangement is not the union of two groups of concurrent lines, then

$$y + z \geq \frac{3}{2} \sum_{i \geq 3} t_i.$$

(c) If $t_n = t_{n-1} = t_{n-2} = 0$, then

$$x + z \leq 3p_4 + \sum_{j \geq 5} jp_j.$$

Problem 33*. Find new inequalities involving numbers t_i and p_j (which do not follow trivially from problems 26 and 31, but, possibly, use problem 32).

Planar arrangements of lines

Solutions of problems before intermediate finish

Problem 1. The answer is: $n + 1 \leq f \leq \frac{n(n+1)}{2} + 1$. The both inequalities can be proved by induction on n . The base of induction $n = 1$, $f = 2$ is evident. Let us add one line. If it has x intersection points with the old lines, then the number of regions increases by $x + 1$ after adding this line. Hence, the n th line increases the number of regions by at least 1 and at most n .

Problem 2. The answer is:

$n=1$, $f = 2$,

$n=2$, $f \in \{3, 4\}$,

$n=3$, $f \in \{4, 6, 7\}$,

$n=4$, $f \in \{5, 8, \dots, 11\}$,

$n=5$, $f \in \{6, 10, 12, \dots, 16\}$,

$n=6$, $f \in \{7, 12, 15, \dots, 22\}$,

$n=7$, $f \in \{8, 14, 18, \dots, 29\}$.

The impossibility of the other values can be deduced from problems 1 and 3(a)(b).

Problem 3. (a) Let us consider p parallel lines of the arrangement and then add the other lines one by one. Each added line has at least p intersection points with the preceding lines, hence, the number of regions increases by at least $p + 1$. In total, if we add $n - p$ lines, we obtain $f \geq (p + 1)(n - p + 1)$.

(b) Let us consider q concurrent lines and then add all the remaining lines one by one. Every new line has at least $q - 1$ intersection points with the preceding lines, hence the number of regions increases by at least q after adding this line. If we add $n - q$ lines, we obtain $f \geq q(n - q + 2)$.

(c) Let us consider p parallel lines, then fix a point on one of these lines and pass $n - p$ other lines through this point one by one. Each new line increases the number of regions by p , and finally we obtain $(p + 1)(n - p)$ regions.

Let us consider q concurrent lines. All the other $n - q$ lines will be parallel to one chosen line of these q lines. Pass them one by one. Every new line increases the number of regions by q , so we obtain $q(n - q + 2)$ regions.

(d) *Solution 1.* Let us add the lines one by one. If the line has x intersection points with the preceding lines, then the number of regions increases by $x + 1$. On the other hand, each of these x intersection points either has multiplicity 2, or one plus its previous multiplicity. Hence the sum $\sum_{i \geq 2} (i - 1)r_i$ increases by x after adding this line.

Solution 2. Let us intersect the given arrangement with the disk of a sufficiently big radius (such that the disc contains all the intersection points of lines). Consider the following graph: its vertices are the intersection points of lines with each other and with the boundary of the disc, its edges are the line and circle segments which do not contain intersection points except its ends. The number of vertices of this graph equals $v = 2n + \sum_{i \geq 2} r_i$, the number of edges

equals $e = 3n + \sum_{i \geq 2} ir_i$. The number of regions f of the plane is less by one than the number of the regions of the disc divided by the edges of the graph. Using the Euler formula for the graphs, we obtain

$$f = n + 1 + \sum_{i \geq 2} (i - 1)r_i.$$

Problem 4. (a) If all the lines are parallel, then $f = p + 1$. If not all the lines are parallel, then $1 \leq p \leq n - 1$. Using problem 3, we obtain $f \geq (p + 1)(n - p + 1)$. The expression $(p + 1)(n - p + 1)$ is the quadratic trinomial in p with the negative leading coefficient. For $p = 1$ and $p = n - 1$, the value of the trinomial $(p + 1)(n - p + 1)$ is $2n$. Hence, for $1 \leq p \leq n - 1$ the value of the trinomial $(p + 1)(n - p + 1)$ is not less than $2n$.

(b) If all or all except one lines are parallel, then $f = n + 1$ or $f = 2n$. Otherwise, using problem 3(a), we have $f \geq (p + 1)(n - p + 1)$. The expression $(p + 1)(n - p + 1)$ is a quadratic trinomial with respect to p with the negative leading coefficient. For $p = 2$ and $p = n - 2$ the value of the trinomial $(p + 1)(n - p + 1)$ equals $3n - 3$. Hence, for $2 \leq p \leq n - 2$ the value of the trinomial $(p + 1)(n - p + 1)$ is not less than $3n - 3$. Consequently, for $2 \leq p \leq n - 2$ we have $f \geq 3n - 3$. If $p = 1$, then, using problem 3(b), we have $f \geq q(n - q + 2)$. If $q = n$, then $f = 2n$. Consider the quadratic trinomial $q(n - q + 2)$. For $3 \leq q \leq n - 1$ we have $f \geq q(n - q + 2) \geq 3n - 3$. The remaining case is $p = 1, q = 2$, where the number of regions is

$$1 + \frac{n(n + 1)}{2} \geq 3n - 3 \quad \Leftrightarrow \quad n^2 - 5n + 8 \geq 0.$$

(c) If $p \geq n - 2$ or $q \geq n - 1$, then $f \leq 3n - 2$. If $3 \leq p \leq n - 3$ or $4 \leq q \leq n - 2$, then by problem 3 we have $f \geq 4n - 8$. The remaining case is $p \leq 2$ and $q \leq 3$. By problem 3 we have $f = n + 1 + r_2 + 2r_3$. Each line of the arrangement intersects at least $n - 2$ other lines. Hence, the number of pairs of intersecting lines equals $r_2 + 3r_3$, which is not less than $\frac{n(n-2)}{2}$. Consequently,

$$f \geq n + 1 + \frac{2}{3}(r_2 + 3r_3) \geq n + 1 + \frac{n^2 - 2n}{3} \geq 4n - 8$$

for $n \geq 8$.

Problem 5. (a) Consider p parallel lines in the arrangement of n lines and add the remaining lines one by one. The line number i , $1 \leq i \leq n - p$, intersects the preceding lines in at most $p + i - 1$ points, hence the number of regions increases by at most $p + i$. If we add $n - p$ lines, we obtain

$$f \leq (p + 1)(n - p + 1) + C_{n-p}^2.$$

The bound is reached for the arrangement containing p parallel lines and $n - p$ lines in general position (i.e. no two are parallel and no three are concurrent), such that they are also in general position with the p parallel lines.

(b) Consider q concurrent lines in the arrangement of n lines and add the remaining lines one by one. The line number i , $1 \leq i \leq n - q$, intersects the preceding ones in at most $q + i - 1$ points, hence the number of regions increases by at most $q + i$. If we add $n - q$ lines, we obtain

$$f \leq q(n - p + 2) + C_{n-q+1}^2 = 1 + C_{n+1}^2 - C_{q-1}^2.$$

The bound is reached for the arrangements of q concurrent lines and $n - q$ lines in general position such that they are also in general position with the q concurrent lines.

Problem 6. Let us take $n - p$ lines in general position and choose some t intersection points of these lines, where $t \leq \min\{p, C_{n-p}^2\}$. Now add p parallel lines in such a way that they pass through t chosen points but do not pass through the other intersection points of the $n - p$ lines. Also, the p added lines should not be parallel to any of the first $n - p$ lines. Then it is easy to check that this arrangement has at most p parallel lines, and that the number of regions equals

$$f = (p + 1)(n - p + 1) + C_{n-p}^2 - t.$$

Problem 7. For given n and p , the minimal number of regions of the arrangement equals $(p + 1)(n - p + 1)$. To reach it, we can take the arrangement containing $n - p + 1$ concurrent lines and $p - 1$ parallel lines such that the parallel lines are also parallel to one chosen line of the first $n - p + 1$ ones. Now note that

$$(p + 1)(n - p + 1) < a(n, p) \Leftrightarrow C_{n-p}^2 > p \Leftrightarrow n > p + \frac{1}{2} + \sqrt{2p + \frac{1}{4}}.$$

The second inequality is also equivalent to $n \geq p + \frac{1}{2} + \sqrt{2p + \frac{9}{4}}$ (if we write $C_{n-p}^2 \geq p + 1$).

Problem 8. (a)

$$L(n) = \max\{k \geq 1 \mid b(n, n - k + 1) \leq a(n, n - k) - 2\} \text{ for } n \geq 3.$$

$$\begin{aligned} b(n, n - k + 1) \leq a(n, n - k) - 2 &\Leftrightarrow \min\left\{n - k, \frac{k(k - 1)}{2}\right\} \leq n - k - 2 \Leftrightarrow \\ &\Leftrightarrow n \geq \frac{k^2 + k}{2} + 2 \Leftrightarrow k \leq \sqrt{2n - \frac{15}{4}} - \frac{1}{2}. \end{aligned}$$

It follows that $L(n) = \left\lceil \sqrt{2n - \frac{15}{4}} - \frac{1}{2} \right\rceil$.

(b) Since

$$n \geq \frac{L^2(n) + L(n)}{2} + 2, \text{ then } \min\left\{n - j, \frac{j(j - 1)}{2}\right\} = \frac{j(j - 1)}{2} \text{ for } 1 \leq j \leq L(n).$$

Hence, $a(n, n - j) = (n - j + 1)(j + 1)$, and the j th gap contains $n - \frac{j(j+1)}{2} - 1$ integers.

Problem 9. If $j \leq p \leq n - j$ or $j + 1 \leq q \leq n - j + 1$, then by problem 3 we have $f \geq (n - j + 1)(j + 1) = a(n, n - j)$. If $p \geq n - j + 1$, then, as follows from problem 5,

$$f \leq (p + 1)(n - p + 1) + C_{n-p}^2 \leq b(n, n - j + 1).$$

If $q \geq n - j + 2$, then by problem 5 we have

$$f \leq q(n - q + 2) + C_{n-q}^2 + 1 \leq b(n, n - j + 1).$$

Problem 10. The number of pairs of intersecting lines equals $\sum_{i=2}^q \frac{i(i-1)}{2} r_i$ which is not less than $\frac{n(n-p)}{2}$, since every line intersects at least $n - p$ lines.

Problem 11. (a) Using problems 3 and 10, we obtain that

$$f - (n + 1) = \sum_{i \geq 2} (i - 1) r_i \geq \sum_{i \geq 2} \frac{i(i - 1)}{q} r_i \geq \frac{n(n - p)}{q}.$$

(b) Suppose the contrary, then by problem 9 we have $p \leq j - 1$ and $q \leq j$, where j is the number of the gap. Note that $n - p \geq n - j + 1$ and $n + 1 \geq n - j + 1$. It contradicts with (a):

$$f \geq n + 1 + \frac{n(n-p)}{q} \geq (n-j+1)\left(\frac{n}{q} + 1\right) \geq (n-j+1)(j+1) = a(n, n-j).$$

Problem 12. Let us intersect the given arrangement with a disc of a sufficiently big radius, such that it contains all the intersection points. We obtain a graph: its vertices are the intersection points of the lines of the arrangement and the intersection points of the lines with the circle, its edges are the line and circle segments, which do not contain intersection points except their ends. The number of vertices v and the number of edges e equal $2n + \sum_{i \geq 2} r_i$ and $3n + \sum_{i \geq 2} i r_i$, respectively. The interior of the disc contains f regions, where

$$f = n + 1 + \sum_{i \geq 2} (i-1)r_i.$$

The sum of the numbers of bounding edges for all the regions in the disc equals

$$2e - 2n = 4n + 2 \sum_{i \geq 2} i r_i.$$

Since $p < n$, every region in the disc is bounded by at least three edges of the graph. So we have $2e - 2n \geq 3f$, which gives the required inequality.

Problem 13. (a) Let $a = \frac{2}{q+3}$ and $b = \frac{q-1}{q+3}$. Consider the following quadratic trinomial in the variable i :

$$a(i^2 - i) + b(3 - i) - (i - 1) = a(i - 2)(i - q) \leq 0 \quad \text{for } 2 \leq i \leq q.$$

Let us multiply its corresponding values by r_i and sum up for all i , $2 \leq i \leq q$:

$$0 \geq a \sum_{i=2}^q i(i-1)r_i + b \sum_{i=2}^q (3-i)r_i - \sum_{i=2}^q (i-1)r_i \geq an(n-p) + b(3-n) - (f-n-1),$$

where the last inequality is obtained from problems 10, 12, and 3. Consequently,

$$f \geq 2 \frac{n(n-p)}{q+3} + (n+1 + \frac{q-1}{q+3}(3-n)) \geq 2 \frac{n(n-p)}{q+3}.$$

(b) Suppose the contrary, then by problem 9 we have $p \leq j - 1$ and $q \leq j$. Using that $n - p \geq n - j + 1$, we get a contradiction with (a):

$$f \geq 2 \frac{n(n-p)}{q+3} \geq (n-j+1) \frac{2n}{q+3} \geq (n-j+1)(j+1) = a(n, n-j),$$

because

$$\frac{(q+3)(j+1)}{2} \leq \frac{j^2 + 4j + 3}{2} \leq \frac{1}{2}L^2(n) < n.$$

Problem 14. (a) The intersection point determines two diagonals passing through it and the ends of these diagonals, which form a four-tuple of vertices of the given n -gon.

Conversely, every four-tuple of distinct vertices of the n -gon determines one intersection point of diagonals. Hence, the number of intersection points is C_n^4 .

(b) *Solution 1.* Let us pass the diagonals one by one. If the added diagonal has x intersection points with the previous diagonals, then the number of regions of the interior of the n -gon is increased by $x + 1$. We can treat it as every diagonal and every intersection point increases the number of regions by 1. Hence, the required number of regions equals $1 + C_n^4 + \frac{n(n-3)}{2}$, because the number of intersection points was found in (a), and the number of diagonals equals $\frac{n(n-3)}{2}$.

Solution 2. Let us consider a graph: its vertices are the vertices of the n -gon and the intersection points of the diagonals, its edges are the diagonal segments and the sides of the n -gon. In this graph, the number of vertices equals $v = n + C_n^4$, and the number of edges equals $e = 2C_n^4 + \frac{n(n-1)}{2}$. By the Euler formula, the number of regions equals $1 + e - v = 1 + C_n^4 + \frac{n(n-3)}{2}$.

Problem 15. See problem 23.

Problem 16. Let us draw the lines each of which passes through exactly two of given points. These m lines divide the plane into at most $1 + m + C_m^2$ regions. Consider all the points of the given set such that for each of these point, no line passing through exactly two points of the given set, passes through this point. It turns out that every region formed by the arrangement of m lines contains at most one such point (prove it yourself). Also find yourself m regions not containing such points. In total, m lines contain at most $2m$ points of the initial set. Hence $n \leq 2m + 1 + C_m^2 = C_{m+2}^2$.

The solutions of the problems after intermediate finish

Problem 17. For the parallel planes α_1 and α_2 , the central projection is just a dilatation, which maps lines to lines and regions to regions. Now suppose that α_1 and α_2 intersect, and let l_1 and l_2 be the intersection lines of the planes α_1 and α_2 with planes passing through the point O parallel to planes α_2 and α_1 , respectively. If a line l does not coincide with l_1 , then its image is a line for $l \parallel l_1$, and is a pointed line if $l \nparallel l_1$ (the line with one point thrown out, namely the point of intersection with l_2). If a region intersects l_1 , then its image consists of two unbounded regions. If a non-bounded region is incident to two non parallel rays, then its image is incident to l_2 .

Problem 18. It is one-to-one by definition. The image and the pre-image will be the lines l_2 and l_1 together with their infinite points. Recall that l_1 and l_2 are the lines of intersection of the planes α_1 and α_2 with the planes passing through O parallel to α_2 and α_1 , respectively.

Problem 19. Every two lines have exactly one common points on the plane considered with its infinite points (if these lines are parallel or one of the lines is infinite, then this point is infinite). The number of pairs of lines is C_n^2 . If an intersection point belongs to i points, it is an intersection point for C_i^2 pairs of lines, which gives the required.

Problem 20. First we suppose that not all the lines of the arrangement of n lines are concurrent, and define the “region” in the projective plane in this case. If one of the lines is infinite, then the regions coincide with the regions of the usual plane divided by $n - 1$ remaining lines. If the arrangement does not contain the infinite line, then the following objects will be the regions:

- a bounded region of the plane,

- a non-bounded region of the plane incident to two parallel rays,
- a pair of non-bounded regions of the plane, the first one incident to two non-parallel rays l_1 and l_2 , the second one to non-parallel rays l_3 and l_4 , such that $l_1 \parallel l_3$ and $l_2 \parallel l_4$. The infinite points corresponding to the directions which are between l_1 and l_2 also belong to this region, they “glue up” two its infinite parts.

If all the lines of the arrangement are concurrent, “regions” are defined in a similar way. Two points belong to the same region if and only if they are connected by a polygonal line not intersecting the lines of the arrangement. Here the ends of the polygonal line are the two given points, and the other vertices can be infinite. Its segments incident to an infinite vertex are rays which are parallel to the direction of this infinite point. After this re-definition, the polygonal line is mapped to a polygonal line via a central projection. Consequently, two points belong to one region if and only if their images via the central projection belong to one region. So the correspondence between regions is one-to-one.

Problem 21. (a) *Solution 1.* Let us map one line of the arrangement to the infinite line via a central projection. The number of regions and the values t_i do not change, but now the number of regions of the projective plane coincides with the number of regions f of the usual plane, divided by the arrangement of $n - 1$ remaining lines. By problem 3, we have $f = n + \sum_{i \geq 2} (i - 1)r_i$. Now note that

$$n - 1 = \sum_{i \geq 2} (i - 1)(t_i - r_i),$$

since the infinite line contains $t_i - r_i$ intersection points, which belong to $i - 1$ lines of the arrangement, and plus the infinite point.

Solution 2. Induction on n . The base $n = 1$ is evident. The step follows from the fact that each added line increases the number of regions by the number of the points of intersection with the previous lines.

(b) Induction on n . The base $n = m$, $f = m$ is evident. The added line number j , $1 \leq j \leq n - m$, has at least m and at most $m + j - 1$ points of intersection with the previous lines, since every two lines intersect in the projective plane. The required inequality follows from the fact that each added line increases the number of regions by the number of points of intersection with the previous lines.

(c) Consider the graph in the projective plane: its vertices are the intersection points of lines, the edges are the line segments. We allow edges to pass through infinite points, such an edge consists of two rays belonging to the same line together with the infinite point of this direction which glues up the two rays. The number of vertices v and the number of edges e of this graph equal $\sum_{i \geq 2} r_i$ and $\sum_{i \geq 2} ir_i$, respectively. Since $m < n$, each region is bounded by at least three edges of the graph, hence

$$3f \leq 2e \Leftrightarrow 3 + 3 \sum_{i \geq 2} (i - 1)t_i \leq 2 \sum_{i \geq 2} ir_i \Leftrightarrow \sum_{i \geq 2} (3 - i)t_i \geq 3.$$

(d) Let $a = \frac{2}{M+3}$ and $b = \frac{M-1}{M+3}$. Consider the following quadratic trinomial in variable i :

$$a(i^2 - i) + b(3 - i) - (i - 1) = a(i - 2)(i - M) \leq 0 \quad \text{if } 2 \leq i \leq m.$$

Multiply the corresponding values of this trinomial by t_i and sum up for all i , $2 \leq i \leq m$:

$$0 \geq a \sum_{i=2}^m i(i - 1)t_i + b \sum_{i=2}^m (3 - i)t_i - \sum_{i=2}^m (i - 1)t_i \geq an(n - 1) + 3b - (f - 1),$$

where the last inequality follows from problems 19, 21(a) and (c). Consequently,

$$f \geq 2 \frac{n(n-1)}{M+3} + \left(1 + \frac{3(M-1)}{M+3}\right) = 2 \frac{n(n-1) + 2M}{M+3}.$$

Problem 22*. Let us choose two points P and Q incident to m lines each, and denote by N the set of lines of the initial arrangement passing through at least one of P and Q . Two cases are possible:

- (i) the line PQ does not belong to the initial arrangement. Then N contains $2m$ lines and divides the projective plane into $m^2 + 2m - 1$ regions (if we do not consider other lines).
- (ii) the line PQ belongs to the initial arrangement. Then N contains $2m - 1$ lines and divides the projective plane into m^2 regions (if we do not consider other lines).

In both cases every remaining line of the arrangement (i.e. a line not from N) intersects the lines from N in at least m points, and there are at most two lines which intersect the lines from N in exactly m points. In the case (i) the inequality is held because

$$f \geq m^2 + 2m - 1 + (m+1)(n-2m) - 2 \geq (m+1)(n-m).$$

Now consider the case (ii). If the arrangement contains at most one line which intersects the lines from N in m points, then the number of regions can be bounded using the number of intersection points of the other lines as follows:

$$f \geq m^2 + (m+1)(n-2m+1) - 1 = (m+1)(n-m).$$

If the arrangement contains two lines intersecting N in m points each, and their intersection point does not belong to the lines from N , then we similarly obtain $f \geq (m+1)(n-m)$.

The remaining case is when the arrangement contains two lines intersecting N in m points each, and their intersection point belongs to a line of N . Denote these lines by l_{2m} and l_{2m+1} , and their intersection point by R . Let us prove in this case that every other line of the arrangement intersects $N \cup l_{2m} \cup l_{2m+1}$ in at least $m+2$ points. It will follow from this fact that

$$f \geq m^2 + 2m + (m+2)(n-2m-1) \geq (m+1)(n-m)$$

which will end the proof in the case (ii).

Let us denote the lines passing through the point P in the sequence order, counting from the line PQ , by $l_1, \dots, l_{m-1}$. Similarly denote the lines passing through Q in the sequence order, counting from PQ , by $l_m, \dots, l_{2m-2}$. Denote by $A_{i,j}$ the point of intersection of lines l_i and l_{m-1+j} , where $1 \leq i, j \leq m-1$. Without loss of generality, we may assume that the line PQ is infinite, that the line l_{2m} passes through the points $A_{i,i}$ for $1 \leq i \leq m-1$, and that the line l_{2m+1} passes through the points $A_{i,m-i}$ for $1 \leq i \leq m-1$. Then the lines l_{2m} and l_{2m+1} intersect in the point $A_{\frac{m}{2}, \frac{m}{2}}$, and m is even. Consider an arbitrary remaining line l of the arrangement. It intersects N in at least $m+1$ points. If at least one point of intersection of l with l_{2m} or with l_{2m+1} does not belong to the lines from N , then l intersects $N \cup l_{2m} \cup l_{2m+1}$ in at least $m+2$ points.

Let us note that if the line l passes through the point $A_{\frac{m}{2}, \frac{m}{2}}$, then the intersection points of l with the lines $l_{\frac{m}{2}-1}$ and $l_{\frac{m}{2}+1}$ or with the lines $l_{m-1+\frac{m}{2}-1}$ and $l_{m-1+\frac{m}{2}+1}$ differ from the points A_{ij} . Hence, the line l intersects N in at least $m+2$ points.

Without loss of generality, we may assume that the intersection point of lines l and PQ and the intersection point of the lines l_{2m} and PQ belong to one line segment PQ of the

line PQ (in the projective line, two points divide the line into two segments). Then the line l intersects l_{2m+1} in a point $A_{a,b}$ with $|a - b| \geq 2$. Hence, the line l passes through at most $\min\{a, b\} + \min\{m - 1 - a, m - 1 - b\} \leq m - 3$ points of form $A_{i,j}$. Consequently, the line l intersects N in at least $m + 2$ points.

The statement is not true for $n = 2m + 1$. The counterexample for every even $m \geq 4$ can be constructed as follows: m lines pass through each of P and Q , the line PQ is common. Two more lines intersect these $2m - 1$ lines in m points each. It gives $f = m^2 + 2m < (m + 1)^2$.

Problem 23*. If we add the infinite line to the arrangement, the number of regions does not change, the number of lines n increases by 1, and we obtain $p + 1$ concurrent lines instead of p parallel lines. It gives us the following statement:

The number f can be the number of regions of the projective plane divided by n lines if and only if f belongs to at least one of the intervals $[a(n, m), b(n, m)]$, $n \geq m \geq 2$, where

$$b(n, m) = m(n - m + 1) + C_{n-m}^2, \quad a(n, m) = b(n, m) - \min\{m - 1, C_{n-m}^2\}.$$

As before, a *gap* is an interval $(b(n, m), a(n, m - 1))$ which contains at least one integer. It follows from problem 8 that $L(n) = \left\lceil \sqrt{2n - 5\frac{3}{4}} - \frac{1}{2} \right\rceil$. In the sequel we denote $L(n)$ just by L , omitting n . Taking into consideration problem 13, it remains to prove that the number of regions cannot belong to the two last gaps numbered $L - 1$ and L .

Suppose that there exists an arrangement such that the value f belongs to the $(L - 1)$ th gap, namely to the interval

$$((n - L + 2)(L - 1) + C_{L-2}^2, L(n - L + 1)).$$

It follows from problem 9 that $m = \max\{p + 1, q\} \leq L - 1$. Apply problem 21 for $M = L - 1$:

$$f \geq \frac{2(n^2 - n)}{L + 2} \geq L(n - L + 1).$$

In the last inequality, we used that $n \geq \frac{L^2 + L}{2} + 3$ as follows:

$$n^2 - n \geq (n + \frac{L}{2} - 3)(n - L + 1) \geq \left(\frac{L^2 + 2L}{2} \right) (n - L + 1).$$

It contradicts with the fact that f belongs to the $(L - 1)$ th gap.

Now let us assume that there exists an arrangement of lines in the projective plane such that the number of regions belongs to the L th gap:

$$f \in (L(n - L + 1) + C_{L-1}^2, (L + 1)(n - L)).$$

By problem 4 we may assume that $L \geq 4$. Using problem 9, we have $m \leq L$. Consider 3 cases.

(1) If $m < L$, then by problem 21(d) for $M = L - 1$ we obtain

$$f > \frac{2(n^2 - n)}{L + 2} \geq (L + 1)(n - L),$$

because it follows from $n \geq \frac{n^2 + n}{2} + 3$ that

$$\frac{(L + 2)(L + 1)}{2}(n - L) \leq (n + L - 2)(n - L) \leq n^2 - 2n.$$

(2) If $m = L$ and $t_m = 1$, then throw out one line passing through a point which belonged to m lines. This operation decreases the number of regions. We can apply the inequality from problem 21(d) for $M = L - 1$ to the remaining arrangement of $n - 1$ lines and obtain

$$f \geq 2 \left(\frac{n^2 - 3n + 2L}{L + 2} \right) \geq (L + 1)(n - L).$$

Let us prove the last inequality. If $n \geq \frac{L^2 + L}{2} + 4$, then

$$n^2 - 3n + 2L \geq (n - L)(n + L - 3) \geq (n - L) \left(\frac{L^2 + 3L + 2}{2} \right).$$

The case $n = \frac{L^2 + L}{2} + 3$ can be checked directly.

(3) If $m = L$ and $t_m \geq 2$, then $n \geq 2m + 2$, and it follows from the preceding case that $f \geq (L + 1)(n - L)$.

Problem 24. (a) Answer: it is the set of values from the main theorem for an arrangement of n lines in the plane. Let us consider a circle centered in the common intersection point and make an inversion with respect to this circle. We obtain an arrangement of lines, and the number of regions did not change. Conversely, if an arrangement of lines is given, then we can make an inversion with respect to some circle such that its circle does not belong to any line. We will get an arrangement of circles with the same number of regions.

(b) Answer: it is the set of doubled values from the main theorem for the projective plane. Consider the projection of the sphere with center O to the plane α tangent to the sphere in its south pole. Then a point X of the sphere is mapped to the point of intersection of the line OX with the plane α . If OX is parallel to α then X is mapped to the infinite point of direction OX . Under this projection, the big circles of the sphere are mapped to the lines of the projective plane, and the pair of opposite (symmetric wrt the center) regions of the sphere are mapped to the same region of the projective plane. Hence, the number of regions of the sphere equals the doubled number of regions of the projective plane divided by the corresponding arrangement of lines. Conversely, for every given arrangement of lines on the projective plane, we can construct an arrangement of big circles on the sphere via the inverse projection from the projective plane to the sphere, and this operation will double the number of regions.

Problem 25. (a) Consider the pair “line AB , point C not on this line”, such that the points A, B, C belong to the given set and the distance from the point C to the line AB is minimal among all such pairs. Suppose that the line AB contains a point D from the given set. Without loss of generality, we may suppose that D is between A and B and that the angle $ADC \geq 90^\circ$. Then the distance between D and AC is less than the distance between C and AB , which contradicts the choice of points A, B , and C . Hence, the line AB does not contain the initial points except A and B .

(b) *Solution 1.* Suppose the contrary, i.e. each intersection point belongs to at least three given lines. It can be easily seen that we are not in the case when there are only two directions of lines. Now we can assume that the arrangement contains three pairwise non-parallel lines which are not concurrent. For all such triples of lines, consider the triangle formed by these three lines, and choose among them the triangle ABC of the minimal nonzero area. Since at least three points pass through each of A, B , and C , and using the fact that the area of ABC is minimal, we obtain that the lines passing through A, B , and C parallel to BC, CA , and AB , respectively, belong to the arrangement. Let us denote by A_1, B_1 , and C_1

the intersection points of these three lines. The vertices of ABC are the midpoints of sides of $A_1B_1C_1$. Hence, the areas of triangles A_1BC , B_1CA , and C_1AB also equal the area of ABC . If we similarly continue with the triangles A_1BC , B_1CA , and C_1AB , we obtain the infinite number of initial lines, contradiction.

Solution 2. Let us reduce the problem to the case (a) via the polar duality. Consider a circle whose center does not belong to the lines of the arrangement. Make a polar transformation with respect to this circle. For every point, it puts into correspondence a line, and for every line, it puts into correspondence a point. The arrangement of n lines is mapped to the arrangement of n non-collinear points. Using (a), there exists a line l containing exactly two poles A and B . If we make this polar transformation once more (i.e. the inverse), we obtain that there exist exactly two lines of the arrangement passing through the pole L of the line l , namely the polar duals a and b of points A and B . Here we used the fact that the polar dual of the intersection point of two lines is the line which passes through the poles of these lines.

Problem 26. Consider a graph on the projective plane: its vertices are the intersection points of lines, the edges are the line segments which do not contain other intersection points in their interior. Let us denote by v and e the numbers of vertices and edges of this graph, respectively. We denote by f , as usually, the number of regions of the projective plane. Without loss of generality let us assume that one of lines is infinite (if not, find a central projection mapping one of the lines to the infinite line, this operation does not change the values v , e , f , t_i , and p_j). Note that if a connected graph on the projective plane contains all the infinite points, then the Euler formula can be written as follows: $v - e + f = 1$. Since $t_n = 0$, all the regions of the projective plane formed by the graph are bounded by at least three edges. Hence, $p_2 = 0$. Note that then

$$v = \sum_{i \geq 2} t_i, \quad e = \sum_{i \geq 2} i t_i = \frac{1}{2} \sum_{j \geq 3} j p_j, \quad f = \sum_{j \geq 3} p_j.$$

Consequently,

$$3 = 3f - (2e + e) + 3v = 3 \sum_{j \geq 3} p_j - \left(\sum_{j \geq 3} j p_j + \sum_{i \geq 2} i t_i \right) + 3 \sum_{i \geq 2} t_i = \sum_{j \geq 3} (3 - j) p_j + \sum_{i \geq 2} (3 - i) t_i.$$

Problem 27. Answer: $\frac{n : \quad 3 \quad 4 \quad 5 \quad 6 \quad 7 \quad 8 \quad 9}{t_2 : \quad 3 \quad 3 \quad 4 \quad 3 \quad 3 \quad 4 \quad 6}$. The example for $n \geq 6$ is constructed in problem 28.

It follows from the problem 26 that $t_2 \geq 3$.

(i) Show that for 5 lines we have $t_2 \geq 4$. It follows from problem 19 that $10 = t_2 + 3t_3 + 6t_4$. Hence, t_2 is not divisible by 3.

(ii) Show that for 8 lines we have $t_2 \geq 4$. If $t_5 + t_6 + t_7 = 1$, then $t_2 \geq 4$. Otherwise it follows from problem 19 that $28 = t_2 + 3t_3 + 6t_4$. Hence, t_2 is not divisible by 3.

(iii) Show that for 9 lines we have $t_2 \geq 6$. If $t_6 + t_7 + t_8 = 1$, then it follows from problem 26 that $t_2 \geq 6$. If $t_5 = 1$, then five concurrent lines intersect four other lines in at least $5 \cdot 4 - 2C_4^2 = 8$ points of multiplicity 2, i.e. $t_2 \geq 8$. If $t_5 + t_6 + t_7 + t_8 = 0$, then

$$36 = t_2 + 3t_3 + 6t_4 \quad \text{and} \quad t_2 \geq 3 + t_4.$$

Now using $t_2 < 6$ from problem 26 we obtain that $t_2 = 3$, $t_3 = 11$, $t_4 = 0$, and all the regions are triangular, $p_3 = 26 = f$. It remains to show that such a configuration does not exist.

Problem 28. (a) Take all the sides of a regular $\frac{n}{2}$ gon and its $\frac{n}{2}$ symmetry axes. For these n lines $t_2 = \frac{n}{2}$.

(b) If $n = 4k + 1$, then add the infinite line to the example for $4k$ lines. If $n = 4k + 3$, then take the preceding example for $4k + 4$ lines and remove one line which does not pass through the vertices of the $2k + 2$ -gon. In both cases we obtain n lines and $t_2 = 3k$.

Problem 29★. The proof can be found in the paper “On the number of ordinary lines determined by n points”, after L. M. Kelly and W. O. J. Moser in the “Canadian Journal of Mathematics”, 1958, pp. 210-219.

Problem 30★. The best known result is: $t_2 \geq \frac{6}{13}n$ for $n \geq 8$. The proof can be found in the paper “There exist $\frac{6n}{13}$ ordinary points”, after J. Csima and E. T. Sawyer in the journal “Discrete and Computational Geometry”, 1993, 9 pp. 187-202.

Problem 31*. If there exist two points such that every line passes through at least one of these points, then the required inequality can be shown as follows. Suppose that a lines pass through the first of these points and that b pass through the second. If $a + b = n$, then

$$a \geq 3, b \geq 3, \quad t_2 = ab, \quad \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i \leq 2a + 2b - 15.$$

If $a + b = n + 1$, then

$$a \geq 4, b \geq 4, \quad t_2 = (a - 1)(b - 1), \quad \sum_{i \geq 4} \left(2i - 7\frac{1}{2}\right) t_i = 2a + 2b - 15.$$

Now let us assume that there are no two points such that every line passes through at least one of them. Apply all the three items of problem 32:

$$3p_4 + \sum_{j \geq 5} jp_j \geq z + x = z + \left(y + 2t_2 - \sum_{i \geq 3} it_i\right) \geq \frac{3}{2} \sum_{i \geq 3} t_i + 2t_2 - \sum_{i \geq 3} it_i = 2t_2 - \sum_{i \geq 3} \left(i - \frac{3}{2}\right) t_i.$$

Using problem 26, we obtain:

$$\sum_{i \geq 2} (9 - 3i)t_i = 9 + 3p_4 + \sum_{j \geq 5} (3j - 9)p_j.$$

Note that $3j - 9 \geq j$ for $j \geq 5$ and $p_j \geq 0$. Hence, we have

$$\sum_{i \geq 2} (9 - 3i)t_i = 9 + 3p_4 + \sum_{j \geq 5} (3j - 9)p_j \geq 3p_4 + \sum_{j \geq 5} jp_j \geq 2t_2 - \sum_{i \geq 3} \left(i - \frac{3}{2}\right) t_i,$$

which implies the required inequality for t_i s.

Problem 32. Consider the corresponding graph: its vertices are the intersection points (colored in one of two colors), the edges are the line segments which do not contain other intersection points except their ends.

(a) Every red vertex is a red edge of four edges. Every red edge has two red edges, every non-colored edge has one red edge, blue edges do not have red ends. There are t_2 red vertices. Hence,

$$4t_2 = 2x + \sum_{i \geq 2} it_i - x - y,$$

which gives the required equality.

(b) Consider an arbitrary blue point O and delete all the lines of the arrangement passing through it. The remaining lines are not concurrent, hence they divide the projective plane into regions, each of them bounded by at least three edges. The point O belongs to one of such regions. By a case-by-case consideration, we see that at least one of the three possibilities holds for O :

(1) In the initial graph, the point O is incident to at least three blue edges.

(2) The point O is incident to at least two blue edges, and O is the vertex of the boundary of at least one green region.

(3) The point O is the vertex of the boundary of at least two green regions.

It means that for every blue vertex, the sum of the number of blue edges incident to it with the doubled number of green regions incident to it is at least 3. If we sum up these sums for all the blue vertices, we obtain $2y + 2s \geq \sum_{i \geq 3} t_i$.

(c) For a green region u , let us define by $x(u)$ and $s(u)$ the number of red edges and the number of blue vertices at the boundary of u , respectively. For a green region u let

$$d(u) = \begin{cases} 0, & \text{if } s(u) \geq 1; \\ 1, & \text{if } s(u) = 0. \end{cases}$$

It is easy to prove that if a green region u is bounded by j edges, then

$$s(u) \leq (j - 1) - x(u) + d(u).$$

Denote by X and by D the sums of $x(u)$ and $d(u)$, respectively, by all the green regions. Summing up the inequality obtained above for all the green regions, we get

$$s \leq \sum_{j \geq 4} (j - 1)p_j - X + D.$$

Note that every red edge is incident to at least one green region (since $t_n = t_{n-1} = 0$). A red edge is called dark red if it is adjacent to two green regions. Let us denote by x_1 the number of dark-red edges. Then $X = x + x_1$. Let us distinguish the 4-hedral regions such that all their vertices are red (all the distinguished regions are green). It is easy to show that every distinguished region is incident to at least two dark-red edges. Hence, the number of distinguished regions is at most x_1 . It follows that $D \leq x_1 + \sum_{j \geq 5} p_j$. Now merge all the inequalities.

КОГДА ЛЮБАЯ ГРУППА ИЗ N ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ?

представляют Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков

Назовем *группой* непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$).¹ Если в группе G найдется преобразование g , для которого $G = \{g, g^2, \dots, g^n, \dots\}$, то группа G называется *циклической*.

Этот цикл задач посвящен следующему интригующему вопросу:

Для каких n любая группа из n перестановок циклическая?

В настоящем цикле задач намечено более простое решение этого вопроса, чем в [В]. Оно не претендует на новизну.

Примеры конечных групп.

(1) Группа S_n всех перестановок n -элементного множества.

(2) Группа перестановок $\{\text{id} = (1)(2)(3)(4), (13)(24), (1234), (1432)\}$ множества из четырех элементов.

(3) Рассмотрим квадрат на плоскости и все движения плоскости, переводящие его в себя. Это тождественное преобразование, 3 поворота и 4 симметрии. Всего 8 преобразований. Возьмем группу из 8 перестановок множества вершин квадрата, происходящих при применении перечисленных восьми преобразований плоскости.

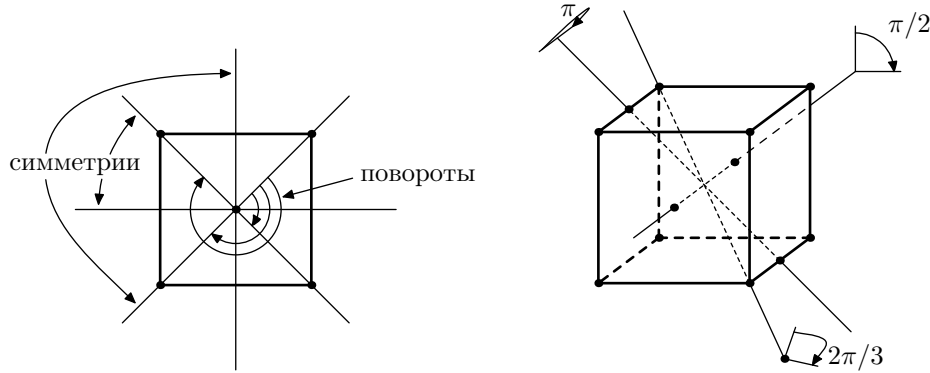


Рисунок: движения квадрата и куба

(4) Рассмотрим куб в пространстве и все вращения пространства (включая тождественное), переводящие его в себя.

(а) Возьмем группу из всех перестановок множества *вершин* куба, происходящих при применении таких вращений.

(б) Возьмем группу из всех перестановок множества *середин ребер* куба, происходящих при применении таких вращений.

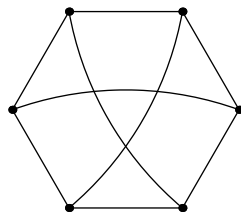


Рисунок: граф $K_{3,3}$

¹ «...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде $f(gh) = (fg)h$. Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет.» (В.И. Арнольд.) При этом на примере решения данного цикла задач школьники увидят, что общее понятие группы все-таки полезно для изучения групп преобразований.

(5) Группа всех перестановок 6-элементного множества, являющихся изоморфизмами графа $K_{3,3}$.

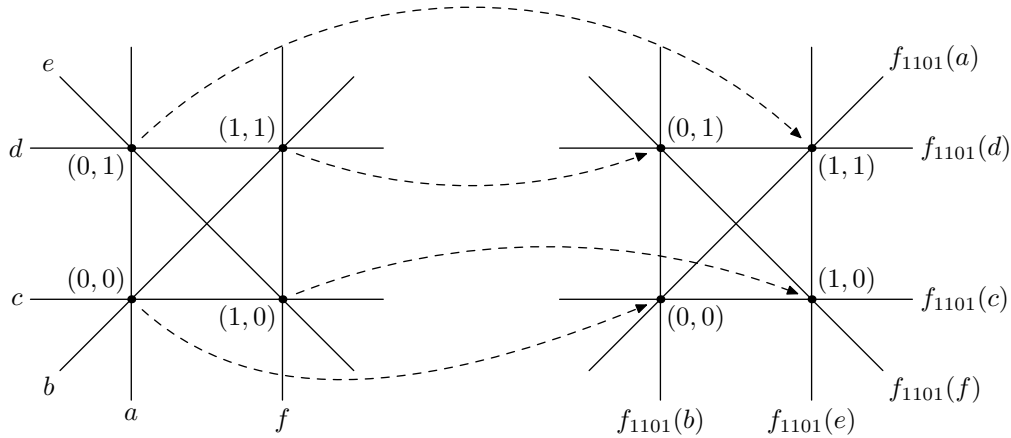


Рисунок: линейное преобразование $f_{1101} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$

(6) Рассмотрим множество $\mathbb{Z}_2^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ упорядоченных пар вычетов по модулю 2. Для любых четырех вычетов a, b, c, d по модулю 2 рассмотрим отображение $f_{abcd} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$, заданное формулой $f_{abcd}(x, y) = (ax + by, cx + dy)$. Среди всех таких отображений выберем взаимно-однозначные. Они образуют группу.

Зачем? На примере исследования этого вопроса мы покажем, как появляются некоторые основные понятия теории групп. Основные идеи будут представлены на «олимпиадных» примерах: на простейших частных случаях и со сведением к необходимому минимуму алгебраического языка.²

«Новичку». За счет принятого стиля изложения Вам *не будет сложнее* решать приведенные задачи, чем школьникам, уже знакомым с основами теории групп. Вы освоите необходимые идеи на примере решения задач 1-й серии, которые все равно просты. Веселые задачи 3-й серии также помогут Вам освоиться.

Школьнику, уже знакомому с основами теории групп. Конечно, Вам будет *интереснее* решать приведенные задачи. Вы можете не разбирать все предлагаемые частные случаи, а сразу доказывать общий результат, из которого они вытекают, чтобы потом сконцентрироваться на новых для Вас задачах. Они имеются уже в самом начале — см. общий вопрос и некоторые пункты задачи 1.5. Если Вы используете другое определение группы, то нужно доказать его эквивалентность вышеприведенному.

Общие замечания к формулировкам задач. Если условие задачи является утверждением, то в задаче требуется это утверждение доказать. Если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками.

Звездочки. За каждое верное ($\geq +.$) письменное решение школьник или команда получает звездочку. По усмотрению жюри звездочка может дополнительно выдаваться за красивые решения, за решения сложных задач и за некоторые решения, набранные в тех'е. Число звездочек у жюри не ограничено. Одну звездочку можно потратить на одну попытку устной сдачи одной из задач.

Благодарим С.А. Дориченко и Г.Р. Челнокова за полезные замечания.

²Это не только сделает материал более доступным, но поможет тем, кто привык к абстрактному изложению, развить математический вкус. Благодаря этому они смогут разумно выбирать проблемы для исследования и ясно излагать собственные открытия, не скрывая ошибок (или известности полученного результата) за чрезмерным формализмом. К сожалению, такое (бессознательное) сокрытие ошибки часто происходит с молодыми математиками, воспитанными на чрезмерно формальных курсах.

1. ДО. 1-я СЕРИЯ.

Через $|X|$ обозначается число элементов в множестве X .

1.1. (а) Код для замка состоит из упорядоченного набора девяти различных ненулевых цифр. Известно следующее правило: если коды A и B открывают замок (допускается возможность $A = B$), то код, полученный заменой каждой цифры k в коде A на цифру, стоящую на k -м месте в коде B , тоже открывает замок. Известно, что замок открывает только код 856291473 и все коды, полученные из него многократным применением указанного правила. Сколько всего кодов открывают замок?

(б) Тот же вопрос для следующего правила: если код A открывает замок и B — произвольный код (допускается возможность $A = B$), то код, полученный заменой каждой цифры в коде A , равной номеру места цифры k в коде B , на цифру, стоящую на k -м месте в коде B , тоже открывает замок.

1.2. (а) Докажите, что множество из примера 6 действительно является группой.

(б) Какие из приведенных примеров групп являются циклическими?

(с) Любая группа содержит тождественное преобразование (оно называется *единичным элементом* и обозначается e).

1.3. (а) Придумайте группу и в ней две перестановки a и b , для которых $ab = b^{-1}a$.

(б) В языке племени Абаба 2 буквы: «а» и «б». Если в любом месте любого слова этого языка вставить или вычеркнуть буквосочетание «ааб» или буквосочетание «бба», то смысл слова от этого не изменится. На скале нацарапано 4 слова на языке Абаба. Докажите, что среди них есть два, совпадающих по смыслу.

1.4. (а) Придумайте группу из 17 перестановок, которые можно так занумеровать числами $0, 1, 2, \dots, 16$, чтобы номер композиции был бы равен *сумме* номеров ‘сомножителей’ по модулю 17.

(б) Придумайте группу из 16 перестановок, которые можно так занумеровать числами $1, 2, \dots, 16$, чтобы номер композиции был бы равен *произведению* номеров ‘сомножителей’ по модулю 17.

(с) Существует ли группа из 8 перестановок, которые можно так занумеровать числами $1, 2, 4, 7, 8, 11, 13, 14$, чтобы номер композиции был бы равен *произведению* номеров ‘сомножителей’ по модулю 15?

1.5. Любая ли группа из n преобразований является циклической для следующих значений n :

(7) 1,2,3,4,5,6,7; (8) 8; (9) 9; (10) 10; (12) 12; (15) 15; (21) 21; (1001) 1001?

Группа G называется *коммутативной*, если $xy = yx$ для любых $x, y \in G$.

Порядком $\text{ord } a$ элемента a группы G с единичным элементом e называется наименьшее целое положительное n , для которого $a^n = e$ (если такое n существует).

1.6. (а) *Теорема Ферма-Эйлера.* Для любого элемента a конечной коммутативной группы G с единичным элементом e выполнено $a^{|G|} = e$.

(б) Любая циклическая группа является коммутативной.

(с) Верно ли обратное?

1.7. Если количество элементов в группе является простым числом, то эта группа циклическая.

1.8. (а) Найдите порядок каждого элемента в группе S_4 .

(б) Любой элемент конечной группы имеет (конечный) порядок.

(с) Если в конечной группе есть элемент порядка 2, то число элементов группы четно.

(d) Если в конечной группе есть элемент порядка 3, то число элементов группы делится на 3.

(e) *Теорема Лагранжа.* Число элементов конечной группы делится на порядок любого ее элемента.

(f) В любой группе из четного числа элементов есть элемент порядка 2.

1.9. (a) Если число n четное составное, то существует группа из n преобразований, не являющаяся циклической.

(b) Если число n делится на квадрат простого, то существует группа из n преобразований, не являющаяся циклической.

1.10. (a) Любая коммутативная группа из 10 элементов является циклической.

(b) То же для 21 элемента.

(c) То же для 1001 элемента.

(d) Для каких n любая коммутативная группа из n элементов является циклической?

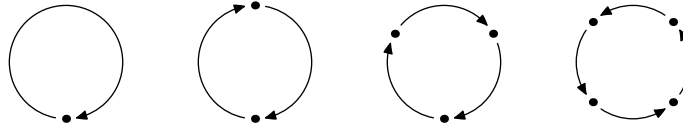


Рисунок: перестановка типа $\langle 1, 2, 3, 4 \rangle$

1.11. Перестановка $(n_1 + \dots + n_k)$ -элементного множества, являющаяся композицией непересекающихся циклов порядков $n_1, \dots, n_k$, называется перестановкой типа $\langle n_1, \dots, n_k \rangle$.

(a) Докажите, что любые две перестановки f и g одного типа сопряжены в группе S_n , т.е. $g = b^{-1}fb$ для некоторой перестановки $b \in S_n$.

(b) Докажите обратное.

(c) Порядки сопряженных перестановок равны.

1.12. Пусть G — группа из 15 элементов.

(a) В G есть элемент порядка 3.

(b) Любой элемент порядка 5 в G сопряжен только со своими степенями.

2. ДО. 2-я СЕРИЯ.

Некоторые решения.

Решение задачи 1.2. (c) $f \in G \Rightarrow f^{-1} \in G \Rightarrow ff^{-1} = e \in G$.

Решение задачи 1.5-7 для $n = 3$. Пусть, напротив, имеется нециклическая группа G из трех перестановок. Обозначим через a нетождественную перестановку в ней. Если $a^2 \neq e$, то перестановки a, a^2, a^3 различны и группа циклическая. Если же $a^2 = e$, то рассмотрим перестановку $b \in G$, отличную от e и a . Тогда перестановка ab отлична от e, a, b . (Действительно $ab \neq a$ и $ab \neq b$ очевидно. Если $ab = e$, то $b = a^2b = a$ — противоречие.) Противоречие.

Решение задачи 1.5-10. Рассмотрим правильный пятиугольник на плоскости. Рассмотрим все движения плоскости, переводящие его в себя. Это тождественное преобразование, 4 поворота и 5 симметрий. Всего 10 преобразований. Нужную группу образуют 10 перестановок множества вершин правильного пятиугольника, происходящих при применении перечисленных десяти преобразований плоскости. Эта группа нециклическая, поскольку для двух перестановок s и t , «пришедших из симметрий», $st \neq ts$. А если бы $s = g^k$ и $t = g^l$ для некоторой перестановки g , то $st = ts$.

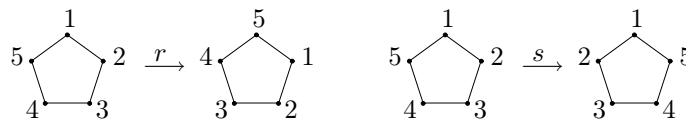


Рисунок: движения правильного 5-угольника

Другое решение задачи 1.5-10. Оно более сложное, чем предыдущее, но зато может помочь Вам в решении задачи 2.1. Рассмотрим перестановки r и s 5-элементного множества вершин правильного 5-угольника, «пришедшие» из поворота на $2\pi/5$ и из симметрии; см. рисунок. Тогда $r^5 = e = s^2$ и $sr = r^{-1}s$. Рассмотрим 10 перестановок $r^k s^l$, $k, l \in \mathbb{Z}$. Из соотношения $sr = r^{-1}s$ можно получить, что это множество является группой. (Именно в этом отличие приводимого решения от предыдущего — мы получили замкнутость относительно композиции и взятия обратного не из геометрических соображений, а из комбинаторных. Поэтому появилась возможность обобщать это доказательство на случаи, когда геометрической интерпретации не видно.) Из этого же соотношения вытекает, что эта группа не является циклической.

Новые задачи.

- 2.1.** (a) Существует нециклическая группа из 21 элемента.
 (b) Существует нециклическая группа из 55 элементов.
 (c) Если p и q простые числа и $q - 1$ делится на p , то существует нециклическая группа из pq элементов.

Указание к 2.1а. См. вышеприведенное другое решение задачи 1.5-10. Попробуйте сообразить, каким соотношениям должны удовлетворять перестановки r и s , чтобы множество $r^k s^l$, $k, l \in \mathbb{Z}$, образовывало бы нециклическую группу из 21 перестановки. А потом попробуйте придумать такие перестановки.

Подгруппой группы G называется подмножество группы G , также являющееся группой.

- 2.2.** (a) Может ли в коммутативной группе из 10 элементов быть два различных элемента порядка 2? (Это подсказка к задаче 1.10а.)

(b) *Теорема Лагранжа.* Число элементов в конечной группе делится на число элементов в любой ее подгруппе.

- 2.3.** (Это подсказка к задаче 1.12b.) Пусть G — группа из 15 элементов и $f, g \in G$ — элементы порядка 5.

- (a) Множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ либо не пересекаются, либо совпадают.
 (b) Один из элементов f, g является степенью другого.

- 2.4.** Пусть G — группа из 15 элементов, $f \in G$ — элемент порядка 5, $b \in G$, $b^{-1}fb = f^m$ и $k \in \mathbb{Z}$, $k > 0$. Тогда $b^{-1}f^k b = f^{km}$ и $b^{-k}fb^k = f^{m^k}$.

- 2.5.** Пусть G — группа из 15 элементов, в которой каждый неединичный элемент имеет порядок 3. Пусть $f, g \in G - e$.

- (a) Множества $\{f, f^2\}$ и $\{g, g^2\}$ либо не пересекаются, либо совпадают.
 (b) Если $\{f, f^2\} \neq \{g, g^2\}$, то $fg \neq gf$.
 (c) С каждым неединичным элементом сопряжено ровно 4 других элемента.

- 2.6.** (a) Если число преобразований в группе есть произведение pq простых чисел, $p < q$ и $q - 1$ не делится на p , то эта группа циклическая.

(b) Пусть G — группа из 1001 элемента и $f \in G - \{e\}$. Докажите, что G циклическая, если f сопряжен только со своими степенями.

3. ДО. 3-я СЕРИЯ

Веселые задачи этой серии на более абстрактном языке описывают важную идею, приведенную в указании к задаче 2.1а. Формально, они не нужны для нашей главной цели.

3.1. ³ В языке Велосипедистов (англ. Cyclists) имеется две буквы a и a^{-1} . Они называются *противоположными*.

В этом и других рассматриваемых языках *словами* называются все конечные упорядоченные наборы из букв; в частности, имеется *пустое* слово, в котором нет букв (т.е. молчание тоже имеет значение).

Слово «восьмерка», состоящее из восьми букв a подряд, считается *неприличным*. Слово, состоящее из двух противоположных букв подряд, называется *запинкой*.

В этом и других рассматриваемых языках смысл слова не меняется от

• зачеркивания в любом месте любого неприличного подслова или запинки, а также от

• добавления в любое место любого неприличного подслова или запинки.

(Научно выражаясь, смысл — класс эквивалентности слов относительно операций вставки и удаления неприличных слов или запинок).

Например, на языке Велосипедистов слова $aaaa^{-1}a$ и aaa различны, но имеют одинаковый смысл.

(a) У Велосипедистов имеется всего 8 смыслов.

(b) Велосипедисты разговаривают о вычетах по модулю 8. Иными словами, множество смыслов с операцией приписывания *изморфно* множеству вычетов по модулю 8 с операцией суммы по модулю 8. Приведем четкую формулировку этого утверждения. Слова можно приписывать одно к другому: из слов X и Y получается слово XY . (Например, из слов aa и $aa^{-1}a$ получается слово $aaaa^{-1}a$.) Эта операция на множестве слов задает операцию «приписывания» на множестве смыслов. Так вот, восемь смыслов можно занумеровать вычетами по модулю 8 так, что номер смысла слова XY равен сумме (по модулю 8) номера смысла слова X и номера смысла слова Y .

3.2. Для обеспечения секретности сотрудники Пентагона придумали специальный язык. В нем имеются четыре буквы a, b, a^{-1} и b^{-1} . Буквы a и a^{-1} называются *противоположными*. Буквы b и b^{-1} тоже. Пять букв a подряд или две буквы b подряд образуют неприличное слово. Еще одно неприличное слово — ... В нем 4 буквы, первые три из которых — такие же, как в слове $abab$, а последние три из которых — такие же, как в слове $a^{-1}bbab^{-1}$.

(a) У сотрудников Пентагона имеется всего 10 смыслов.

(b) Сотрудники Пентагона разговаривают о движениях множества вершин правильного пятиугольника на плоскости. Дайте сами четкую формулировку этого утверждения!

3.3. В языке Ценителей Совершенства также четыре буквы a, b, a^{-1} и b^{-1} . Три буквы a подряд или две буквы b подряд образуют неприличное слово. Еще одно неприличное слово — ... В нем 10 букв, и оно получается записыванием пять раз подряд слова ba .

(a) У Ценителей Совершенства имеется конечное количество смыслов.

(b) Ценители Совершенства разговаривают о некоторой группе. Дайте сами четкую формулировку этого утверждения!

3.4. (a) В языке Алгебраистов также четыре буквы a, b, a^{-1} и b^{-1} . Неприличные слова настолько неприличны, что в этом тексте неуместно не только описывать их, но даже говорить, конечно ли их число. Докажите, что Алгебраисты разговаривают о некоторой группе. Дайте сами четкую формулировку этого утверждения! (Эта группа может оказаться бесконечной, даже если неприличных слов конечное число.)

(b) Если в язык Алгебраистов добавить новые буквы c и c^{-1} и некоторые новые неприличные слова, то Алгебраисты по-прежнему будут разговаривать о некоторой группе.

³Это — пример *некрасивой* задачи по математике. Понять ее условие сложнее, чем придумать решение (понимая условие). Однако нам эта задача нужна, чтобы на простейшем примере показать важную конструкцию.

4. ПОСЛЕ. 4-я СЕРИЯ.

Некоторые решения.

1.8. (d) Пусть a — элемент порядка 3. Выпишем все элементы группы. Теперь будем постепенно зачеркивать их следующим образом: на каждом шаге выбираем произвольным образом незачеркнутый элемент x и зачеркиваем 3 элемента x, xa, xa^2 . При этом никакой элемент мы не зачеркнем больше одного раза: действительно, предположим, что, например, зачеркиваемый элемент xa уже был зачеркнут. Тогда либо $xa = y$, либо $xa = ya$, либо $xa = ya^2$ для некоторого ранее выбранного элемента y . Но тогда либо $x = ya^2$, либо $x = y$, либо $x = ya$. Таким образом, элемент x уже был зачеркнут. Полученное противоречие доказывает, что на каждом шаге зачеркивается ровно 3 новых элемента. В конце будут зачеркнуты все элементы. Значит, число элементов группы делится на 3.

(e) *Теорема Лагранжа.* Для $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$. По определению порядка указанные элементы различны. Значит, в этом множестве $\text{ord } f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\text{ord } f$.

1.10. (a) Обозначим через p порядок неединичного элемента f . Если $p = 10$, то группа циклическа. Пусть теперь $p < 10$. По теореме Лагранжа $p \in \{5, 2\}$. Если есть элемент g порядка $10/p$, то $G = \{fg, (fg)^2, \dots, (fg)^{10}\}$. Иначе есть элемент $g \notin \{f, f^2, \dots, f^p\}$ порядка p . Тогда $\{f^k g^l\}_{k,l \in \mathbb{Z}}$ есть подгруппа порядка p^2 . Противоречие с теоремой Лагранжа.

1.11. *Указание.* Перенумеруем элементы множества так, чтобы f перешла в g . Эта перенумерация задает требуемую перестановку b .

2.3. (a) Предположим, что эти множества пересекаются. Тогда существуют такие натуральные числа $1 \leq k, l \leq 4$, что $f^k = g^l$. Так как $\text{НОД}(k, 5) = 1$, то существует такое целое число m , что $5 \mid km - 1$. Тогда $f = f^{km} = (f^k)^m = (g^l)^m = g^{lm}$. Отсюда следует, что эти множества совпадают.

(b) Рассмотрим 25 элементов $f^k g^l$ для $1 \leq k, l \leq 5$. Так как в группе всего 15 элементов, то существуют $1 \leq k, l, m, n \leq 5$ такие, что $(k, l) \neq (m, n)$ и $f^k g^l = f^m g^n$. Домножая на f^{-m} слева и на g^{-l} справа, получаем $f^{k-m} = g^{n-l}$. Так как f и g — элементы порядка 5, то множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ пересекаются. Из (a) получаем, что они совпадают.

2.5. (c) *Указание.* Рассмотрим элемент $f \neq e$. Обозначим число сопряженных с ним элементов $c(f)$ (вместе с самим элементом f). Рассмотрим множество

$$Z(f) := \{g \in G : fg = gf\}$$

. Из (b) следует, что $Z(f) = \{e, f, f^2\}$. Теперь из того, что $c(f) \cdot |Z(f)| = |G|$ получаем $c(f) = 15/3 = 5$.

2.1. (a) *Новое указание.* Искомая группа является группой некоторых перестановок 49-элементного множества $\mathbb{Z}_7^2$. Для описания группы представим его элементы как пары (x, y) вычетов по модулю 7. Для любых целых неотрицательных k, l определим преобразование

$$f_{k,l} : \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^2 \quad \text{формулой} \quad f_{k,l}(x, y) := (2^k x, lx + y).$$

Проверьте, что

- таких преобразований ровно 21;
- они образуют группу;
- эта группа не является циклической.

2.1. (b) *Указание.* Воспользуйтесь тем, что $2^5 = 33 - 1$. Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_{11}^2 \rightarrow \mathbb{Z}_{11}^2$ формулой $f_{k,l}(x, y) := (4^k x, lx + y)$.

3.3. *Указание.* Проще всего использовать то, что Ценители Совершенства являются Алгебраистами.

3.4. *Указание.* Сопоставьте каждому смыслу преобразование множества смыслов, определяемое как «приписывание данного смысла слева».

Новые задачи.

4.1. Существует нециклическая группа из 39 элементов.

4.2. Пусть G — группа из 1001 элемента и $f \in G - \{e\}$. Предположим, что f сопряжен только с некоторыми своими степенями. Пусть $h \notin \langle f \rangle := \{f, f^2, \dots, f^n, \dots\}$. Обозначим через q наименьшее из целых положительных n , для которых $h^n \in \langle f \rangle$.

- (a) q делит $\text{ord } h$.
- (b) Если $h^{-1}fh = f^k$, то $h^{-n}fh^n = f^{k^n}$.
- (c) $h^{-1}fh = f$.
- (d) $\{fh, (fh)^2, (fh)^3, \dots, (fh)^{q \cdot \text{ord } f}\}$ подгруппа в G .

4.3. Пусть G — группа из 1001 элемента, не являющаяся циклической.

(a) Каждый элемент содержится в максимальной по включению подгруппе, не совпадающей со всей G .

Такие подгруппы будем сокращенно называть *максимальными подгруппами*.

(b) Каждая максимальная подгруппа является циклической.

4.4. Назовем *коммутативизатором* группы G множество

$$Z = Z(G) := \{a \in G : ga = ag \text{ для любого } g \in G\}$$

тех элементов, которые коммутируют со всеми. (Мы надеемся, что использование слова *коммутативизатор* вместо общепринятого *центр* более удобно для начинающих.)

- (a) Найдите $Z(S_n)$ для каждого $n = 2, 3, 4, \dots$
- (b) Коммутативизатор группы является подгруппой.

4.5. Пусть G — группа из 1001 элемента, не являющаяся циклической. Пусть порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.

- (a) Любая максимальная подгруппа содержит коммутативизатор.
- (b) Выразите через $|F|$ и $|Z|$ число элементов, сопряженных элементам максимальной подгруппы F .

5. ПОСЛЕ. 5-я СЕРИЯ

Указание к задаче 1.4с. Такую группу удобно придумывать как подгруппу в группе перестановок множества $\{1, 2, 4, 7, 8, 11, 13, 14\}$

5.1. (a) Для любых группы G и элемента $g \in G$ множество

$$N(g) = N_G(g) := \{a \in G : ga = ag^k \text{ для некоторого } k\}$$

является подгруппой.

- (b) Найдите $N_{S_3}(g)$ для каждого $g \in S_3$.
- (c) Число различных подгрупп, сопряженных с $\langle g \rangle$, равно $|G|/|N(g)|$.

5.2. Пусть G — группа из 1001 элемента, не являющаяся циклической. Предположим, что порождающий элемент любой максимальной подгруппы (напомним, что по утверждению задачи 4.3b она циклическая) сопряжен не только со своими степенями.

- (a) Пересечение двух максимальных подгрупп равно коммутативизатору.
- (b) Число различных подгрупп, сопряженных с максимальной подгруппой F , равно $1001/|F|$.
- (c) Для числа $\hat{F}$ элементов, сопряженных элементам максимальной подгруппы F и не лежащих в коммутативизаторе, справедливы неравенства $500 < \hat{F} \leq 1000 - |Z|$.

Теорема о первообразном корне. Для любого простого p существует число g , для которого остатки от деления на p чисел $g^1, g^2, g^3, \dots, g^{p-1} \equiv 1 \pmod p$ различны.

5.3. Доказательство теоремы о первообразном корне. Здесь латинскими буквами обозначаются целые неотрицательные числа. Пусть p простое и a не делится на p .

(а) $p - 1$ делится на наименьшее $k > 0$, для которого $a^k \equiv 1 \pmod{p}$.

Указание: используйте малую теорему Ферма.

(b) Для любых целых n и a сравнение $x^n \equiv a \pmod{p}$ имеет не более n решений.

(c) Если $p - 1$ делится на d , то сравнение $x^d \equiv 1 \pmod{p}$ имеет ровно d решений.

(d) Докажите теорему о первообразном корне для $p = 2^m + 1$.

(e) Докажите теорему о первообразном корне для $p = 2^m \cdot 3^n + 1$.

(f) Докажите теорему о первообразном корне для произвольного простого p .

(g)* Верно ли, что число 3 является первообразным корнем по модулю любого простого числа вида $p = 2^m + 1$?

5.4. Для каких n любая группа из n элементов является коммутативной?

6. УКАЗАНИЯ И РЕШЕНИЯ, ВЫДАВАЕМЫЕ ПОСЛЕ ОКОНЧАТЕЛЬНОГО ФИНИША

2.1c. По теореме о первообразном корне существует элемент $a \in \mathbb{Z}_q$ порядка p . Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_q^2 \rightarrow \mathbb{Z}_q^2$ формулой $f_{k,l}(x, y) := (a^k x, lx + y)$. Нетрудно проверить, что

- таких преобразований ровно pq ;
- они образуют группу;
- эта группа не является циклической.

3.1. Указание. Положим номер смысла данного слова равным разности между числом букв a и a^{-1} в этом слове по модулю 8.

3.2. Указание. Биекция между смыслами и движениями правильного пятиугольника строится следующим образом: букве a поставим в соответствие поворот на 72° против часовой стрелки с центром в центре пятиугольника. Букве b поставим в соответствие такое отражение, что выполняется $a \circ b \circ a \circ b^{-1} = id$; смыслу слова будет соответствовать композиция движений, соответствующих его буквам.

3.3b. Первое решение. Следует из задачи 3.4a.

3.3b. Второе решение. Ценители Совершенства разговаривают о группе всех таких перестановок вершин правильного икосаэдра, которые получены из вращений трехмерного пространства, переводящих икосаэдр в себя. То есть о группе A_5 .

4.2. (b) Утверждение доказывается индукцией по n .

5.3. Указания. (b) Докажем более общее утверждение: *многочлен степени n не может иметь более n корней в множестве $\mathbb{Z}/p\mathbb{Z}$ вычетов по модулю p (в котором имеются операции сложения и умножения по модулю p)*. Здесь многочленом называется бесконечный упорядоченный набор $(a_0, \dots, a_n, \dots)$ вычетов по модулю p , в котором лишь конечное число элементов отлично от нуля. Обычно многочлен записывается в виде $a_0 + a_1x + \dots + a_kx^k$ (если $a_{k+1} = a_{k+2} = \dots = 0$). Эта запись дает отображение $\mathbb{Z}/p\mathbb{Z} \rightarrow \mathbb{Z}/p\mathbb{Z}$. Будьте осторожны: разным многочленам может соответствовать одно и то же отображение. Корнем многочлена $a_0 + a_1x + \dots + a_kx^k$ называется такой вычет x_0 по модулю p , что выполнено

$$a_0 + a_1x_0 + \dots + a_kx_0^k = 0.$$

Пусть многочлен $P(x)$ степени n имеет в $\mathbb{Z}_p$ различные корни $x_1, \dots, x_n, x_{n+1}$. Представьте его в виде

$$P(x) = b_n(x - x_1) \dots (x - x_n) + b_{n-1}(x - x_1) \dots (x - x_{n-1}) + \dots + b_1(x - x_1) + b_0$$

(‘интерполяция Ньютона’). Последовательно подставляя в сравнение $P(x) \equiv 0 \pmod{p}$ вычеты $x_1, \dots, x_n, x_{n+1}$, получим $b_0 \equiv b_1 \equiv \dots \equiv b_{n-1} \equiv b_n \equiv 0 \pmod{p}$.

То же самое решение можно записать и так. Пусть P — многочлен. Тогда $P - P(a) = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Поэтому если $P(a) = 0$, то

$P = (x - a)Q$ для некоторого многочлена Q степени меньше $\deg P$. Теперь требуемое в задаче утверждение доказывается индукцией по степени многочлена P с использованием простоты числа p .

(с) *Первое указание.* Заметьте, что многочлен $x^{p-1} - 1$ имеет ровно $p - 1$ корень в множестве $\mathbb{Z}/p\mathbb{Z}$ и делится на $x^d - 1$. Докажите, что если многочлен степени a имеет ровно a корней и делится на многочлен степени b , то этот многочлен степени b имеет ровно b корней.

(с) *Второе указание.* Если $p = kd$, то для любого a сравнение $y^k \equiv a \pmod{p}$ имеет не более k решений.

(d) Если первообразного корня нет, то по (а) сравнение $x^{2^{m-1}} \equiv 1 \pmod{p}$ имеет $p - 1 = 2^m > 2^{m-1}$ решений.

(e,f) Аналогично (d).

5.4. Указание. Все группы порядка n абелевы тогда и только тогда, когда в разложении числа n на простые сомножители $n = p_1^{k_1} \dots p_l^{k_l}$

- $k_i < 3$;
- p_i не делит $p_j^{k_j} - 1$.

Доказывается это примерно так же, но в случае 1 надо воспользоваться тем, что любая конечная абелева группа раскладывается в прямое произведение циклических подгрупп.

Остальные задачи тривиальны или покрываются прилагаемым текстом [BKS].

Литература

[A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.

[B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf

[BKS] В. Брагин, А. Клячко, А. Скопенков. Когда любая группа из n элементов циклическая?

[KS] Л.А. Калужнин, В.И. Слущанский, Преобразования и перестановки. М.: 1979, 112 стр.

[KM] Каргаполов М.И., Мерзляков Ю.И., Основы теории групп, М., Наука, 1982. <http://arhivknig.com/obrazovanie/87077-osnovy-teorii-grupp.html>

[K] А.И. Кострикин, Введение в алгебру. Основы алгебры. 1994.

КОГДА ЛЮБАЯ ГРУППА ИЗ n ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ? ¹

В. Брагин, Ант. Клячко и А. Скопенков

В этой заметке приводится простое доказательство известного факта: любая группа из n элементов является циклической тогда и только тогда, когда n взаимно просто с $\phi(n)$. Заметка доступна школьникам: для понимания не требуется знаний по теории групп. Она может быть также интересным ‘легким чтением’ для профессиональных математиков.

Введение

Назовем *группой* непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). Общепринятое название: группа преобразований. Ср. [А, стр. 49, комментарий к задаче 5].

Если в конечной группе G найдется преобразование g , из всех возможных степеней которого состоит G (т.е. $G = \{g, g^2, \dots, g^n, \dots\}$), то группа G называется *циклической*.

Мы докажем следующую теорему.

Теорема (фольклор). *Любая группа из n элементов является циклической тогда и только тогда, когда n взаимно просто с $\phi(n)$.*

Здесь $\phi(n)$ — количество целых чисел от 1 до n , взаимно простых с n (функция Эйлера).

Заметим, что условие взаимной простоты n и $\phi(n)$ равносильно тому, что в разложении числа n на простые сомножители $n = p_1 \dots p_t$

(*) все p_i различны и

(**) p_i не делит $p_j - 1$ ни для каких i и j .

Для понимания доказательства не требуется никаких знаний по теории групп. Небольшое количество необходимых понятий вводятся в процессе доказательства. В частности, наше доказательство не привлекает (явно или неявно) понятия факторгруппы, в отличие от более традиционных доказательств (см., например, [В]). Идея приводимого доказательства близка к [???]. Как придумать приводимое доказательство, видно из [BKKSS].

Доказательство части «только тогда»

Если нарушается вышеприведенное условие (*), например, $p_1 = p_2 = p$, то в качестве нециклической группы из n элементов можно взять группу

$$\left\{ (1, 2, \dots, p)^i (p+1, p+2, \dots, 2p)^j (2p+1, 2p+2, \dots, 2p+\frac{n}{p^2})^k \mid i, j = 1, \dots, p, k = 1, \dots, \frac{n}{p^2} \right\}.$$

Если нарушается вышеприведенное условие (**), например, p_1 делит $p_2 - 1$, то по теореме о первообразном корне существует элемент $a \in \mathbb{Z}_{p_2}$, для которого степени $a, a^2, \dots, a^{p_1} = 1$ различны. Обозначим через G_{p_1, p_2} группу преобразований $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$, заданных формулой $f_{k, l}(x, y) := (a^k x, lx + y)$ для $k \in \mathbb{Z}_{p_1}$ и $l \in \mathbb{Z}_{p_2}$.² Тогда в качестве нециклической (даже некоммутативной) группы из n элементов можно взять группу

$$\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}. \quad QED$$

Доказательство части «тогда».

Через $|X|$ обозначается число элементов в множестве X . Обозначим данную группу через G . Используем индукцию по числу простых сомножителей в $n = |G|$. Если сомножитель один, то часть «тогда» вытекает из следующей теоремы Лагранжа.

Порядком $\text{ord } a$ элемента a группы с единичным элементом e называется наименьшее целое положительное n , для которого $a^n = e$. Если группа конечна, то ясно, что такое n существует.

¹Обновляемая версия поддерживается на www.arxiv.org. Благодарим К. Кохаса за полезные замечания.

²Научно говоря, $G_{p_1, p_2} = \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, l \in \mathbb{Z}_{p_2} \right\}$.

Теорема Лагранжа (частный случай). Число элементов конечной группы делится на порядок любого ее элемента.

Доказательство. Обозначим данную группу через G . Для любого $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, x f^{\text{ord } f-1}\}$. По определению порядка указанные элементы различны. Значит, в этом множестве $\text{ord } f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\text{ord } f$. QED

Пусть теперь простых сомножителей в $n = |G|$ больше одного. Нам понадобится следующая общая версия теоремы Лагранжа.

Подгруппой группы называется подмножество этой группы, которое само по себе является группой.

Теорема Лагранжа. Число элементов конечной группы делится на число элементов любой ее подгруппы.

Доказательство. Обозначим данную группу через G , а ее подгруппу через $\{h_1, \dots, h_m\}$. Для любого $x \in G$ рассмотрим множество $\{xh_1, xh_2, \dots, xh_m\}$. В этом множестве $|H|$ элементов. Если $xh_k = yh_l$, то $y = xh_k h_l^{-1}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на m . QED

Максимальной подгруппой назовем максимальную по включению подгруппу, не совпадающую со всей группой и содержащую более одного элемента. По предположению индукции и теореме Лагранжа каждая максимальная подгруппа является циклической.

Для элемента f группы G обозначим через $\langle f \rangle \subset G$ множество всех его степеней (в т.ч. нулевых и отрицательных). Элемент f называется **порождающим** для (циклической) подгруппы $\langle f \rangle$.

Предположим противное, т.е. что группа G не является циклической. Тогда каждый элемент f содержится в некоторой максимальной подгруппе (в максимальной по включению подгруппе, содержащей $\langle f \rangle$).

Элементы f и g группы G называются **сопряженными** в G , если $g = b^{-1}fb$ для некоторого $b \in G$.

Первый случай: порождающий элемент f некоторой максимальной подгруппы сопряжен только с некоторыми своими степенями. Возьмем $h \in G - \langle f \rangle$. Тогда $h^{\text{ord } h} \in \langle f \rangle$. Обозначим через q наименьшее из целых положительных n , для которых $h^n \in \langle f \rangle$. Возьмем $k \in \mathbb{Z}$, для которого $h^{-1}fh = f^k$. Так как $h^q \in \langle f \rangle$, то $f = h^{-q}fh^q = f^{k^q}$ (последнее равенство доказывается индукцией по q). Поэтому $k^q \equiv 1 \pmod{\text{ord } f}$.

По условию (*) и теореме Лагранжа $\text{ord } f$ является произведением $p_1 \dots p_s$ различных простых. Тогда $k^q \equiv 1 \pmod{p_i}$ для любого $i = 1, 2, \dots, s$. Так как $|G|$ делится на $\text{ord } h$ и $\text{ord } h$ делится на q , то по условию (*) q является произведением различных простых. По условию (**) ни одно из этих простых p_j не делит никакое $p_i - 1$. Следовательно, q взаимно просто с каждым $p_i - 1$. Поэтому существуют целые $x = x_i$ и $y = y_i$, для которых $qx + (p_i - 1)y = 1$. Значит, $k \equiv k^{qx+(p_i-1)y} \equiv 1 \pmod{p_i}$ для любого $i = 1, 2, \dots, s$. Поэтому $k \equiv 1 \pmod{\text{ord } f}$, т.е. $fh = hf$.

Тогда в G есть подгруппа $\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$ из $q \text{ord } f$ элементов. Значит, по условию (*) и теореме Лагранжа $\text{ord } f$ и q взаимно просты. Так как $(fh)^j = f^j h^j$ для любого j , то $\text{ord}(fh)$ делится на q и на $\text{ord } f$. Поэтому $\text{ord}(fh) = q \text{ord } f$. Так как подгруппа $\langle f \rangle$ максимальна, то $\langle fh \rangle = G$. Значит, G циклическая. Противоречие.

Второй случай: порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.

Произведением двух подмножеств X и Y группы G называют множество всевозможных произведений xu , где $x \in X$ и $u \in Y$. Если одно из этих подмножеств состоит только из одного элемента, например, $Y = \{u\}$, то для краткости пишут Xu вместо $X\{u\}$.

(1) Любая максимальная подгруппа F содержит центр

$$Z = Z(G) := \{a \in G : ga = ag \text{ для любого } g \in G\},$$

т.е. множество тех элементов, которые коммутируют со всеми.

Доказательство утверждения (1). Иначе FZ — большая коммутативная подгруппа. Ввиду максимальной F имеем $FZ = G$. Противоречие с условием второго случая. QED

(2) Пересечение двух максимальных подгрупп равно центру.

Доказательство утверждения (2). Неединичный элемент в пересечении коммутирует с элементами обеих подгрупп. Значит, он коммутирует с любым произведением нескольких сомножителей, каждый из которых лежит в одной из наших подгрупп. Множество таких произведений является подгруппой. В силу максимальной наших подгрупп эта подгруппа совпадает со всей группой. Значит, пересечение содержится в центре.

Из (1) вытекает обратное включение. QED

(3) Для любой максимальной подгруппы F число различных подгрупп, сопряженных с F (включая F), равно $|G|/|F|$.

Доказательство утверждения (3). Рассмотрим множество

$$N(F) := \{a \in G : Fa = aF\}.$$

Нетрудно проверить, что $N(F)$ является подгруппой. По условию второго случая $N(F) \neq G$. Так как $N(F) \supset F$, то в силу максимальной $N(F) = F$.

Сопряжение каждым элементом группы G переводит подгруппу F в одну из сопряженных подгрупп. Если сопряжение двумя разными элементами u, v группы G переводит подгруппу F в одну и ту же подгруппу, т.е. $u^{-1}Fu = v^{-1}Fv$, то $Fuv^{-1} = uv^{-1}F$. Это означает, что $uv^{-1} \in N(F) = F$ или, что то же самое, $u \in Fv$. Обратно, условие $u \in Fv$ влечет $u^{-1}Fu = v^{-1}Fv$.

Ясно, что $|Fv| = |F|$. Поэтому число элементов в G , сопряжение с которыми переводит подгруппу F в данную фиксированную сопряженную подгруппу, равно $|F|$. Значит, число подгрупп, сопряженных к F , ровно в $|F|$ раз меньше, чем $|G|$. QED

(4) Обозначим через $\hat{F}$ число элементов, сопряженных элементам максимальной подгруппы F и не лежащих в центре. Тогда $|G|/2 \leq \hat{F} < |G| - |Z|$.

Доказательство утверждения (4). Подгруппа, сопряженная к максимальной, также максимальна. (Действительно, если $g^{-1}Fg \subset F' \subset G$, то $F \subset gF'g^{-1} \subset G$.)

$$\text{Поэтому и ввиду (3)} \quad \hat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right).$$

Так как $|G| > |F|$, то $\hat{F} < |G| - |Z|$.

По условию второго случая $Z \neq F$. По (1) и теореме Лагранжа $|Z|$ делит $|F|$. Поэтому $\hat{F} \geq |G|/2$.

Завершение разбора второго случая: подсчет. Пусть $F_1, \dots, F_s$ — наибольший набор попарно несопряженных максимальных подгрупп. Напомним, что любой элемент группы содержится в некоторой максимальной подгруппе. Значит, он сопряжен некоторому элементу в некоторой подгруппе F_i . Тогда ввиду (2) $|G| = |Z| + \sum_i \hat{F}_i$. Ввиду левого неравенства в (4) число слагаемых не превосходит единицы. Ввиду правого неравенства в (4) одного слагаемого тоже быть не может. QED

Литература

- [A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.
 [B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf
 [BKKSS] Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков, Когда любая группа из n элементов циклическая? Материалы ЛКТГ 2011, www.turgor.ru

WHEN ARE ALL GROUPS OF ORDER N CYCLIC?

D. Baranov, A. Klyachko, K. Kokhas, A. Skopenkov and M. Skopenkov

A *group* is a nonempty set of transformations (= permutations or rearrangements of elements) of some set such that it is closed with respect to compositions of transformations and taking the inverse transformation. (i.e., if $f, g \in G$ then $f \circ g \in G$ and $f^{-1} \in G$). We say that a group G is *cyclic*, if there exists a transformation $g \in G$ such that $G = \{g, g^2, \dots, g^n, \dots\}$.

This set of problems is devoted to the following intriguing question:

For which n an arbitrary group of n permutations is cyclic?

Examples of (finite) groups.

- (1) The group S_n of *all* permutations of a n -element set. It is called a *symmetric group*.
- (2) The group $\{\text{id}, (13)(24), (1234), (1432)\}$ of transformations of a set consisting of 4 elements.
- (3) Consider a square on the plane and all the transformations of the plane that map the square onto itself. These are the identity transformation, 3 rotations and 4 symmetries; 8 transformations in all. Let the group consist of 8 permutations of the set of vertices of the square induced by these 8 transformations.

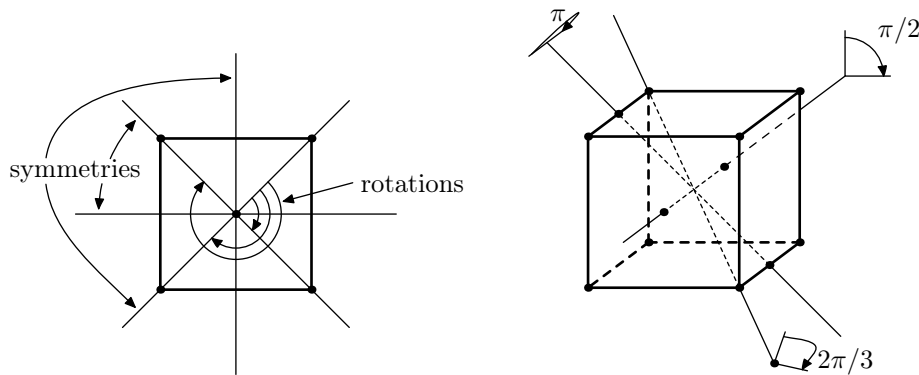


Figure: transformations of a square and a cube.

- (4) Consider a cube in the 3-dimensional space and all the rotations of the space mapping the cube onto itself.

(a) Consider the group of all permutations of the set of *vertices* of the cube induced by these rotations.

(b) Consider the group of all permutations of the set of *edge midpoints* of the cube induced by these rotations.

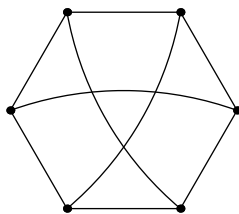


Figure: the graph $K_{3,3}$

- (5) The group of all permutations of the 6-element set of vertices of the graph $K_{3,3}$ which are isomorphisms of the graph.

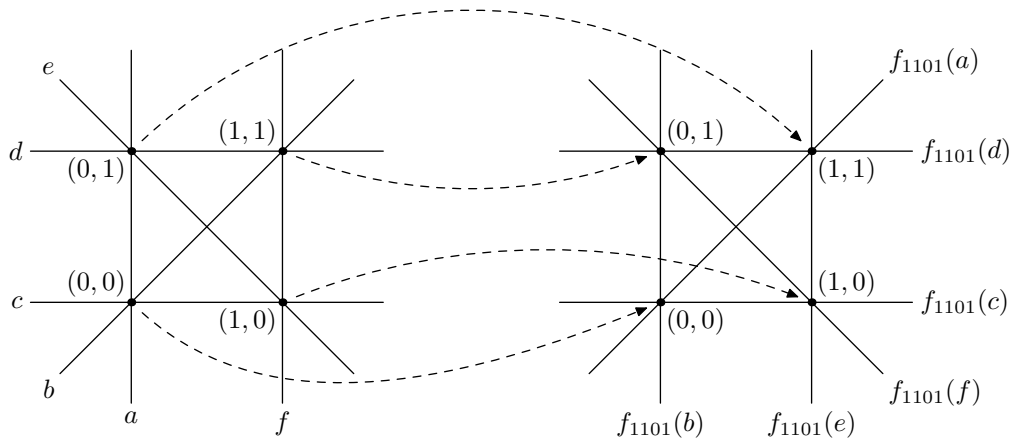


Figure: linear transformation $f_{1101} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$

(6) Consider the set $\mathbb{Z}_2^2 = \{(0,0), (0,1), (1,0), (1,1)\}$ of ordered pairs of residues modulo 2. For any 4 residues a, b, c, d consider a transformation $f_{abcd} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$ defined by the formula $f_{abcd}(x, y) = (ax + by, cx + dy)$. The set of invertible transformations of this form is a group.

General remarks. If the condition of the problem consists of a single statement, you have to prove this statement. If the problem looks like too difficult, try to solve the neighboring problems, they can contain hints.

Star-mining. A team gets a star for each correct ($\geq +$) written solution. Jury may also award stars for elegant solutions, for solutions of difficult problems and for (some) solutions written in $\text{T}_{\text{E}}\text{X}$. The jury has infinite number of stars. A team may present the solution orally paying 1 star for each attempt.

BEFORE. 1ST SERIES

1.1. (a) A combination lock can be opened by a 9-digit combination. It happens that if two combinations A and $B = b_1b_2 \dots b_9$ open the lock ($A = B$ is allowed), then the combination obtained from A by replacing its every digit k (simultaneously for all k) with the digit b_k opens the lock too. It is known that the lock can be opened by the combination 856291473 and the combinations obtained by (multiple) applying the above rule only. How many combinations open the lock?

(b) The same question for the following rule. If the combination A opens the lock and B is an arbitrary combination ($A = B$ is allowed), then the combination obtained from A by replacing (simultaneously for each k) the digit in the combination A that equals the number of the position of the digit k in combination B with b_k .

1.2. (a) Prove that the set in the example 6 is indeed a group.

(b) What groups in the examples above are cyclic?

(c) Every group contains the identity transformation. It is called *unity* and is denoted by e .

1.3. (a) Construct a group that contains two permutations a and b such that $ab = b^{-1}a$.

(b) The alphabet of Ababa tribe consists of two letters «a» and «b». No word change the sense if we insert or delete at any place in this word the fragments «aab» or «bba». 4 words of Ababa language are scratched on the rock. Prove that two of them have the same sense.

1.4. (a) Construct a group of 17 permutations numbered by numbers $0, 1, \dots, 16$, such that the number of composition of any two permutations equals the sum of the numbers of these permutations modulo 17.

(b) Construct a group of 16 permutations numbered by numbers $1, 2, \dots, 16$, such that the number of composition of any two permutations equals the product of the numbers of these permutations modulo 17.

(c) Does there exist a group of 8 permutations, that can be numbered by numbers 1, 2, 4, 7, 8, 11, 13, 14 so that the number of composition of any two permutations equals the product of the numbers of these permutations modulo 15?

1.5. Determine for the following values of n whether every group of n permutations is cyclic.

(7) 1,2,3,4,5,6,7; (8) 8; (9) 9; (10) 10; (12) 12; (15) 15; (21) 21; (1001) 1001.

Denote by $|X|$ the number of elements in the set X . The group G is called *commutative* if $xy = yx$ for each $x, y \in G$. The *order* of an element $a \in G$ is the minimal positive integer n such that $a^n = e$ (where e is the identity). If the order exists then it is denoted by $\text{ord } a$.

1.6. (a) *Fermat–Euler theorem*. If G is a commutative group, e is its unity, then $a^{|G|} = e$ for each $a \in G$.

(b) Every cyclic group is commutative.

(c) Is the opposite statement true?

1.7. If the number of elements of a group is prime then the group is cyclic.

1.8. (a) Find the order of each element in the group S_4 .

(b) The order is well-defined for each element of a finite group.

(c) If a group contains an element of order 2 then the number of elements in the group is even.

(d) If a group contains an element of order 3 then the number of elements in the group is divisible by 3.

(e) *Lagrange theorem*. The number of elements of a finite group is divisible by the order of every its element.

(f) If the number of elements in G is even then G contains an element of order 2.

1.9. (a) If $n > 2$ is even then there exists a noncyclic group of n permutations.

(b) If n is divisible by the square of a prime number then there exists a noncyclic group of n permutations.

1.10. (a) Each commutative group of 10 elements is cyclic.

(b) The same is true for each 21-element group.

(c) The same is true for each 1001-element group.

(d) For which n every commutative group of n elements is cyclic?

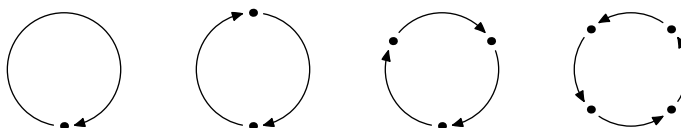


Figure: a permutation of type $\langle 1, 2, 3, 4 \rangle$

1.11. If a permutation of a $(n_1 + \dots + n_k)$ -element set is a composition of nonintersecting cycles of order $n_1, \dots, n_k$, we call it a permutation of type $\langle n_1, \dots, n_k \rangle$.

(a) Prove that any two permutations f and g of the same type are conjugate in the group S_n , that means that $g = b^{-1}fb$ for a suitable permutation $b \in S_n$.

(b) Prove the opposite statement.

(c) The conjugate permutations have the same orders.

1.12. Let G be a group of 15 elements.

(a) G contains an element of order 3.

* (b) Each element of order 5 in G can be conjugate with its powers only.

2. BEFORE. 2ND SERIES.

Solution of Problem 1.2. $f \in G \Rightarrow f^{-1} \in G \Rightarrow ff^{-1} = e \in G$.

Solution of Problem 1.5-7 for $n = 3$. Assume the converse: there is a noncyclic group G consisting of 3 permutations. Denote by a one of the permutations distinct from the identity. If $a^2 \neq e$ then the permutations a, a^2, a^3 are distinct and hence the group G is cyclic. If $a^2 = e$ then take a permutation $b \in G$ distinct from e and a . Then the permutation ab is distinct from e, a, b . (Indeed, obviously $ab \neq a$ and $ab \neq b$. If $ab = e$ then $b = a^2b = a$, a contradiction.) This contradiction proves the problem.

Solution of Problem 1.5-10. Answer: the group is not necessarily cyclic.

Consider a regular pentagon in the plane and all the isometries of the plane that map the pentagon onto itself. These motions are the identity, 4 rotations and 5 symmetries, 10 transformations at all. Consider permutations of the vertices of the pentagon under these transformations. These 10 permutations form a noncyclic group, and for any two symmetries s and t we have $st \neq ts$. That means that the group is noncyclic, because if $s = g^k$ and $t = g^l$ for some g , then $st = ts = g^{k+l}$.

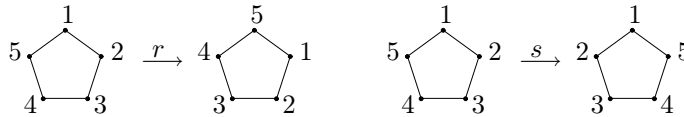


Figure: transformations of a regular 5-gon

Another solution of Problem 1.5-10. (It can be useful for solving Problem 2.1.) Let r be a rotation by $2\pi/5$ of the regular pentagon, s be a symmetry (see fig. 2). Then $r^5 = e = s^2$ and $sr = r^{-1}s$. Consider 10 transformations $r^k s^l$, $k = 0, 1, 2, 3, 4$ and $l = 0, 1$. Due to the relation $sr = r^{-1}s$ one can obtain that this set of transformations is a group. (This step is the main difference with the previous solution. We check that the set is a group algebraically but not geometrically. Therefore we can use the similar ideas when the objects have no geometrical interpretations.) The same relation allows to establish that the group is noncyclic.

- 2.1.** (a) There exists a noncyclic group of 21 elements.
 (b) There exists a noncyclic group of 55 elements.
 (c) If p and q are primes and $q - 1$ is divisible by p , then there exists a noncyclic group of pq elements.

Hint to the problem 2.1a. Choose the relations for elements r and s that provide the set $r^k s^l$, $k, l \in \mathbb{Z}$ to be a noncyclic group of 21 element, then construct the suitable permutations.

A *subgroup* of the group G is a subset of G that is a group itself.

- 2.2.** (a) Can a commutative group of 10 elements contain two elements of order 2? (This is a hint to the problem 1.10a.)
 (b) *Lagrange theorem.* The number of elements of a finite group is divisible by the number of elements of any its subgroup.

2.3. (Hint to the problem 1.12b.) Let G be a group of 15 elements and $f, g \in G$ be its elements of order 5.

- (a) The sets $\{f, f^2, f^3, f^4\}$ and $\{g, g^2, g^3, g^4\}$ either coincide or do not intersect.
 (b) One of the elements f, g is a power of the other.

2.4. Let G be a group of 15 elements, $f \in G$ be an element of order 5, $b \in G$, $b^{-1}fb = f^m$ and $k \in \mathbb{Z}$, $k > 0$. Then $b^{-1}f^k b = f^{km}$ and $b^{-k}fb^k = f^{m^k}$.

2.5. Let G be a group of 15 elements such that all its elements (except the unity) have order 3. Let $f, g \in G \setminus \{e\}$.

- (a) The sets $\{f, f^2\}$ and $\{g, g^2\}$ either coincide or do not intersect.
 (b) If $\{f, f^2\} \neq \{g, g^2\}$, then $fg \neq gf$.
 (c) Every $f \in G$, $f \neq e$, has exactly 4 conjugate elements.
 (d) This group does not exist.

2.6. (a) If the number of elements of G equals pq , where p and q are primes, $p < q$ and $q - 1$ is not divisible by p , then the group is cyclic.

(b) Let G be a group of 1001 elements and $f \in G \setminus \{e\}$ is an element that is conjugate with its powers only. Prove that G is cyclic.

3. BEFORE. SERIES 3

These funny problems in an abstract way describe the idea that was given in the hint to Problem 2.1a. Formally we do not need them for our main goal.

3.1. ¹ There are two letters in Cyclists' language: a and a^{-1} . They are called *opposite*.

A *Word* in Cyclists' and other considered languages is defined as an ordered collection of letters; in particular, there is an *empty* word – word with no letters (silence has a sense).

The word that consists of eight letters a is *indecent*. The word that consists of two opposite letters is named *stumble*.

In Cyclists' and other languages that we consider sense of a word does not change after

- inserting an indecent word or a stumble or
- deleting an indecent word or a stumble.

(Scientifically, sense is equivalence class of words with respect to inserting and deleting indecent words and stumbles operations.)

For example, words $aaaa^{-1}a$ and aaa are different but have the same sense.

(a) There are only 8 senses in Cyclists' language.

(b) Cyclists speak about residue classes modulo 8. In other words, the set of all senses with operation of concatenation is *isomorphic* to the set of all residue classes modulo 8 with sum operation.

Exact wording of this statement is as follows. We may concatenate words: X and Y gives XY . (For example, aa and $aa^{-1}a$ gives $aaaa^{-1}a$.) The operation of concatenation of words sets operation of concatenation of senses. So, there is a correspondence between residue classes to senses such that residue class of XY is the sum of residue classes of words X and Y .

3.2. In order to provide secrecy the Pentagon's workers created a language. There are four letters a, b, a^{-1} and b^{-1} . Letters a and a^{-1} are called *opposite*. Letters b and b^{-1} are opposite too. Five a letters or two b letters form an indecent word. ... is an indecent word too. It consists of 4 letters, first three letters are first three letters of $abab$ and last three letters of this word are last three letters of $a^{-1}bbab^{-1}$.

(a) The Pentagon's workers language has 10 senses.

(b) They speak about isometries of regular Pentagon. Give an exact wording of this statement.

3.3. Connoisseurs' of Perfection language has 4 letters a, b, a^{-1} and b^{-1} . Three a letters or two letters b form an indecent word. ... is an indecent word too. It has 10 letters and it is a concatenation of 5 copies of ba .

(a) Connoisseurs' of Perfection language has a finite number of senses.

(b) Connoisseurs of Perfection speak about a group. Give an exact wording of this statement.

3.4. (a) In Algebraists' language there are 4 letters a, b, a^{-1} and b^{-1} . We will not describe indecent words or even tell if there is a finite number of indecent words or not because they are indecent. Prove that algebraists speak about a group. Give an exact wording of this statement. (This group is able to be infinite even if there is a finite number of indecent words.)

(b) If we add 2 new letters c and c^{-1} to the Algebraists' language and some new indecent words, they will all the same speak about a group.

¹This is an example of an *ugly* mathematical problem. Understanding it's conditions is more difficult then solving it. However, this problem is necessary because it helps us to introduce an important construction.

4. AFTER. SERIES 4

Some Solutions.

1.8. (e) *The proof of the Lagrange Theorem.* For $x \in G$ consider the set $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$. These elements are different by definition of order. Thus this set has $\text{ord } f$ elements. If $xf^k = yf^l$ then $y = xf^{k-l}$. Thus for different x these sets either are equal or do not intersect. So $\text{ord } f$ divides $|G|$.

1.10. (a) Denote by p the order of a nonidentity element f . If $p = 10$ then the group is cyclic. Assume that $p < 10$. By Lagrange's Theorem $p \in \{5, 2\}$. If there exists an element g of order $10/p$ then $G = \{fg, (fg)^2, \dots, (fg)^{10}\}$. Else there is an element $g \notin \{f, f^2, \dots, f^p\}$ of order p . Then $\{f^k g^l\}_{k,l \in \mathbb{Z}}$ is a subgroup of order p^2 . Contradiction to Lagrange's Theorem.

1.11. *Hint.* Change the numeration of the elements of the set to transform f into g . The change of numeration determines the required permutation b .

2.3. (a) Suppose that the two given sets intersect. Then there are integers $1 \leq k, l \leq 4$ such that $f^k = g^l$. Since $\text{GCD}(k, 5) = 1$ it follows that there is an integer m such that $5 \mid km - 1$. Then $f = f^{km} = (f^k)^m = (g^l)^m = g^{lm}$. This implies that the two given sets are equal.

(b) Consider 25 elements $f^k g^l$, where $1 \leq k, l \leq 5$. Since the entire group has only 15 elements, it follows that there are $1 \leq k, l, m, n \leq 5$ such that $(k, l) \neq (m, n)$ and $f^k g^l = f^m g^n$. Multiplying by f^{-m} from the left and by g^{-l} from the right, we get $f^{k-m} = g^{n-l}$. Since f and g have order 5 it follows that the sets $\{f, f^2, f^3, f^4\}$ and $\{g, g^2, g^3, g^4\}$ intersect. Then by assertion (a) the sets coincide, and the problem follows.

2.5. (c) *Hint.* Take an element $f \neq e$. Let $c(f)$ be the number of elements conjugate to f (including the element f itself). Consider the set $Z(f) := \{g \in G : fg = gf\}$. By assertion (b) it follows that this set is $\{e, f, f^2\}$. Now apply the following general result: $c(f) \cdot |Z(f)| = |G|$. Thus $c(f) = 15/3 = 5$.

2.1. (a) *New hint.* This group is a group of some permutations of the (49-element) set $\mathbb{Z}_7^2$. In order to define this group let us represent such elements as pairs (x, y) of residue classes modulo 7. For non-negative integers k, l define a map

$$f_{k,l} : \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^2 \quad \text{by} \quad f_{k,l}(x, y) := (2^k x, lx + y).$$

Check that

- there are exactly 21 such maps;
- they form a group;
- this group is not cyclic.

2.1. (b) *Hint.* Observe that $2^5 = 33 - 1$. For nonnegative integers k, l define a map $f_{k,l} : \mathbb{Z}_{11}^2 \rightarrow \mathbb{Z}_{11}^2$ by $f_{k,l}(x, y) := (4^k x, lx + y)$.

3.3. *Hint.* Use that Connoisseurs of Perfection are Algebraists.

3.4. *Hint.* Map each sense to the transformation of the set of senses defined as «left concatenation».

New problems

4.1. There exists a noncyclic group of 39 elements.

4.2. Let G be a group with 1001 elements and $f \in G - \{e\}$. Suppose that f is conjugated only with its exponents. Let $g \notin \langle f \rangle := \{f, f^2, \dots, f^n, \dots\}$. Denote by q the smallest positive integer n such that $g^n \in \langle f \rangle$.

- (a) $\text{ord } g$ is divisible by q . (b) If $g^{-1}fg = f^k$ then $g^{-n}fg^n = f^{k^n}$.
(c) $g^{-1}fg = f$. (d) $\{fg, (fg)^2, (fg)^3, \dots, (fg)^{q^{\text{ord } f}}\}$ is a subgroup of G .

4.3. Let G be a noncyclic group of 1001 elements.

(a) Each element of G is contained in a subgroup maximal by inclusion and different from G .

Such subgroups are called *maximal*.

(b) Each maximal subgroup is cyclic.

4.4. The *commutativiser* of a group G is the set

$$Z = Z(G) := \{a \in G : ga = ag \text{ for any } g \in G\}$$

of elements that commute with all elements.

(We hope that the word “commutativiser” is more accessible for beginners than *center*.)

(a) Find $Z(S_n)$ for each $n = 2, 3, 4, \dots$

(b) The commutativiser is a subgroup.

4.5. Let G be a noncyclic group of 1001 elements. Assume that the generator of each maximal subgroup is conjugate not only to its powers.

(a) Every maximal subgroup contains the commutativiser.

(b) Find the number $a(F)$ of elements that are conjugate to some element of given maximal subgroup F , if $|F|$ and $|Z|$ are known.

5. AFTER. SERIES 5

Hint to the problem 1.4c. Try to choose a suitable subgroup in the group of permutations of the set $\{1, 2, 4, 7, 8, 11, 13, 14\}$.

5.1. (a) For any group G and an element $g \in G$ the set

$$N(g) = N_G(g) := \{a \in G : ga = ag^k \text{ for some } k\}$$

is a subgroup.

(b) Determine $N_{S_3}(g)$ for each $g \in S_3$.

(c) The number of subgroups conjugated to $\langle g \rangle$ equals $|G|/|N(g)|$.

A *generator* of a finite cyclic group G is any element g such that G consists of powers of g . (A generator needs not to be unique.)

5.2. Let G be a noncyclic group of 1001 elements. Assume that certain generator of each maximal subgroup is conjugated not with its powers only.

(a) The intersection of any two maximal subgroups is exactly the center of the group.

(b) The number of subgroups conjugated to maximal subgroup F equals $1001/|F|$.

(c) Denote by $\hat{F}$ the number of elements of G conjugate to elements of a maximal subgroup F and not contained in the commutativizer. Prove that $500 < \hat{F} \leq 1000 - |Z|$.

Primitive root theorem. For any prime p there exists a non negative integer g such that all the residues modulo p of $g^1, g^2, g^3, \dots, g^{p-1} \equiv 1$ are distinct.

5.3. *Proof of the theorem.* Let p be a prime and let a be a non negative integer that is not divisible by p .

(a) $p - 1$ is divisible by the minimal $k > 0$ for which $a^k \equiv 1 \pmod{p}$.

(b) for any two positive integers n and a the congruence $x^n \equiv a \pmod{p}$ has at most n solutions.

(c) If $p - 1$ is divisible by d , then the congruence $x^d \equiv 1 \pmod{p}$ has exactly d solutions.

(d) Prove the primitive root theorem for $p = 2^m + 1$.

(e) Prove the primitive root theorem for $p = 2^m \cdot 3^n + 1$.

(f) Prove the primitive root theorem for an *arbitrary* prime p .

(g)* Is it true that the number 3 is a primitive root modulo $p = 2^m + 1$?

5.4. For which n any group of n elements is commutative?

6. SOLUTIONS

1.8. (d) Let a be the element of order 3. Make a list of all the elements of the finite group. Let us cross out the elements from the list as follows. At each step, choose an element x which has not been crossed out yet, and cross out each of the 3 elements x , xa , and xa^2 . This procedure never leads to crossing out an element more than once. Indeed, assume that, say, xa has already been crossed out. This implies that for element y chosen before we have either $xa = y$, or $xa = ya$, or $xa = ya^2$. But then either $x = ya^2$, or $x = y$, or $x = ya$, respectively. Thus x must also have been crossed out before according to our rule, a contradiction. Thus exactly 3 elements are removed at each step. Since the group is finite, the process ends in a finite time. This implies that the number of elements in the list (and hence in the group) is divisible by 3.

1.12. *Hint.* See Problem 2.3.

2.1c. This group is a group of some permutations of the (q^2 -element) set $\mathbb{Z}_q^2$. In order to define this group let us represent such elements as pairs (x, y) of residue classes modulo q . By the primitive root theorem there exists an element $a \in \mathbb{Z}_q$ of order p . For nonnegative integers k, l define a map $f_{k,l} : \mathbb{Z}_q^2 \rightarrow \mathbb{Z}_q^2$ by $f_{k,l}(x, y) := (a^k x, lx + y)$. Check that

- there are exactly pq such maps;
- they form a group;
- this group is not cyclic.

3.1. *Hint.* Given a word, define the *number of its meaning* to be the difference between the quantities of letters a and a^{-1} in the word modulo 8.

3.2. *Hint.* The bijection between the meanings and isometries of the regular pentagon is constructed as follows. Assign to the letter a a counterclockwise rotation through 72° about the center of the pentagon. To the letter b assign a suitable reflection so that the relation $a \circ b \circ a \circ b^{-1} = id$ holds. Now interpret each word as the composition of the corresponding isometries.

3.3b. *First solution.* This follows from problem 3.4a.

3.3b. *Second solution.* Connoisseurs of Perfection talk about the group of those permutations of the vertices of a regular icosahedron which are obtained from the isometries of 3-space taking the icosahedron into itself. That is, about the group A_5 .

4.2. (b) This follows by induction over n .

5.3. *Hints.* (b) Let us prove the following more general statement: a polynomial of degree n cannot have more than n roots in $\mathbb{Z}_p$. Here by a polynomial we mean the collection of coefficients but not the function.

Assume that a polynomial $P(x)$ of degree n has in $\mathbb{Z}_p$ different roots $x_1, \dots, x_n, x_{n+1}$. Represent $P(x)$ as

$$P(x) = b_n(x - x_1) \dots (x - x_n) + b_{n-1}(x - x_1) \dots (x - x_{n-1}) + \dots + b_1(x - x_1) + b_0$$

('the Newton interpolation'). Put in the congruence $P(x) \equiv 0 \pmod{p}$ residues $x = x_1, \dots, x_n, x_{n+1}$ in this order. We obtain $b_0 \equiv b_1 \equiv \dots \equiv b_{n-1} \equiv b_n \equiv 0 \pmod{p}$.

The same solution can be presented in the following way. Let P be a polynomial. Then polynomial $P - P(a)$ is divisible by $x - a$, i.e. $P - P(a) = (x - a)Q$ for some polynomial Q such that $\deg Q < \deg P$. Since $P(a) = 0$, it follows that $P = (x - a)Q$ for some polynomial Q of degree less than $\deg P$. Now the required statement can be proved by induction over the degree of the polynomial P .

(c) Obviously, polynomial $x^{p-1} - 1$ in $\mathbb{Z}_p$ has exactly $p - 1$ roots and is divisible by $x^d - 1$. Prove that if a polynomial of degree a has a roots and is divisible by a polynomial of degree b , then the polynomial of degree b has exactly b roots.

(d) If there are no primitive roots, then by problem 2a the congruence $x^{2^{m-1}} \equiv 1 \pmod{p}$ has $p - 1 = 2^m > 2^{m-1}$ solutions.

(e),(f) Similarly to (d).

5.4. Hint. All groups of order n are abelian if and only if the prime decomposition of this number $n = p_1^{k_1} \dots p_l^{k_l}$ has the following properties:

- $k_i < 3$;
- p_i does not divide $p_j^{k_j} - 1$.

You can prove this by the same way, but in the case 1 you need the following fact: any finite abelian group is a direct product of cyclic subgroups.

The remaining problems are covered by the supplied paper [BKS].

References

- [A] V.I. Arnold, Ordinary differential equations, M, Nauka, 1984.
- [B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf
- [BKS] V. Bragin, Ant. Klyachko, A. Skopenkov, When any group of n elements is cyclic?
- [KS] L.A. Kaluzhnin, V.I. Sluschanskiy, Transformations and permutations. M.: 1979, 112 pages.
- [KM] M.I. Kargapolov, Yu.I. Merzlyakov, Foundations of group theory. M.: Nauka, 1982. <http://arhivknig.com/obrazovanie/87077-osnovy-teorii-grupp.html>
- [K] A.I. Kostrikin, Introduction to algebra. Foundations of algebra, 1994.

WHEN ANY GROUP OF N ELEMENTS IS CYCLIC? ¹

V. Bragin, Ant. Klyachko, and A. Skopenkov

We give a simple proof of the well-known fact: any group of n -elements is cyclic if and only if n and $\varphi(n)$ are coprime. This paper is accessible for high-school students because no knowledge of group theory is required. It could also be an interesting easy reading for mature mathematicians.

Introduction

We call a *group* a nonempty family G of transformations (i.e. permutations or rearrangements) of some set, which family is closed with respect to composition and taking inverse transformation (i.e. if $f, g \in G$, then $f \circ g \in G$ and $f^{-1} \in G$). Common term: transformation group. Cf. [A, comment to problem 5].

If a finite group G contains an element g such that G consists of all powers of g (i.e. $G = \{g, g^2, \dots, g^n, \dots\}$), then group G is called *cyclic*.

We prove the following theorem.

Theorem (folklore). *Any group consisting of n elements is cyclic if and only if n and $\varphi(n)$ are coprime.*

Here $\varphi(n)$ is the number of positive integers not exceeding n and coprime to n (the Euler function).

Note that n and $\varphi(n)$ are coprime if and only if in the prime decomposition $n = p_1 \dots p_k$

(*) all p_i are different and

(**) p_i does not divide $p_j - 1$ for any i and j .

The understanding of the proof requires no knowledge of group theory. A few necessary notions are introduced in the course of the proof. In particular, our arguments does not use the notion of a quotient group, as opposed to more traditional proofs (see, e.g., [B]). Our proof uses ideas similar to [???]. One can understand how to invent this proof from [BKKSS].

Proof of the “only if” part.

If condition (*) above is violated, e.g., $p_1 = p_2 = p$, then the following group consists of n elements and is not cyclic:

$$\left\{ (1, 2, \dots, p)^i (p+1, p+2, \dots, 2p)^j (2p+1, 2p+2, \dots, 2p + \frac{n}{p^2})^k \mid i, j = 1, \dots, p, k = 1, \dots, \frac{n}{p^2} \right\}.$$

If condition (**) above is violated, e.g., p_1 divides $p_2 - 1$, then by the primitive root theorem there is $a \in \mathbb{Z}_{p_2}^*$ for which the powers $a, a^2, \dots, a^{p_1} = 1$ are different. Denote by G_{p_1, p_2} the group of transformations $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$ defined by the formula $f_{k, l}(x, y) := (a^k x, lx + y)$ for $k \in \mathbb{Z}_{p_1}$ and $l \in \mathbb{Z}_{p_2}$. ² Then the following group is not cyclic (it is even nonabelian):

$$\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}. \quad QED$$

Proof of the “if” part.

We use the induction on the number of prime factors of $|G|$. If this order is prime, then the “if” part is implied by the following Lagrange Theorem.

The **order** $\text{ord } a$ of an element a of a group with the identity element e is the minimal positive integer n such that $a^n = e$. If the group is finite, it is clear that such n exists.

Lagrange Theorem (particular case). *The number of elements of any finite group is divisible by the order of any its element.*

Proof. Denote the group by G . For each $x \in G$ consider the set $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$. By the definition of order these elements are different. Therefore this set contains $\text{ord } f$ elements. If

¹See update version on www.arxiv.org. We would like to acknowledge K. Kohas for useful discussions.

²In more advanced notation $G_{p_1, p_2} := \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, l \in \mathbb{Z}_{p_2} \right\}$.

$xf^k = yf^l$, then $y = xf^{k-l}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by $\text{ord } f$. QED

Now suppose that the number of factors is greater than one. We need the following general version of the Lagrange Theorem.

A **subgroup** of a group G is a subset of G that is itself a group.

Lagrange Theorem. *The number of elements of any finite group is divisible by the number of elements of any subgroup.*

Proof. Denote the group by G and the subgroup by $\{h_1, h_2, \dots, h_m\}$. For each $x \in G$ consider the set $\{xh_1, xh_2, \dots, xh_m\}$. This set contains m elements. If $xh_k = yh_l$, then $y = xh_k h_l^{-1}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by m . QED

A **maximal subgroup** of a group is a maximal by inclusion subgroup not coinciding with G and containing more than one element. By the induction hypothesis and the Lagrange Theorem, *each maximal subgroup is cyclic.*

For an element f of a group G let $\langle f \rangle$ be the set of all powers of f (including zero and negative ones). The element f is called **generating** for the (cyclic) subgroup $\langle f \rangle$.

Suppose to the contrary that the group G is noncyclic. Then each element is contained in a maximal subgroup.

Elements f, g of a group G are **conjugate** in G if $g = b^{-1}fb$ for some $b \in G$.

First case: *generator f of some maximal subgroup is conjugate only to (some of) its powers.* Take $h \in G \setminus \langle f \rangle$. Then $h^{\text{ord } h} \in \langle f \rangle$. Let q be the minimal positive integer such that $h^q \in \langle f \rangle$. Take $k \in \mathbb{Z}$ such that $h^{-1}fh = f^k$. The inclusion $h^q \in \langle f \rangle$ implies $f = h^{-q}fh^q = f^{k^q}$ (here the last equality is proved by induction on q). Therefore $k^q \equiv 1 \pmod{\text{ord } f}$.

By condition (*) and the Lagrange Theorem $\text{ord } f$ is a product $p_1 \dots p_s$ of different primes. Then $k^q \equiv 1 \pmod{p_i}$ for any $i = 1, 2, \dots, s$. Since $|G|$ is divisible by $\text{ord } h$ and $\text{ord } h$ is divisible by q , by condition (*) we obtain that q is a product of different primes. By condition (**) none of these primes p_j divides none $p_i - 1$. Therefore q is coprime to each $p_i - 1$. Hence there exist integers $x = x_i$ and $y = y_i$ such that $qx + (p_i - 1)y = 1$. Therefore $k \equiv k^{qx + (p_i - 1)y} \equiv 1 \pmod{p_i}$ for any $i = 1, 2, \dots, s$. Hence $k \equiv 1 \pmod{\text{ord } f}$, i.e., $fh = hf$.

Then G contains a subgroup $\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$ of $q \text{ ord } f$ elements. Hence by condition (*) and the Lagrange Theorem $\text{ord } f$ is coprime to q . Since $(fh)^j = f^j h^j$ for each j , we obtain that $\text{ord}(fh)$ is divisible both by q and by $\text{ord } f$. $\text{ord}(fh) = q \text{ ord } f$. Thus $\text{ord}(fh) = q \text{ ord } f$. Since the subgroup $\langle f \rangle$ is maximal, we have $\langle fh \rangle = G$ and G is cyclic. Contradiction.

Second case: *generator of any maximal subgroup is conjugate not only to its powers.*

The **product of subsets X and Y** of a group G is the set of all products xy , where $x \in X$ and $y \in Y$. If one of these subsets consists of only one element, e.g., $Y = \{y\}$, then we write Xy instead of $X\{y\}$.

(1) *Any maximal subgroup F contains the **center***

$$Z = Z(G) := \{a \in G : ga = ag \text{ for any } g \in G\},$$

i.e., the set of elements commuting with each element of the group.

Proof of assertion (1). Otherwise FZ is a larger commutative subgroup. By the maximality of F we have $FZ = G$, which contradicts to the assumption of the second case. QED

(2) *The intersection of two maximal subgroups equals the center.*

Proof of assertion (2). A nontrivial element of the intersection commutes with all elements of both subgroups. Hence it commutes with any product of several multiples, each multiple being an element of one of our subgroups. The set of such products is a subgroup. By the maximality of our subgroups this subgroup coincides with the entire group. Therefore the intersection is contained in the center.

Assertion (1) implies the converse inclusion. QED

(3) The number of different subgroups conjugate to a maximal subgroup F (including F) is $|G|/|F|$.

Proof of assertion (3). Consider the set

$$N(F) := \{a \in G : Fa = aF\}.$$

It is easy to verify that $N(F)$ is a subgroup. By the assumption of the second case $N(F) \neq G$. Since $N(F) \supset F$, the maximality implies that $N(F) = F$.

The conjugation by each element of G takes F to a conjugate subgroup. If the conjugation by two different elements u and v takes the F to the same subgroup, i.e., $u^{-1}Fu = v^{-1}Fv$, then $Fuv^{-1} = uv^{-1}F$. This means that $uv^{-1} \in N(F) = F$ or, equivalently, $u \in Fv$. Conversely, the condition $u \in Fv$ implies $u^{-1}Fu = v^{-1}Fv$.

Clearly, $|Fv| = |F|$. Therefore the number of elements of G conjugation by which takes F to a given subgroup equals $|F|$. Therefore the number of different subgroups conjugate to F is precisely $|F|$ times less than $|G|$. QED

(4) Denote by $\widehat{F}$ the number of elements of G conjugate to elements of a maximal subgroup F and not contained in the center. Then $|G|/2 \leq \widehat{F} < |G| - |Z|$.

Proof of assertion (4). A subgroup conjugate to a maximal subgroup is also maximal. (Indeed, if $g^{-1}Fg \subset F' \subset G$, then $F \subset gF'g^{-1} \subset G$.)

$$\text{Therefore by (3) } \widehat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right).$$

The inequality $|G| > |F|$ implies $\widehat{F} < |G| - |Z|$.

By the assumption of the second case, $Z \neq F$. By (1) and the Lagrange theorem, $|Z|$ divides $|F|$. Therefore $\widehat{F} \geq |G|/2$.

Conclusion of the proof of the second case: calculations. Let $F_1, \dots, F_n$ be a maximal family of pairwise non-conjugate maximal subgroups. Recall that each element of the group is contained in some maximal subgroup. Hence the element is conjugate to some element in certain F_i . By this and (2) $|G| = |Z| + \sum_i \widehat{F}_i$. By the left inequality in (4), the number of summands is at most one. By the right inequality in (4), one summand also gives a contradiction. QED

References

- [A] V. I. Arnold, Ordinary Differential Equations, Springer, Berlin, 19??.
- [B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf
- [BKKSS] D. Baranov, A. Klyachko, K. Kohas, A. Skopenkov and M. Skopenkov, When are all groups of order n are cyclic? Materials of LKTG 2011, www.turgor.ru

Элементы математики в задачах:

через олимпиады и кружки — к профессии

Алгебра

А. Б. Скопенков

Геометрия и комбинаторика

Под редакцией А. А. Заславского и М. Б. Скопенкова

В книги вошли материалы занятий, проведенных в разное время в ряде российских университетов, школ и кружков. Большинство задач подобраны так, что в процессе их решения читатель (точнее, решатель) познакомится с глубокими идеями и освоит основы важных теорий. Книга может использоваться как школьниками и студентами для самостоятельных занятий, так и преподавателями.

К ключевым задачам приведены указания или решения.

Это обновляемая электронная версия. Ее пересечение с изданной книгой выложено в интернет с разрешения издательства.

Часть опубликованной версии книги:

<https://mccme.ru/~mskopenkov/skopenkov-pdf/sturm-2018.pdf>.

Оглавление

1	Введение	13
1.1	Зачем и для кого эта книга	13
1.2	Изучение путём решения и обсуждения задач	14
1.3	Исследовательские задачи для школьников	16
1.4	Как устроена книга	16
1.5	Важные соглашения	19
1.6	Основные обозначения	20
2	Делимость и деление с остатком	24
2.1	Делимость (1)	25
2.2	Простые числа (1)	28
2.3	НОД и НОК (1)	31
2.4	Деление с остатком и сравнения (1)	34
2.5	Линейные диофантовы уравнения (2)	36
2.6	Каноническое разложение (2*)	39
2.7	Целые точки под прямой (2*)	42
3	Умножение по простому модулю	47
3.1	Малая теорема Ферма (2)	47
3.2	Проверка простоты (3*). <i>С. В. Конягин</i>	49
3.3	Квадратичные вычеты (2*)	52
3.4	Квадратичный закон взаимности (3*)	55
3.5	Первообразные корни (3*)	59
3.6	Высокие степени (3*). <i>А. Я. Канель-Белов, А. Б. Скопенков</i>	61
4	Многочлены и комплексные числа	66
4.1	Рациональные и иррациональные числа (1-2)	67
4.2	Решение уравнений 3-й и 4-й степени (2)	70

4.3	Теорема Безу и её следствия (2)	76
4.4	Делимость для многочленов (3*). <i>А. Я. Канель-Белов, А. Б. Скопенков</i>	80
4.5	Применения комплексных чисел (3*)	83
4.6	Теорема Виета и симметрические многочлены (3*)	87
4.7	Диофантовы уравнения и гауссовы числа (4*). <i>А. Я. Канель-Белов</i>	89
4.8	Диагонали правильных многоугольников (4*). <i>И. Н. Шнурников</i>	93
5	Перестановки	98
5.1	Порядок, тип, сопряжённость (1)	98
5.2	Чётность перестановки (1)	101
5.3	Комбинаторика классов эквивалентности (2)	104
6	Неравенства	110
6.1	В направлении неравенства Йенсена (2)	110
6.2	Некоторые основные неравенства (2)	115
6.3	Применения основных неравенств (3*). <i>М. А. Берштейн</i>	118
6.4	Геометрическая интерпретация (3*)	126
7	Последовательности и пределы	131
7.1	Конечные суммы и разности (3)	131
7.2	Линейные рекурренты (3)	134
7.3	Конкретная теория пределов (4*)	137
7.4	Как компьютер вычисляет корень? (4*) <i>А. С. Воронцов, А. И. Сгибнев</i>	140
7.5	Методы суммирования рядов (4*)	143
7.6	Примеры трансцендентных чисел	147
7.6.1	Введение (1)	147
7.6.2	Задачи (3*)	149
7.6.3	Доказательство теоремы Лиувилля (2)	150
7.6.4	Простое доказательство теоремы Малера (3*)	151
8	Функции	157
8.1	График и количество корней кубического многочлена	157

	8.1.1	Введение	157
	8.1.2	Задачи	158
	8.1.3	Формулировки основных результатов	160
	8.1.4	Доказательства	162
	8.2	Элементы анализа для многочленов (2)	167
	8.3	Число корней многочлена (3*)	169
	8.4	Оценки и неравенства (4*). <i>В. А. Сендеров</i> . . .	173
	8.5	Применения компактности (4*). <i>А. Я. Канель-Белов</i>	175
9		К алгоритмам решения алгебраических уравнений . .	182
	9.1	Введение и формулировки результатов	182
	9.1.1	О чём этот параграф	182
	9.1.2	Построимость (1)	184
	9.1.3	Неразрешимость в вещественных ра- дикалах (2)	186
	9.1.4	Неразрешимость в комплексных ра- дикалах (2)	189
	9.1.5	Чем интересны приводимые доказа- тельства	191
	9.1.6	Исторические комментарии	193
	9.1.7	Связь с построениями циркулем и ли- нейкой (1)	194
	9.2	Решаем уравнения: метод резольвент Лагранжа	196
	9.2.1	Определение радикальности многочле- на (2)	196
	9.2.2	Решение уравнений малых степеней (2)	199
	9.2.3	Переформулировка теоремы Гаусса (2)	205
	9.2.4	Идея доказательства построимости в тео- реме Гаусса (2)	206
	9.2.5	Доказательство построимости в тео- реме Гаусса (3)	209
	9.2.6	Эффективные доказательства постро- имости (4*)	210
	9.3	Задачи о неразрешимости в радикалах	219
	9.3.1	Одно извлечение квадратного корня (1-2)	219

9.3.2	Несколько извлечений квадратных корней (3^*)	225
9.3.3	Одно извлечение корня третьей степени (2)	230
9.3.4	Одно извлечение корня простой степени (3^*)	234
9.3.5	Неразрешимость «в вещественных многочленах» (2)	240
9.3.6	Неразрешимость «в многочленах» (3)	242
9.3.7	Единственность способа решения квадратного уравнения (2)	244
9.3.8	Неразрешимость «в комплексных числах» (4^*)	246
9.3.9	Выразимость с данным числом радикалов (4^*)	246
9.4	Доказательства неразрешимости в радикалах	249
9.4.1	Поля и их расширения (2)	249
9.4.2	Неразрешимость «в вещественных многочленах» (3)	250
9.4.3	Неразрешимость «в многочленах» (3)	251
9.4.4	Непостроимость в теореме Гаусса (3^*)	252
9.4.5	Неразрешимость «в вещественных числах» (3^*)	254
9.4.6	Неразрешимость «в числах» (4^*)	255
9.4.7	Теорема Кронекера о неразрешимости (4^*)	256
9.4.8	Вещественный аналог теоремы Кронекера (4^*)	260
10	Группы. <i>В. А. Брагин, А. А. Клячко, А. Б. Скопенков</i>	265
10.1	Зачем, для кого и как устроен этот параграф	265
10.2	Как придумать	267
10.2.1	Постановка задачи (2)	267
10.2.2	Примеры групп (2)	268
10.2.3	Докажем и применим теорему Лагранжа (2)	270
10.2.4	Применим сопряжение (3)	272

10.3	Итог: формулировка и доказательство	279
10.3.1	Формулировка основного результата (2)	279
10.3.2	Доказательство части «только тогда» (3*)	279
10.3.3	Доказательство части «тогда» (4*)	280
11	О преподавании	286
11.1	Олимпиады и математика	286
11.2	Начинать с языка или содержания?	287
11.3	О необходимости мотивировок	290
11.3.1	«За» и «против» мотивировок	291
11.3.2	О мотивировках теории Галуа	293
11.3.3	Почему не принимается мотивированное изложение?	294
11.4	Кружки и олимпиады как путь в математику и как спорт. <i>А. Я. Канель-Белов, А. И. Буфетов</i>	304
11.4.1	Введение	304
11.4.2	Спортивный подход	304
11.4.3	Олимпиада как путь в математику	306

Оглавление

1	Геометрия	330
12	Треугольник	330
12.1	Принцип Карно (1). <i>В. Ю. Протасов, А. А. Гаврилюк</i>	331
12.2	Центр вписанной окружности (2). <i>В. Ю. Протасов</i>	333
12.3	Прямая Эйлера (2). <i>В. Ю. Протасов</i>	337
12.4	Формула Карно (2*). <i>А. Д. Блинков</i>	338
12.5	Ортоцентр, ортотреугольник и окружность девяти точек (2). <i>В. Ю. Протасов</i>	343
12.6	Несколько неравенств, связанных с треугольником (3*). <i>В. Ю. Протасов</i>	345
12.7	Биссектрисы, высоты и описанная окружность (2). <i>П. А. Кожевников</i>	348
12.8	«Полувписанная» окружность (3*). <i>П. А. Кожевников</i>	353
12.9	Обобщённая теорема Наполеона (2*). <i>П. А. Кожевников</i>	360
12.10	Изогональное сопряжение и прямая Симсона (3*). <i>А. В. Акопян</i>	367
13	Окружность	379
13.1	Простейшие свойства окружности (1). <i>А. Д. Блинков</i>	379
13.2	Вписанный угол (1). <i>А. Д. Блинков, Д. А. Пермяков</i>	384

13.3	Вписанные и описанные окружности (2). <i>А. А. Гаврилюк</i>	389
13.4	Радикальная ось (2). <i>И. Н. Шнурников, А. И. Засорин</i>	391
13.5	Касание (2). <i>И. Н. Шнурников, А. Засорин</i>	392
13.6	Теоремы Птолемея и Кези (3*). <i>А. Д. Блинков, А. А. Заславский</i>	394
13.6.1	Теорема Птолемея	394
13.6.2	Теорема Кези	395
14	Геометрические преобразования	402
14.1	Применения движений. (1) <i>А. Д. Блинков</i>	402
14.2	Классификация движений плоскости (2). <i>А. Б. Скопенков</i>	410
14.3	Классификация движений пространства (3*). <i>А. Б. Скопенков</i>	412
14.4	Применение подобия и гомотетии (1). <i>А. Д. Блинков</i>	414
14.5	Поворотная гомотетия (2). <i>П. А. Кожевников</i>	422
14.5.1	Вводные задачи: немного о велосипедистах	422
14.5.2	Основные задачи	423
14.5.3	Дополнительные задачи	424
14.6	Подобие (1). <i>А. Б. Скопенков</i>	429
14.7	Сжатие к прямой (2). <i>А. Я. Канель-Белов</i>	430
14.8	Параллельная проекция и аффинные преобразования (2). <i>А. Б. Скопенков</i>	432
14.9	Центральная проекция и проективные преобразования (3). <i>А. Б. Скопенков</i>	435
14.10	Инверсия (2). <i>А. Б. Скопенков</i>	438
15	Аффинная и проективная геометрия	445
15.1	Буря на Массовом поле (2). <i>А. А. Гаврилюк</i>	446
15.2	Двойные отношения (2). <i>А. А. Гаврилюк</i>	449
15.3	Полярное соответствие (2). <i>А. А. Гаврилюк, П. А. Кожевников</i>	454
16	Комплексные числа и геометрия (3). <i>А. А. Заславский</i>	462
16.1	Комплексные числа и элементарная геометрия.	463

16.2	Комплексные числа и круговые преобразования.	466
17	Построения и геометрические	
	места точек	470
17.1	Геометрические места точек (1). <i>А. Д. Блинков</i>	470
17.2	Задачи на построение и ГМТ, связанные с площадями (1). <i>А. Д. Блинков</i>	478
17.3	Построения. Ящик инструментов (2). <i>А. А. Гаврилюк</i>	484
17.4	Дополнительные построения (2*). <i>И. Н. Шнурников</i>	487
18	Стереометрия	496
18.1	Задачи на пространственное воображение	
	<i>М. А. Корчемкина, И. А. Пушкарёв</i>	496
18.1.1	Фигуры из кубиков	496
18.1.2	Траектории	497
18.1.3	Рисование	498
18.2	Рисование. <i>А. Б. Скопенков</i> (1-2)	499
18.3	Правильные многогранники (3)	502
18.3.1	Вписанные и описанные. <i>А. Я. Канель-Белов</i>	502
18.3.2	Самосовмещения. <i>А. Б. Скопенков</i>	505
18.4	Многомерье (4*). <i>А. Я. Канель-Белов</i>	507
18.4.1	Простейшие многогранники в многомерном пространстве. <i>Ю. М. Бурман, А. Я. Канель-Белов</i>	507
18.4.2	Многомерные объёмы	511
18.4.3	Объёмы и сечения	513
18.4.4	Две задачи для исследования	514
18.4.5	Разбиение на части меньшего диаметра. <i>А. М. Райгородский</i>	515
19	Разные задачи по геометрии	525
19.1	Геометрические задачи на экстремальные значения (2). <i>А. Д. Блинков</i>	525
19.2	Площади (2). <i>А. Д. Блинков</i>	532
19.3	Конические сечения (3*). <i>А. В. Акопян</i>	541

19.4	Криволинейные треугольники и неевклидова геометрия (3*). <i>М. Б. Скопенков</i>	552
2	Комбинаторика	559
20	Подсчеты в комбинаторике	559
20.1	Подсчеты числа способов (1). <i>А. А. Гаврилюк, Д. А. Пермяков</i>	559
20.2	Наборы подмножеств (2). <i>Д. А. Пермяков</i> . . .	563
20.3	Формула включений и исключений (2). <i>Д. А. Пермяков</i>	566
21	Конечные множества	575
21.1	Принцип Дирихле (1). <i>А. Я. Канель-Белов</i> . . .	575
21.2	Правило крайнего (2). <i>А. Я. Канель-Белов</i> . . .	579
21.3	Цикличность I (2) ¹ . <i>А. Я. Канель-Белов</i>	581
21.4	Цикличность II (2). <i>П. А. Кожевников</i>	585
21.5	Конечное и счётное (2). <i>П. А. Кожевников</i> . . .	588
22	Графы. <i>Д. А. Пермяков, А. Б. Скопенков</i>	596
22.1	Графы под шубой (2)	596
22.2	Подсчёты в графах (2)	602
22.3	Пути в графах (2)	605
23	Конструкции и инварианты	608
23.1	Конструкции ² (1). <i>А. В. Шаповалов</i>	609
23.2	Инварианты I (1). <i>А. Я. Канель-Белов</i>	623
23.3	Инварианты II (1) ³ . <i>А. В. Шаповалов</i>	627
23.4	Раскраски	637
23.4.1	Замощения (1). <i>А. Я. Канель-Белов</i> . . .	637
23.4.2	Таблицы (2) ⁴ . <i>Д. А. Пермяков</i>	638
23.5	Полуинварианты ⁵ (1). <i>А. В. Шаповалов</i>	639
24	Алгоритмы	650
24.1	Игры (1) ⁶ . <i>Д. А. Пермяков, М. Б. Скопенков, А. В. Шаповалов</i>	650
24.2	Информационные задачи (2). <i>А. Я. Канель-Белов</i>	664
24.3	Коды, исправляющие ошибки (2). <i>М. Б. Скопенков</i>	667
24.4	Булев куб (2). <i>А. Б. Скопенков</i>	670

24.5	Выразимость для функций алгебры логики. <i>А. Б. Скопенков</i>	675
24.5.1	Примеры и определения (1)	675
24.5.2	Теорема Поста (2*)	677
24.6	Сложность суммирования ⁷ . <i>Ю. Г. Кудряшов, А. Б. Скопенков</i>	681
24.6.1	Вводные задачи (2)	681
24.6.2	Определения и примеры (3*)	682
24.6.3	Асимптотические оценки (4*)	684
25	Вероятность ⁸	693
25.1	Классическое определение вероятности (1). <i>А. А. Заславский, А. Б. Скопенков</i>	694
25.2	Более общее определение вероятности (1). <i>А. А. Заславский, А. Б. Скопенков</i>	697
25.3	Условная вероятность (1). <i>А. А. Заславский, А. Б. Скопенков</i>	701
25.4	Математическое ожидание (3). <i>А. А. Заславский, А. Б. Скопенков</i>	707
25.5	Дисперсия и ее применения (3). <i>А. А. Заславский, А. Б. Скопенков</i>	714
25.6	Случайные блуждания и электрические цепи ⁹ (3). <i>А. А. Заславский, М. Б. Скопенков, А. В. Устинов</i>	716
26	Комбинаторная геометрия	746
26.1	О ковровых дорожках и салфетках (2). <i>П. А. Кожевников</i>	746
26.2	Теорема Хелли (2). <i>А. В. Акопян</i>	753
26.3	Многоугольники на клетчатой бумаге (2). <i>В. В. Прасолов, М. Б. Скопенков</i>	756
26.4	Принцип Дирихле на прямой (3). <i>А. Я. Канель-Белов</i>	775
26.5	Принцип Дирихле и его применения в геометрии ¹⁰ (3). <i>И. В. Аржанцев</i>	776
26.6	Фазовые пространства (3). <i>А. Я. Канель-Белов</i>	784
26.7	Линейное варьирование (3). <i>А. Я. Канель-Белов</i>	786

- 26.8 Собери квадрат (3^*). *М. Б. Скопенков, О. А. Малиновская, С. А. Дориченко, Ф. А. Шаров* . . . 789
- 26.9 Можно ли из тетраэдра сделать куб?¹¹ (3). *М. В. Прасолов, М. Б. Скопенков* 806

1 Введение

1.1 Зачем и для кого эта книга

Глубокое понимание математики полезно и математику, и профессионалу в наукоёмкой отрасли. В частности, «профессия» в названии этой книги не обязательно означает профессию математика.

Эта книга предназначена для старшеклассников и младшекурсников (в частности, ориентированных на олимпиады). См. подробнее п. 11.1 «Олимпиады и математика». Книгу можно использовать как для самостоятельных занятий, так и для преподавания.

В этой книге мы пытаемся построить мост (путем указания на отсутствие пропасти) между обычными школьными задачами и более сложными абстрактными математическими понятиями. Наша основная цель — помочь широкой аудитории читателей научиться применять математические методы для решения проблем, мотивированных «реальным миром или реальной работой» [Meu], и овладеть инструментами и способами мышления, которые будут полезны за пределами школы в самых разных дисциплинах.

Книга содержит наиболее стандартный «базовый» материал (впрочем, частично, скорее, для повторения, чем для первоначального изучения). Основное содержание книги составляет более сложный материал. Некоторые темы малоизвестны в традиции математических кружков, но полезны как для математического образования, так и для подготовки к олимпиадам.

Книга основана на занятиях, проведённых авторами и редакторами в разное время на математическом факультете Высшей школы экономики, в Независимом московском университете, в школах им. А. Н. Колмогорова (СУНЦ МГУ), «Интеллектуал» и № 1543 г. Москвы, летней школе «Современная математика», в Кировской и Костромской летних математических школах, в Московской выездной олимпиадной школе, в кружках «Математический семинар» и «Олимпиады и математика», на летней конференции Турнира городов, при подготовке команды России к международной математической олимпиаде, в системе дистанционного обучения математике МИОО.

Книга доступна уже старшеклассникам, интересующимся мате-

матикой¹. Приводятся почти все определения, не входящие в школьную программу. Если где-то нужны дополнительные сведения, то приводятся ссылки.

При этом многие темы трудны, если изучать их «с нуля». Однако *последовательность изложения* помогает преодолевать трудности. В то же время многие темы *независимы* друг от друга. См. подробнее п. 1.4 «Как устроена книга».

1.2 Изучение путём решения и обсуждения задач

Мы следуем традиции изучения материала в виде решения и обсуждения задач. Эти задачи подобраны так, что в процессе их решения читатель (точнее, решатель) освоит основы важных теорий — как классических, так и современных. Основные идеи демонстрируются по одной и на «олимпиадных» примерах, т. е. на простейших частных случаях, свободных от технических деталей. Этим мы показываем, *как можно придумать* эти теории. См. подробнее п. 11.1 «Олимпиады и математика».

Обучение путём решения задач не только характерно для серьёзного изучения математики, но и продолжает древнюю культурную традицию. Например, послушники дзенских монастырей обучаются, размышляя над загадками, данными им наставниками. Впрочем, эти загадки являются скорее парадоксами, а не задачами. См. подробнее [Su]; ср. [Pl, с. 26–33]. А вот некоторые «математические» примеры: [Ar01, BS, GDI, GIF, KK08, Pr07-1, PoSe, SCY, Sk09, Sk19, SZ, Vag, Zv]; кое-где не только приведены задачи, но и изложены *принципы отбора* удачных задач. Об американской традиции см. [IBL, Meu, RMP].

Учиться, решая задачи, трудно. В частности, потому, что такое обучение обычно не создаёт *иллюзию* понимания. Однако усилия сполна вознаграждаются глубоким пониманием материала — в первую очередь, умением проводить аналогичные (и даже не очень

¹Часть материала в некоторых кружках и летних школах изучается теми, кто только знакомится с математикой (например, 6-классниками). Однако приводимое изложение рассчитано на читателя, уже имеющего хотя бы минимальную математическую культуру. Заниматься с 6-классниками нужно по-другому, см., например, [GIF].

аналогичные) рассуждения. Кое-где вслед за великими математиками в процессе изучения интересных задач читатель увидит, как естественно возникают важные понятия и теории. Надеемся, это поможет ему совершить собственные настолько же полезные открытия (не обязательно в математике)!

Для решения задач достаточно понимания их условий. Другие знания и теории не нужны. (Впрочем, такие знания и теории как раз появляются при решении подобранных задач.) Но может потребоваться владение другими частями книги, что отражено в подсказках и указаниях.

К важнейшим задачам приводятся подсказки, указания, решения и ответы. Они расположены в конце каждого пункта. Однако к ним стоит обращаться после прорешивания каждой задачи.

Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то её утверждение важное.

Как правило, мы приводим *формулировку* красивого или важного утверждения (в виде задачи) перед его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться следующие задачи. Это всегда явно оговаривается в подсказках, а иногда и прямо в тексте. Поэтому если некоторая задача не получается, то читайте дальше. (На занятии задача-подсказка выдаётся только тогда, когда ученик немного подумал над самой задачей.) Такой процесс обучения полезен, поскольку моделирует реальную исследовательскую ситуацию. См. подробнее п. 11.3 «О необходимости мотивировок».

Всё это — попытка продемонстрировать занятие в виде *диалога*, основанного на решении и обсуждении задач. Подробнее см. [КК15].

Напутствие. А. Я. Канель-Белов

Для успешного решения задач математических олимпиад высшего уровня необходимы в первую очередь общеукрепляющие средства: хорошая проработка алгебры (культура алгебраических преобразований), проработка школьной геометрии. Задачи этих олимпиад (кроме первых задач) практически всегда предполагают смешанный сценарий решения; редки задачи на применение некоторого метода или идеи в чистом виде. Решению таких «смешанных» задач

должна предшествовать работа с ключевыми задачами, в которых идеи работают в чистом виде.

Умение преобразовывать алгебраические выражения — одно из базовых. Его недостает «олимпиадникам», из-за его отсутствия часто возникают нелепые и обидные ошибки. Поэтому для успешного решения задач алгебраического, теоретико-числового и комбинаторного типа рекомендуем нарабатывать культуру арифметических выкладок.

1.3 Исследовательские задачи для школьников

Многим талантливым школьникам и студентам интересно решать исследовательские задачи. Они часто предлагаются в форме сложных задач, разбитых на шаги, см. [LKTG]. Возможно, конечный результат даже неизвестен заранее, а естественно появляется в процессе работы. Это одна из форм развития творческих способностей, близкая к научной деятельности, которая для многих учеников может оказаться наиболее удачной. Кроме того, обычно ученику интереснее изучать теорию в том случае, когда он сразу же применяет ее к конкретным задачам. Поэтому интерес к исследовательским задачам полезно поддерживать и развивать. Надеемся, настоящая книга поможет это делать.

Многие из приведённых задач — хорошие темы для исследовательских работ старшеклассников и младшекурсников, связанных с алгеброй, комбинаторикой и информатикой. С их решениями можно выступать на конференциях. Описание удачных примеров этой деятельности читатель может найти в материалах Московской математической конференции школьников [М]. Хотя большинство этих задач не претендуют на научную новизну, возможно их развитие в сторону новых результатов.

1.4 Как устроена книга

Книгу не обязательно изучать подряд. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана. Для занятия кружка можно использовать любой пункт (или подпункт) книги.

Книга разбита на главы, параграфы и пункты (некоторые пункты разбиты на подпункты). Структура параграфов приблизительно описана в их начале. Если в задаче используется материал другого пункта, то можно либо игнорировать эту задачу, либо посмотреть то место, на которое приводится ссылка. Это даёт большую свободу читателю при изучении книги, но одновременно может требовать его внимательности.

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них можно начать изучение параграфа. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга. При изучении полезно *возвращаться* к пройденному материалу, но на новом уровне. Поэтому разные пункты одного параграфа можно изучать *не подряд*, а с перерывами на другие темы.

Обозначения, используемые во всей книге, приведены в конце введения. Понятия и обозначения, используемые в некоторой главе, вводятся в начале главы. В конце книги есть предметный указатель. Жирным шрифтом выделены номера страниц, на которых приводятся *формальные определения* понятий.

Параграф 11 составлен из заметок об общих принципах преподавания, адресованных прежде всего учителям. Возможно, заметки окажутся полезными и ученикам.

Обновляемая электронная версия части книги, пересечение которой с изданной книгой выложено в интернет с разрешения издательства: <http://www.mcsme.ru/circles/oim/materials/sturm.pdf>.

О литературе и источниках

В конце каждого параграфа приводится литература, относящаяся ко всему параграфу, и отдельно литература по каждому пункту. Ссылки на книги [GDI, GKP, ZSS, Sk19, SZ], относящиеся ко многим параграфам, приведены в этом параграфе. Мы старались указать не только литературу, использованную при подготовке кон-

кретного материала, но также и жемчужины научно-популярного жанра на изучаемые темы. Мы надеемся, что наш список литературы, хотя бы в первом приближении, сможет стать путеводителем в море научно-популярной литературы по математике. Однако в него наверняка не вошли многие замечательные материалы, ввиду необъятности их количества. Важно, что обращение к литературе не нужно для решения задач, если явно не указано обратное.

Многие задачи не оригинальны, но первоисточник (даже если его можно установить) обычно не указывается. Ссылка после условия задачи указывает источник, из которого взята задача. Эти ссылки приведены для того, чтобы читатель смог сравнить своё решение с приведённым там. Если мы знали, что пересечение какого-то пункта с каким-то источником велико, то упоминали об этом.

Мы не даём ссылок на интернет-версии статей в журналах «Квант» и «Математическое Просвещение», их можно найти на сайтах

<http://kvant.ras.ru>, <http://kvant.mccme.ru>,
<http://www.mccme.ru/free-books/matpros.html>.

Благодарности и сведения о редакторах

Мы благодарим за серьёзную работу авторов материалов. Благодарим за полезные замечания рецензентов книги Е. А. Авксентьева, А. В. Антропова, Е. В. Бакаева, В. Н. Дубровского, К. А. Кнопа, Д. В. Мусатова, Л. Э. Медникова, А. А. Полянского, А. И. Сгибнева, С. Л. Табачникова, А. И. Храброва, Г. И. Шарыгина, и Д. Э. Шноля, а также анонимных рецензентов отдельных материалов. Благодарим А. Я. Канеля-Белова и А. В. Шаповалова (<http://www.ashap.info>), авторов большого количества материалов, высказавших также ряд полезных идей и замечаний. Благодарим Д. А. Пермякова, редактора книги [ZPS]. Благодарим учеников за каверзные вопросы и указания на неточности. Благодарим Е. С. Горскую и П. В. Широкова за подготовку многих рисунков. Благодарности по отдельным материалам приводятся прямо в них.

Мы приносим извинения за допущенные неточности и будем благодарны читателям за указания на них.

Главы 1 «Геометрия» и 2 «Комбинаторика» редактировали А. А. Заславский и М. Б. Скопенков соответственно. Мы организовали ре-

цензирование материалов параграфа 11, но редактировали их сами авторы.

А. Б. Скопенков и М. Б. Скопенков частично поддержаны грантами фонда Саймонса и фонда «Династия».

Места работы и интернет-страницы.

А. А. Заславский: ЦЭМИ РАН, школа 1543.

А. Б. Скопенков: Московский физико-технический институт (ГУ) и Независимый московский университет, www.mscme.ru/~skopenko.

М. Б. Скопенков: Национальный исследовательский университет Высшая школа экономики (факультет математики) и Институт проблем передачи информации РАН, www.mscme.ru/~mskopenkov.

1.5 Важные соглашения

Пункты внутри каждого параграфа расположены примерно в порядке возрастания сложности материала. Цифры в скобках после названия пункта означают его «относительный уровень»: 1 — самый простой, 4 — самый сложный. Первые пункты (не отмеченные звёздочкой) являются базовыми; если не указано противное, с них можно начать изучение главы. А к остальным пунктам (отмеченным звёздочкой) можно возвращаться потом; если не указано противное, то они независимы друг от друга.

Номера задач обозначаются жирным шрифтом. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. *Загадкой* называется не сформулированный чётко вопрос; здесь нужно придумать и чёткую формулировку, и доказательство, ср. [VIN]. В задачах, отмеченных кружочком $\circ$, требуется привести только ответ без доказательства. Наиболее трудные задачи отмечены звёздочкой $*$. Если в условии задачи написано «найдите», то нужно дать ответ без знака суммы и многоточия. *Указание и решение* к задаче может опираться на *подсказку* к ней. Если некоторая задача не получается, то читайте дальше — следующие задачи могут оказаться подсказками.

1.6 Основные обозначения

- $[x] = [x]$ — (нижняя) целая часть числа x («пол»), т. е. наибольшее целое число, не превосходящее x .
- $\lceil x \rceil$ — верхняя целая часть числа x («потолок»), т. е. наименьшее целое число, не меньшее x .
- $\{x\}$ — дробная часть числа x .
- $d \mid n$, или $n : d$ — число n делится на число d , т. е. $d \neq 0$ и существует такое целое k , что $n = kd$ (число d называется *делителем* числа n).
- $\mathbb{R}, \mathbb{Q}, \mathbb{Z}$ — множества всех действительных, рациональных и целых чисел соответственно.
- $\mathbb{Z}_2$ — множество $\{0, 1\}$ остатков от деления на 2 с операциями сложения и умножения по модулю 2.
- $\mathbb{Z}_m$ — множество $\{0, 1, \dots, m-1\}$ остатков от деления на m с операциями сложения и умножения по модулю m . (Специалисты по алгебре чаще обозначают это множество $\mathbb{Z}/m\mathbb{Z}$, а через $\mathbb{Z}_m$ обозначают множество *целых m -адических чисел* для простого m .)
- $\binom{n}{k}$ — количество k -элементных подмножеств n -элементного множества (другое обозначение: C_n^k).
- $|X|$ — число элементов во множестве X .
- $A - B = \{x \mid x \in A \text{ и } x \notin B\}$ — разность множеств A и B .
- $A \sqcup B$ — дизъюнктное объединение множеств A и B , т. е. объединение $A \cup B$ непересекающихся множеств A и B .
- $A \subset B$ — «множество A содержится в множестве B ». (В некоторых других книгах это обозначают $A \subseteq B$, а $A \subset B$ означает «множество A содержится в множестве B и не равно B ».)
- Фраза «обозначим $x = a$ » сокращается до $x := a$.
- id — отображение множества в себя, переводящее каждый элемент в себя (тождественное).

Литература

- [GDI] *Глибичук А. А., Дайняк А. Б., Ильинский Д. Г., Кунавский А. Б., Райгородский А. М., Скопенков А. Б., Чернов А. А.* Элементы дискретной математики в задачах. М.: МЦНМО, 2016. Abridged version:
<http://www.mccme.ru/circles/oim/discrbook.pdf>.
- [GIF] *Генкин С. А., Итенберг И. В., Фомин Д. В.* Ленинградские математические кружки. Киров, 1994.
- [GKP] *Грэхем Р., Кнут Д., Паташник А.* Конкретная математика. М.: Мир, 1998.
- [LKTG] Summer Conferences of Town Tournament.
<http://www.turgor.ru/en/lktg/index.php>
- [M] Московская математическая конференция школьников.
<http://www.mccme.ru/mmks/index.htm>.
- [Mey] *D. Meyer.* <http://blog.mrmeyer.com/starter-pack>.
- [Pl] *Платон.* Федон, в кн.: Федон, Пир, Федр, Парменид. М.: Мысль, 1999.
- [Ro04] *Рохлин В. А.* Лекция о преподавании математики нематематикам // Математическое просвещение. Сер. 3. 2004. Вып. 8. С. 21–36.
- [RMP] Ross Mathematics Program, <http://u.osu.edu/rossmath>.

- [VIN] *Виро О. Я., Иванов О. А., Нецветаев Н. Ю., Харламов В. М.* Элементарная топология. М.: МЦНМО, 2010.
- [Ar04] *Арнольд В. И.* Задачи для детей от 5 до 15 лет. М.: МЦНМО, 2004.
- [BSh] *Блинков А. Д., Шаповалов А. В.* (ред.). Серия «Школьные математические кружки».
- [IBL] http://en.wikipedia.org/wiki/Inquiry-based_learning
- [KK08] *Канель-Белов А. Я., Ковальджи А. К.* Как решают нестандартные задачи. М.: МЦНМО, 2008.
- [KK15] *Ковальджи А. К., Канель-Белов А. Я.* Занятия по математике — листки и диалог // Математическое просвещение. Сер. 3. 2015. Вып. 19. С. 206–233.
- [PoSe] *Пойа Д, Сегё Г.* Задачи и теоремы из анализа. М.: Наука, 1978.
- [Pr07-1] *Прасолов В. В.* Задачи по планиметрии. М.: МЦНМО, 2007.
- [Sk09] *Скопенков А. Б.* Основы дифференциальной геометрии в интересных задачах. М.: МЦНМО, 2009;
<http://arxiv.org/abs/0801.1568>.
- [Sk19] *A. Skopenkov*, Mathematics via problems: from olympiades and math circles to a profession. Algebra. AMS, Providence, to appear.
- [SCY] *Шклярский Д. О., Ченцов Н. Н., Яглом И. М.* Избранные задачи и теоремы элементарной математики. М.: Физматлит, 2001.
- [Su] *Судзуки Д.* Основы дзэн-буддизма. Наука дзэн — ум дзэн. Киев: Преса України. 1992.
- [SZ] *Mathematics via problems: from olympiades and math circles to a profession. Geometry and Combinatorics*, editors: M. Skopenkov and A. Zaslavsky. AMS, Providence, to appear.

- [ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии. Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. Изд-во МЦНМО, 2018. Abridged version: <http://www.mccme.ru/circles/oim/materials/sturm.pdf>.
- [ZPS] Математика в задачах. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. М.: МЦНМО, 2009;
<http://www.mccme.ru/free-books/olymp/matprob.pdf>.
- [Va87-1] *Васильев Н. Б.* и др. Заочные математические олимпиады. М.: Наука, 1987.
- [Zv] *Звонкин А. К.* Малыши и математика. М.: МЦНМО, 2006.

2.1 Делимость (1)

2.1.1. (а) Сформулируйте и докажите признаки делимости на 2, 4, 5, 10, 3, 9, 11.

(б) Делится ли число $11\dots 1$ из 1993 единиц на 111111?

(с) Число $1\dots 1$ из 2001 единиц делится на 37.

2.1.2. Если a делится на 2 и не делится на 4, то количество чётных делителей числа a равно количеству его нечётных делителей.

2.1.3. Какие из следующих утверждений верны для любых a, b :

(а) $2|(a^2 - a)$; (б) $4|(a^4 - a)$; (с) $6|(a^3 - a)$; (д) $30|(a^5 - a)$;

(е) если $c|a$ и $c|b$, то $c|(a + b)$;

(ф) если $b|a$, то $bc|ac$ для любого $c \neq 0$;

(г) если $bc|ac$ для некоторого c , то $b|a$?

При решении задачи 2.1.3 (с) вы использовали следующий факт 2.1.4 (а). Докажите его по определению делимости, не используя единственности разложения на простые множители (задача 2.2.8 (с))! Использование единственности может привести к порочному кругу, ведь обычно при доказательстве единственности используется факт, близкий к утверждению 2.1.4 (а).

2.1.4. (а) Если число a делится на 2 и на 3, то a делится на 6.

(б) Если число a делится на 2, на 3 и на 5, то a делится на 30.

(с) Если число a делится на 17 и на 19, то a делится на 323.

2.1.5. (а) Если k не кратно ни 2, ни 3, ни 5, то $k^4 - 1$ кратно 240.

(б) Если $a + b + c$ делится на 6, то и $a^3 + b^3 + c^3$ делится на 6.

(с) Если $a + b + c$ делится на 30, то и $a^5 + b^5 + c^5$ делится на 30.

(д) Если $n \geq 0$, то $20^{2n} + 16^{2n} - 3^{2n} - 1$ делится на 323.

Подсказки

2.1.4. (а) Имеем $3a - 2a = a$, поэтому a делится на 6.

3 Умножение по простому модулю

Из этого параграфа далее используются в основном теорема Ферма—Эйлера (задачи 3.1.1 и 3.1.5) и теорема о первообразном корне (задача 3.5.6 (b)). Впрочем, при применении теоремы о первообразном корне понимать её доказательство не обязательно.

В этом параграфе латинскими буквами обозначаются *целые числа* или *вычеты* по простому модулю p (что именно — видно из контекста).

3.1 Малая теорема Ферма (2)

3.1.1. (a) Обозначим $\mathbb{Z}_{97} = \{0, 1, \dots, 96\}$. Определим отображение $f: \mathbb{Z}_{97} \rightarrow \mathbb{Z}_{97}$ так: $f(a)$ равно остатку от деления числа $14a$ на 97. Тогда f — взаимно однозначное соответствие.

Обсуждение. Достаточно доказать либо сюръективность, либо инъективность. Обычно доказывают *инъективность*. Но необходимая для этого основная лемма арифметики 2.5.7.b обычно доказывается через разрешимость уравнения $97x + 14y = 1$, из которой сразу вытекает *сюръективность*.

(b) Справедливо соотношение $(14 \cdot 1) \cdot (14 \cdot 2) \cdot \dots \cdot (14 \cdot 96) \equiv 96! \pmod{97}$.

(c) Справедливо соотношение $14^{96} \equiv 1 \pmod{97}$.

(d) **Малая теорема Ферма.** Если p простое, то $n^p - n$ делится на p для любого целого n .

(e) *Alio modo.* Если p простое и n не делится на p , то $n^{p-1} - 1$ делится на p .

(f) Для простого p число $\binom{p}{k}$ делится на p для любого $k = 1, 2, \dots, p-1$. (Из этого получается иное — по индукции — доказательство малой теоремы Ферма.)

3.1.2. Найдите остаток от деления

- (a) 2^{100} на 101; (b) 3^{102} на 101; (c) 8^{900} на 29;
 (d) 3^{2000} на 43; (e) 7^{60} на 143; (f) $2^{60} + 6^{50}$ на 143.

3.1.3. (a) Если p простое и $p > 2$, то $7^p - 5^p - 2$ делится на $6p$.

(b) Число $111\dots 11$ из 2002 единиц делится на 2003.

(с) Если p и q — различные простые числа, то $p^q + q^p - p - q$ делится на pq .

(d) Число $30^{239} + 239^{30}$ составное.

(е) Если p простое, то длина периода десятичной дроби $1/p$ делит $p - 1$.

3.1.4. Для простого p и a , не делящегося на p , назовём *порядком* $\text{ord } a = \text{ord}_p a$ числа (или вычета) a по модулю p наименьшее $k > 0$, для которого $a^k \equiv 1 \pmod{p}$:

$$\text{ord } a = \text{ord}_p a := \min\{k \geq 1 \mid a^k \equiv 1 \pmod{p}\}.$$

(а) Множество $\{m \geq 0 : a^m \equiv 1 \pmod{p}\}$ состоит из целых неотрицательных чисел, кратных $\text{ord } a$.

(b) Если $a^m \equiv a^n \pmod{p}$, то $m - n$ делится на $\text{ord } a$.

(с) **Лемма.** Число $p - 1$ делится на $\text{ord } a$.

(d) Если $\text{ord } x$ и $\text{ord } y$ взаимно просты, то $\text{ord}(xy) = \text{ord } x \cdot \text{ord } y$.

(е) Для любых ли a, x, p верно, что $a \text{ord}_p x^a = \text{ord}_p x$?

Заметим, что по простому модулю можно определить деление и отрицательные степени. Аналоги утверждений 3.1.4 (а, b) справедливы для отрицательных степеней.

3.1.5. В этой задаче буквами $p, q, p_1, \dots, p_k$ обозначаются различные простые числа.

(а) Если $p \neq q$ и n не делится ни на p , ни на q , то $n^{(p-1)(q-1)} - 1$ делится на pq .

(b) Если n не делится на p , то $n^{p^\alpha(p-1)} - 1$ делится на $p^{\alpha+1}$.

(с) **Теорема Эйлера.** Если n взаимно просто с $m = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$ и $\varphi(m) := (p_1 - 1)p_1^{\alpha_1-1} \cdot \dots \cdot (p_k - 1)p_k^{\alpha_k-1}$, то $n^{\varphi(m)} - 1$ делится на m .

(d) Число $\varphi(m)$ равно количеству чисел от 1 до m , взаимно простых с m .

3.1.6. (Загадка.) Известно, что n — нечётное число от 3 до 47, не делящееся на 5. Как быстро вычислять неизвестное n по известному $n^7 \bmod 50$?

Решение этой загадки показывает, почему для шифрования так важно быстро находить разложение числа на простые множители, в частности быстро распознавать простоту числа.

3.3 Квадратичные вычеты (2*)

Цель этого цикла задач — мотивировать и обсудить проблему разрешимости сравнения $x^2 \equiv a \pmod{p}$ для простого p . В этом пункте через p обозначается нечётное простое число.

3.3.1. (а) Какие остатки могут давать квадраты целых чисел при делении на 3, 4, 5, 6, 7, 8, 9, 10?

(b) Если $a^2 + b^2$ делится на 3 (на 7), то a и b делятся на 3 (на 7).

(c) Число вида $4k + 3$ не представимо в виде суммы двух квадратов.

(d) Существует бесконечно много чисел, не представимых в виде суммы трёх квадратов.

3.3.2. Решите уравнения в целых числах:

(a) $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = y^2$ (в нечётных числах);

(b) $3x = 5y^2 + 4y - 1$; (c) $x^2 + y^2 = 3z^2$; (d) $2^x + 1 = 3y^2$;

(e) $x^2 = 2003y - 1$; (f) $x^2 + 1 = py$, где $p = 4k + 3$;

3.3.3. (а) Если $p = 4k + 3$ делит $a^2 + b^2$, то $p|a$ и $p|b$.

(b) Число, в каноническое разложение которого некоторый простой делитель вида $4k+3$ входит в нечётной степени, не представимо в виде суммы двух квадратов (целых чисел).

(c)* Уравнение $x^2 + 1 = py$ разрешимо в целых числах при $p = 4k + 1$ (и неразрешимо при $p = 4k + 3$).

(d)* Любое простое число вида $4k + 1$ представимо в виде суммы двух квадратов.

(e)* Число, в каноническое разложение которого любой простой делитель вида $4k + 3$ входит в чётной степени, представимо в виде суммы двух квадратов.

(f) Простых чисел вида $4k + 1$ бесконечно много.

Доказательство Дон Загира утверждения (d) можно найти в книге [Pr07-1].

3.3.4. (Загадка.) «Сведите» уравнение $py = at^2 + bt + c$, $a \neq 0$, к сравнению $x^2 \equiv k \pmod{p}$.

Остаток $a \neq 0$ называется *квадратичным вычетом* (квадратичным невычетом) по модулю p , если сравнение $x^2 \equiv a \pmod{p}$ разрешимо (неразрешимо). Слова «по модулю p » далее опускаются.

3.4 Квадратичный закон взаимности (3*)

Здесь строится алгоритм выяснения разрешимости сравнения $x^2 \equiv a \pmod{p}$ для простого p . Используется п. 3.3 «Квадратичные вычеты».

3.4.1. Если число $p = 8k + 5$ простое, то

- (a) $2^{4k+2} \equiv -1 \pmod{p}$;
- (b) уравнение $x^2 - 2 = py$ неразрешимо в целых числах.

3.4.2. Если число $p = 8k + 1$ простое, то

- (a) $2^{4k} \equiv 1 \pmod{p}$;
- (b) уравнение $x^2 - 2 = py$ разрешимо в целых числах.

3.4.3. (a) Если число $p = 8k \pm 1$ простое, то $2^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) Если число $p = 8k \pm 3$ простое, то $2^{(p-1)/2} \equiv -1 \pmod{p}$.

(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 2 = py$?

3.4.4. (a) Если число $p = 12k \pm 1$ простое, то $3^{(p-1)/2} \equiv 1 \pmod{p}$.

(b) Если число $p = 12k \pm 5$ простое, то $3^{(p-1)/2} \equiv -1 \pmod{p}$.

(c) Для каких простых p разрешимо в целых числах уравнение $x^2 - 3 = py$?

3.4.5. Для нечётного простого числа p рассмотрим символ Лежандра

$$\left(\frac{a}{p}\right) := \begin{cases} +1, & a - \text{квадратичный вычет по модулю } p; \\ -1, & a - \text{квадратичный невычет по модулю } p. \end{cases}$$

Например, $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$ по задаче 3.4.3 и $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ по задаче 3.3.8.

(a) **Критерий Эйлера.** Справедливо соотношение

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

(b) **Лемма Гаусса.** Справедливо соотношение

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{(p-1)/2} \left[\frac{2ax}{p}\right]}.$$

3.5 Первообразные корни (3*)

3.5.1. (2–7) Сформулируйте и обоснуйте алгоритм решения сравнения $a^x \equiv b \pmod{m}$ для заданных a, b , взаимно простых с заданным $m \in \{2, 3, 4, 5, 6, 7\}$.

(Решение такого сравнения — одна из основных мотивировок этого занятия.)

3.5.2. (a) Если $(a, 35) = 1$, то $a^{12} \equiv 1 \pmod{35}$.

(b) Если m делится на два различных простых нечётных числа и $(a, m) = 1$, то $a^{\frac{\varphi(m)}{2}} \equiv 1 \pmod{m}$.

Пусть $(g, m) = 1$. Вычет g называется *первообразным корнем* по модулю m , если остатки от деления на m чисел $g^1, g^2, \dots, g^{\varphi(m)} \equiv 1$ различны. Например,

- число 2 является первообразным корнем по модулю 5, а число 4 — нет;

- по задаче 3.5.2 (b) если m делится на два различных простых нечётных числа, то не существует первообразного корня по модулю m .

3.5.3. Докажите существование первообразного корня по простому модулю следующего вида:

(a) 257; (b) $2^l + 1$; (c) $2^k \cdot 3^l + 1$; (d) 151; (e) $2^k \cdot 3^l \cdot 5^m + 1$.

Простой метод решения пунктов (a), (b), (c), не проходит для (d), (e). Продемонстрируем метод решения пунктов (d), (e) на примерах.

3.5.4. (a) Вычет g — первообразный корень по модулю 97 тогда и только тогда, когда ни g^3 , ни g^{32} не сравнимы с 1 по модулю 97.

(b) Сравнение $x^3 \equiv 1 \pmod{97}$ имеет ровно 3 решения.

(c) Сравнение $x^{32} \equiv 1 \pmod{97}$ имеет ровно 32 решения.

(d) Существует первообразный корень по модулю 97.

(e) Количество первообразных корней по модулю 97 равно 63.

3.5.5. (a) Вычет g — первообразный корень по модулю 151 тогда и только тогда, когда ни g^{30} , ни g^{50} , ни g^{75} не сравнимы с 1 по модулю 151.

3.6 Высокие степени (3*). А. Я. Канель-Белов, А. Б. Скопенков

- 3.6.1.** (а) Для любых n и нечетного k число $k^{2^n} - 1$ делится на 2^{n+2} .
(б) Для любого n число $2^{3 \cdot 7^n} - 1$ делится на 7^{n+1} .

3.6.2. При каких a

- (а) $2^a - 1$ делится на 3^{100} ; (б) $2^a + 1$ делится на 3^{100} ;
(с) $5^a - 1$ делится на 2^{100} ; (д) $2^a - 1$ делится на 5^{100} ?

Утверждение 3.6.1 (а) означает, что ни при каком $n \geq 3$ не существует первообразного корня по модулю 2^n (см. определение в п. 3.5). Ответы к задачам 3.6.2.(а),(д),(с) и утверждение 3.6.1.(б) означают, что для любого n число 2 является первообразным корнем по модулю 3^n и по модулю 5^n , а числа 5 и 2 не являются первообразными корнями по модулю 2^n и по модулю 7^n .

3.6.3. (а) Найдите первообразный корень по модулю 7^{100} .

(б) **Теорема.** Первообразные корни существуют только по модулям $2, 4, p^n, 2p^n$.

3.6.4. Пусть $p > 2$ простое, g — первообразный корень по модулю p и $g^{p-1} - 1$ не делится на p^2 . Тогда g — первообразный корень по модулю

- (а) p^2 ; (б) p^3 ; (с) p^n для любого n .

3.6.5. Пусть $p > 2$ простое.

(а) Если g — первообразный корень по модулю p , то одно из чисел $g^{p-1} - 1$ и $(g + p)^{p-1} - 1$ не делится на p^2 .

(б) Если g — первообразный корень по модулю p^2 , то g — первообразный корень по модулю p^n для любого n .

(с) Для любого целого положительного n существует первообразный корень по модулю p^n .

(д) То же по модулю $2p^n$.

3.6.6. Лемма об уточнении показателя. Пусть p — простое число, $p > 2$ или $n > 1$, q не делится на p и $x - 1$ делится на p^n , но не на p^{n+1} .

- (а) Число $x^q - 1$ делится на p^n , но не на p^{n+1} .

4.2 Решение уравнений 3-й и 4-й степени (2)

Благодарю О. Е. Орёл за полезные обсуждения.

Приведённый здесь материал важен и широко известен, но не входит в школьную или университетскую программу. Отличие приводимого рассуждения от встречающихся в других источниках в том, что (вместо немотивированных замен) уравнения естественно сводятся к таким, которые ясно, как решать.

Например, уравнение $x^2 + 4x - 1 = 0$ сводится к уравнению $y^2 - 5 = 0$ заменой переменной $y = x + 2$.

4.2.1. (а) Уравнение $x^3 + 3x^2 + 5x + 7 = 0$ «сводится» заменой переменной к уравнению $y^3 + py + q = 0$ с некоторыми числами p, q .

(б) Уравнение $ax^3 + bx^2 + cx + d = 0$ при $a \neq 0$ «сводится» заменой переменной к уравнению $y^3 + py + q = 0$ с некоторыми числами p, q .

(с) Уравнение $ax^4 + bx^3 + cx^2 + dx + e = 0$ при $a \neq 0$ «сводится» заменой переменной к уравнению $y^4 + py^2 + qy + r = 0$ с некоторыми числами p, q, r .

4.2.2. (а) Докажите, что $\sqrt[3]{2 + \sqrt{5}} - \sqrt[3]{\sqrt{5} - 2} = 1$.

(б) Найдите хотя бы одно решение уравнения $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

Указание. Метод дель Ферро. Так как

$$(u + v)^3 = u^3 + v^3 + 3uv(u + v),$$

то число $u + v$ является корнем уравнения $x^3 - 3uvx - (u^3 + v^3) = 0$.

(с) Решите уравнение $x^3 - 3\sqrt[3]{2}x + 3 = 0$.

4.2.3. (а) Разложите на множители выражение $a^3 + b^3 + c^3 - 3abc$.

(б) Справедливо неравенство $a^2 + b^2 + c^2 \geq ab + bc + ca$. Когда достигается равенство?

(с) Справедливо неравенство $a^3 + b^3 + c^3 \geq 3abc$ при $a, b, c > 0$.

(д) Разложите выражение $a^3 + b^3 + c^3 - 3abc$ на линейные множители с комплексными коэффициентами.

Задачи этого пункта о комплексных числах можно пропустить. Но для их решения необходимы лишь минимальные сведения о комплексных числах: достаточно уметь решать задачи 4.5.1 и 4.5.2.

4.2.4. (а) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^2 + px + q = 0$.

(b) Сформулируйте и докажите теоремы, описывающие все вещественные (все комплексные) решения уравнения $x^3 + px + q = 0$ в том случае, когда работает метод дель Ферро (см. задачу 4.2.2). А при каком условии на p, q применим этот метод для вещественных решений, если квадратные корни разрешается извлекать только из положительных чисел?

(с) Составьте алгоритм (точного, или символьного) нахождения всех вещественных корней уравнения $ax^3 + bx^2 + cx + d = 0$, где $a \neq 0$.

При решении некоторых кубических уравнений методом дель Ферро в формулах неожиданным образом возникают комплексные числа — как раз тогда, когда все корни исходного уравнения вещественны. Такие уравнения можно также решать следующим «чисто вещественным» методом. Он также интересен тем, что подводит к *трансцендентным методам* решения уравнений [PSo].

4.2.5. (а) Решите уравнение $4x^3 - 3x = \frac{1}{2}$.

(b) Решите уравнение $x^3 - 3x - 1 = 0$.

(с) Используя функции $\cos$ и $\arccos$, напишите общую формулу для решения уравнения $x^3 + px + q = 0$ методом, намеченным в этой задаче. При каком условии уравнение $x^3 + px + q = 0$ решается этим методом?

4.2.6. Решите уравнение

(а) $(x^2 + 2)^2 = 9(x - 1)^2$; (b) $x^4 + 4x - 1 = 0$;

(с) $x^4 + 2x^2 - 8x - 4 = 0$; (d) $x^4 - 12x^2 - 24x - 14 = 0$.

Указание к задаче 4.2.6 (b). Метод Феррари. Подберите такие α, b, c , что

$$x^4 + 4x - 1 = (x^2 + \alpha)^2 - (bx + c)^2.$$

Для этого найдите хотя бы одно α , для которого квадратный трёхчлен $(x^2 + \alpha)^2 - (x^4 + 4x - 1)$ от x является полным квадратом. Для этого найдите дискриминант этого квадратного трёхчлена. Он является кубическим многочленом от α и называется *кубической резольвентой* многочлена $x^4 + 4x - 1$.

4.7 Диофантовы уравнения и гауссовы числа (4*). А. Я. Канель-Белов

Всем хорошо знаком алгоритм Евклида. Даны два числа a, b . Из них выбирается большее, из большего вычитается меньшее, большее заменяется на разность, и с новой парой чисел производится та же процедура. См. задачу 2.5.9 (b). С помощью алгоритма Евклида доказываются арифметические свойства чисел и это Вы изучали раньше (см. п. 2.5 «Линейные диофантовы уравнения» и п. 4.4 «Делимость для многочленов»). Приведём принципиально новые (для большинства школьников) его применения.

4.7.1. Решите уравнения в целых числах:

$$(a) \ x^2 + 4 = y^3; \quad (b) \ x^2 + 2 = y^n; \quad (c)^* \ x^3 + y^3 = z^3.$$

Попробуйте порешать их, не читая дальнейшего! Впрочем, у Вас вряд ли получится. Возвращайтесь к этой задаче по мере чтения дальнейшего материала.

При решении уравнения $x^2 + 4 = y^3$ в целых числах хочется действовать так: $x^2 + 4 = (x + 2i)(x - 2i)$. При нечётном x оба эти множителя взаимно просты, и потому оба являются кубами. Из этого получается решение. (Случай чётного x хитрее: обе скобки могут делиться на $(1 + i)^3$.) Попробуйте довести решение до конца, а затем сравнить с приведённым в конце темы.

Одним словом, хочется наслаждаться дополнительными возможностями при разложении на множители за счёт использования *гауссовых чисел*, т. е. чисел вида $a + bi$ с целыми a и b . Однако не всё коту масленица — так получается не всегда (см. задачи 2.2.8 (b) и 4.7.3 (b)), но иногда получается. Чтобы применять разложение на множители для решения уравнений, нужна *однозначность разложения на простые множители*. Если она имеет место, то мы имеем всё те же арифметические удовольствия, что и для целых чисел. Следующая задача показывает удивительный факт: для *арифметических* удовольствий достаточно доказать *геометрический* факт о возможности деления с остатком.

4.7.2. Гауссово число называется *простым*, если оно не разлагается на два множителя, каждый из которых отличен от ± 1 и $\pm i$. В этой задаче латинские буквы обозначают гауссовы числа.

(а) Однозначность разложения на простые множители вытекает из следующего свойства (аналога леммы Евклида 2.5.7 (с)).

Факториальность. Для любых a, b если простое число p делит ab , то p делит a или p делит b .

(b) Факториальность вытекает из следующего свойства (аналога леммы о представлении НОД 2.5.7 (а)).

Главной идеальность. Для любых a, b существуют такие x, y , что $xa + yb = \gcd(a, b)$. (Дайте определение наибольшего общего делителя $\gcd(a, b)$ чисел a, b самостоятельно!)

(с) Главной идеальность обеспечивается следующим свойством (аналогом теоремы о делении с остатком 2.4.1 (b)).

Евклидовость. Для любых $b \neq 0$ и a существует такое k , что $|a - kb| < |b|$.

4.7.3. Верна ли евклидовость (и, значит, факториальность!) для множества $\mathbb{Z}[\xi]$ чисел вида $a + b\xi$ с целыми a, b , если ξ есть

- (а) $\sqrt{-2}$; (b) $\sqrt{-3}$; (с) $(1 - \sqrt{-3})/2$; (d) $(1 - \sqrt{-5})/2$;
(е) $(1 - \sqrt{-7})/2$?

4.7.4. (а) Никакое простое число вида $4k - 1$ не разлагается в сумму двух квадратов.

(b) Любое простое число вида $4k + 1$ разлагается в сумму двух квадратов, причём ровно одним способом.

(b) Существует целое число, ровно 1024 способами разлагающееся в сумму двух квадратов.

Эту задачу проще решать без гауссовых чисел (см. п. 3.3), однако полезно потренироваться в их применении!

Подробнее см. [Pos, § 4]. См. также задачу 4.4.7.

Указания, ответы и решения

4.7.1. (а) (Р. И. Девятов) *Ответ:* $x = \pm 2, y = 2$ и $x = \pm 11, y = 5$.
Перейдём к целым гауссовым числам и получим $(x + 2i)(x - 2i) = y^3$.

Целое гауссово число называется *точным кубом*, если оно равно b^3 для некоторого целого гауссова числа b . Заметим, что все «обратимые» числа $\pm 1, \pm i$ являются точными кубами. Поэтому точным

5.3 Комбинаторика классов эквивалентности (2)

Этот пункт посвящён подсчёту числа классов эквивалентности (т. е. раскрасок и т. д.). Такой подсчёт подводит читателя к важному понятию *группы преобразований* и к элементарной формулировке *леммы Бёрнсайда*. Формулировка и доказательство этого и других результатов на языке абстрактной теории групп делает их менее доступными. Ср. [ZSS, § 28 «О необходимости мотивировок»].

Не требуется, чтобы в раскраске присутствовали все данные цвета. Раскраски, совмещающиеся вращением пространства (т. е. движением пространства, сохраняющим ориентацию и имеющим неподвижную точку), считаются одинаковыми (кроме задачи 5.3.1 (с)).

Следующие определения используются только в задачах 5.3.1.(b), 5.3.6.(e), 5.3.11 (и потому могут быть пропущены при решении остальных задач).

Изоморфизм между графами— такая биекция между множествами их вершин, что для любых двух вершин эти вершины соединены ребром тогда и только тогда, когда их образы при биекции соединены ребром. *Аutomорфизм* графа— его изоморфизм на себя.

5.3.1. Сколько существует

- (a) раскрасок граней куба в красный и серый цвета;
- (b) различных (т. е. неизоморфных) неориентированных графов с 4 вершинами;
- (c) раскрасок в r цветов вершин правильного тетраэдра?

Здесь раскраски, совмещающиеся движением пространства (не обязательно сохраняющим ориентацию), считаются одинаковыми.

5.3.2. Для простого p найдите количество замкнутых ориентированных связных p -звенных ломаных (возможно, самопересекающихся), проходящих через все вершины данного правильного p -угольника.

Здесь ломаные, совмещающиеся поворотом, неотличимы.

Задачи 5.3.1 и 5.3.2 простые, их можно решить без идей, приводящих к лемме Бёрнсайда.

5.3.3. Найдите количество раскрасок карусели из n незанумерованных вагончиков в r цветов (т. е. количество раскрасок вершин

правильного n -угольника в r цветов, если раскраски, совмещающиеся поворотом, неотличимы) для

(a) $n = 5$; (b) $n = 4$; (c) $n = 6$.

Задачу 5.3.3 для произвольного n можно решить способом, аналогичным придуманному вами для малых n . Однако решение будет громоздким. Приведём более простой (для «очень непростых» n) способ на примере решения задачи 5.3.3 (c).

Назовём (*раскрашенным*) *поездом* раскраску карусели из *занумерованных* вагончиков в r цветов. Тогда всего имеется r^6 поездов из 6 вагончиков.

Распределим поезда по вокзалам так, чтобы на каждом вокзале находились все поезда, полученные из некоторой одной раскраски карусели всевозможными разрубаниями, т. е. искомое количество Z раскрасок равно количеству вокзалов.

Назовем *периодом* $T(\alpha)$ поезда α наименьшую положительную величину циклического сдвига, переводящего поезд α в себя.

5.3.4. Количество поездов на вокзале равно периоду каждого из поездов, стоящих на этом вокзале. В частности, периоды поездов, стоящих на одном вокзале, равны.

На каждом вокзале выберем один поезд. Посадим в него 6 пассажиров и выдадим им билеты с числами 0, 1, 2, 3, 4, 5. Тогда нужно найти общее число $6Z$ пассажиров.

По команде каждый пассажир переходит в (раскрашенный) поезд, полученный из выбранного поезда циклическим сдвигом на число, указанное в билете пассажира. Ясно, что каждый пассажир остается на прежнем вокзале.

5.3.5. (a) В выбранном поезде α останется $6/T(\alpha)$ пассажиров. Более формально, количество тех $s \in \{0, 1, 2, 3, 4, 5\}$, для которых циклический сдвиг на s переводит поезд α в себя, равно $6/T(\alpha)$.

(b) В каждом поезде α окажется $6/T(\alpha)$ пассажиров.

Значит, общее число $6Z$ пассажиров равно количеству всех пар (α, s) , в которых $s \in \{0, 1, 2, 3, 4, 5\}$ и α — поезд, переходящий в себя

при циклическом сдвиге на s вагончиков. Циклический сдвиг на s переводит в себя ровно $r^{\gcd(s,6)}$ поездов. Поэтому

$$6Z = r^6 + r + r^2 + r^3 + r^2 + r.$$

Приведенный план решения можно представить в виде формулы

$$6Z = \sum_x T(x) \cdot \frac{6}{T(x)} = \sum_{\alpha} \frac{6}{T(\alpha)} = r^6 + r + r^2 + r^3 + r^2 + r.$$

Здесь первое суммирование происходит по всем по всем раскраскам x каруселей, а второе — по всем поездам α .

5.3.6. Найдите количество

- (а) раскрасок карусели из n вагончиков в r цветов;
- (б) r -цветных ожерелий из $n = 2k+1$ бусин (ожерелья считаются одинаковыми, если они совмещаются либо поворотом вокруг центра ожерелья, либо осевой симметрией ожерелья);
- (с) раскрасок незанумерованных граней куба в r цветов;
- (д) раскрасок незанумерованных вершин куба в r цветов;
- (е) раскрасок незанумерованных вершин графа $K_{3,3}$ (рис. 2) в r цветов (раскраски считаются одинаковыми, если они совмещаются автоморфизмом этого графа).

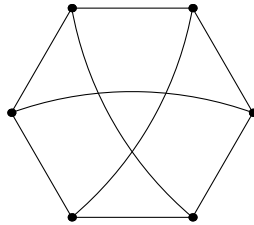


Рис. 2: Граф $K_{3,3}$

5.3.7. Перечислите все вращения куба (т.е. вращения пространства, переводящие куб в себя). (Эта задача разбита на шаги в [SZ, п. «Самосовмещения»].)

Приведем план решения задачи 5.3.6 (с). (Пункты (б)–(е) решаются аналогично. Пункт (б) решается и без этого указания.)

Назовём (*раскрашенной*) *коробкой* (или *замороженной раскраской*) раскраску занумерованных граней куба в r цветов. Тогда всего имеется r^6 коробок.

Распределим коробки по комнатам так, чтобы в каждой комнате находились все коробки, полученные из некоторой одной коробки всевозможными вращениями, т. е. искомое количество Z раскрасок равно количеству комнат.

В каждой комнате выберем одну коробку. Посадим в нее 24 таракана, соответствующих вращениям куба. Тогда нужно найти общее число тараканов $24Z$.

По команде каждый таракан переползает в коробку, полученную из выбранной тем вращением, которое соответствует этому таракану. Ясно, что каждый таракан остается в прежней комнате. Число тараканов, оставшихся в выбранной коробке, равно количеству вращений куба, переводящих эту коробку в себя. Обозначим через $st\alpha$ количество вращений куба, переводящих (раскрашенную) коробку (т. е. замороженную раскраску) α в себя.

5.3.8. (a) Число тараканов, оказавшихся в коробке α , равно $st\alpha$. Более формально, если существует вращение, переводящее замороженную раскраску α в замороженную раскраску α' , то количество таких вращений равно $st\alpha$.

(b) В любой другой коробке из выбранной комнаты окажется столько же тараканов, сколько в выбранной коробке. Более формально, для любых двух замороженных раскрасок α и α' , переходящих друг в друга при некотором вращении, выполняется равенство $st\alpha = st\alpha'$. (Эти равные числа обозначаются stx , где x — соответствующая раскраска незанумерованных граней куба.)

Поэтому общее число тараканов равно количеству всех пар (α, s) , в которых s — вращение куба и α — коробка, переходящая в себя при вращении s . Поэтому осталось решить следующую задачу.

5.3.9. Для каждого вращения куба s найдите количество $fixs$ коробок (т. е. замороженных раскрасок), переходящих в себя при вращении s .

Обозначим через N_x количество замороженных раскрасок, отвечающих раскраске x . Тогда для любой раскраски x число $stx \cdot N_x$

равно количеству вращений куба, т. е. 24. Поэтому приведенный план решения можно представить в виде формулы

$$24Z = \sum_x \text{st}x \cdot N_x = \sum_\alpha \text{st}\alpha = \sum_s \text{fix}s.$$

Здесь первое суммирование происходит по всем раскраскам x пронумерованных граней, второе — по всем замороженным раскраскам α , а третье — по всем вращениям куба s .

Как сформулировать общий результат, который можно было применять вместо повторения намеченных решений задач 5.3.6 (а), (с)?

5.3.10. Лемма Бёрнсайда. Пусть заданы конечное множество M и семейство $\{g_1, g_2, \dots, g_n\}$ преобразований этого множества, замкнутое относительно взятия композиции и взятия обратного элемента. Назовём элементы множества M *эквивалентными*, если один из них можно перевести в другой одним из данных преобразований. Тогда количество классов эквивалентности равно $\frac{1}{n} \sum_{k=1}^n \text{fix}(g_k)$, где $\text{fix}(g_k)$ — количество элементов множества M , которые преобразование g_k переводит в себя.

5.3.11. Найдите количество графов с n вершинами с точностью до изоморфизма. (Ответ можно оставить в виде суммы.)

5.3.12. (а) Найдите количество b_n отображений $\{0, 1\}^n \rightarrow \{0, 1\}$ с точностью до перестановки переменных.

(б) Докажите, что существует предел $\lim_{n \rightarrow \infty} n!b_n/2^{2^n}$ и найдите его. (см. определение в задаче 7.4.2; те, кто не знают, что это такое, могут пропустить этот пункт).

Подсказки

5.3.1. *Ответы:* (а) 10; (б) 11; (с) $r(r+1)(r+2)(r+3)/24$.

5.3.2. *Ответ:* $p - 2 + ((p-1)! + 1)/p$.

5.3.3. *Ответы:* (а) $(r^5 + 4r)/5$; (б) $(r^4 + r^2 + 2r)/4$;
(с) $(r^6 + r^3 + 2r^2 + 2r)/6$.

7 Последовательности и пределы

Этот параграф почти независим от остальной части книги. В других местах из него используются лишь простые факты.

7.1 Конечные суммы и разности (3)

Последовательностью сумм последовательности $\{a_n\}_{n=1}^{\infty}$ называется последовательность $b_n = \Sigma a_n := a_1 + \dots + a_n$, а *последовательностью разностей* — последовательность $c_n = \Delta a_n := a_{n+1} - a_n$.

Например, $\Delta 2^n = 2^n$ и $\Sigma 2^n = 2^{n+1} - 2$.

(Сумма и разность — аналоги *интеграла* и *производной*.)

В этом пункте n обозначает номер члена последовательности, «по которому» берётся сумма и разность. Так, например, $\Delta 2^k = 0$.

7.1.1. Найдите

(а) Δn^k для каждого целого $k \geq -1$; (б) $\Delta \cos n$; (с) $\Delta(n \cdot 2^n)$.

7.1.2. Найдите

(а) $\Sigma \sin n$; (б) $\Sigma \frac{1}{n(n+1)\dots(n+k)}$ для каждого целого $k > 0$.

7.1.3. Какие из указанных равенств выполняются для некоторой непостоянной последовательности a_n :

(а) $\Delta a_n = 0$; (б) $\Delta a_n = 1$; (с) $\Delta a_n = a_n$;
(д) $\Sigma a_n = a_n$; (е) $\Sigma \Delta a_n = a_n$; (ф) $\Delta \Sigma a_n = a_n$?

7.1.4. (а) Найдите $\sum_{k=0}^n (-1)^k k^2 \binom{n}{k}$.

(б) **Лемма.** k -я разность многочлена k -й степени есть постоянная, а $(k+1)$ -я равна 0.

(с) (Загадка.) Выразите $\Delta^k a_n$ через $a_n, a_{n+1}, \dots, a_{n+k}$.

(д) **Лемма.** Равенство $\Delta^k a_n = 0$ имеет место тогда и только тогда, когда a_n — многочлен от n степени не выше $k-1$.

(е) Для некоторого многочлена $P_\lambda(n)$, имеющего степень l при $\lambda \neq 1$ и степень $l-1$ при $\lambda = 1$, выполняется равенство $\Delta(n^l \lambda^n) = P_\lambda(n) \lambda^n$.

(ф) **Формула Лейбница.** Справедливо равенство

$$\Delta(a_n b_n) = a_{n+1} \Delta b_n + b_n \Delta a_n.$$

7.2.3. Ответы: (a) $2^n - 1$; (b) 3^{n-1} ; (c) $2n - 1$;
(d) $(n + 1)2^{n-2}$; (f) $\frac{a-7}{6}3^n + \frac{9-a}{2}(2^n - 1)$, $a := a_3$.

7.2.4. Ответы: (a) $5 \cdot 2^{n-1}$; (b) $3 \cdot 2^n - 1$; (c) $7 \cdot 2^{n-1} - n - 1$;
(d) $2^n + 3^n$; (e) $(n + 4)2^{n-1}$; (f) $(n - 3)3^n + 11 \cdot 2^{n-1}$.

7.2.5. Ответы, в которых $a := a_2$:

- (a) $(a - 10)3^{n-1} + (15 - a)2^{n-1}$;
- (b) $\left(a - \frac{19}{2}\right)3^{n-1} + (14 - a)2^{n-1} + \frac{1}{2}$;
- (c) $\left(a - \frac{37}{4}\right)3^{n-1} + (13 - a)2^{n-1} + \frac{n}{2} + \frac{3}{4}$;
- (d) $(n + a - 14)3^{n-1} + (18 - a)2^{n-1}$;
- (e) $(a - 8)3^{n-1} + (14 - a - n)2^{n-1}$;
- (f) $\left(\frac{n^2-7n}{2} + a - 1\right)3^{n-1} + (9 - a)2^{n-1}$.

7.3 Конкретная теория пределов (4*)

Задачи этого пункта интересны не только как простейший способ разобраться в теории пределов. Похожие задачи о конкретных, хотя и грубых оценках часто возникают и на олимпиадах, и в прикладной математике, и в теоретической математике.

В решении этих задач нельзя пользоваться функциями $\sqrt[n]{x}$, a^x , $\log_a x$, $\arcsin x$ и т. п. без определения этих функций (поскольку для их определения — например, для доказательства существования такого x , что $x^2 = 2$, — фактически нужно эти задачи решить). Исключение: если некоторая функция используется в условии, то её можно использовать и в решении. Можно пользоваться без доказательства свойствами неравенств.

7.3.1. Найдите хотя бы одно такое N , чтобы для любого $n > N$ выполнялось неравенство $a_n > 10^9$, если

- (a) $a_n = \sqrt{n}$; (b) $a_n = n^2 - 3n + 5$; (c) $a_n = 1,02^n$;
- (d) $a_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \dots + \frac{1}{n}$.

7.3.2. Неравенство Бернулли. Докажите, что $(1 + x)^a \geq 1 + ax$ для любых $x \geq -1$ и

- (a) целого $a \geq 1$; (b) рационального $a \geq 1$;

7.6.2 Задачи (3*)

7.6.1. Следующие числа иррациональны:

$$(a) e := \sum_{n=0}^{\infty} \frac{1}{n!}; \quad (b) \lambda := \sum_{n=0}^{\infty} 2^{-n!}; \quad (c) \mu := \sum_{n=0}^{\infty} 2^{-2^n}.$$

(Используемые здесь бесконечные суммы определены в п. 7.5.)

7.6.2. (e) , (λ) , (μ) Ни одно из чисел e , λ , μ не является корнем квадратного уравнения с целыми коэффициентами.

7.6.3. Для любого рационального числа p/q , не являющегося корнем многочлена f степени t с целыми коэффициентами, выполнено неравенство $|f(p/q)| \geq q^{-t}$.

Теорема 7.6.4 (Лиувилль). (a) Число λ трансцендентно.

(b) Для любых многочлена степени t с рациональными коэффициентами и его иррационального корня α существует такое $C > 0$, что для любых целых p, q выполнено неравенство $\left| \alpha - \frac{p}{q} \right| > Cq^{-t}$.

7.6.5. (a) Число μ не является корнем кубического уравнения с целыми коэффициентами.

(b) Справедливо равенство $\mu^q = \sum_{n=0}^{\infty} d_n(q)2^{-n}$, где $d_n(q)$ есть количество упорядоченных представлений числа n в виде суммы q степеней двойки (не обязательно различных степеней):

$$d_n(q) = |\{(w_1, \dots, w_q) \in \mathbb{Z}^q \mid n = 2^{w_1} + \dots + 2^{w_q} \text{ и } w_1, \dots, w_q > 0\}|.$$

Например, $d_3(2) = 2$, поскольку $3 = 2^0 + 2^1 = 2^1 + 2^0$. По определению полагаем $d_0(0) = 1$.

Лемма 7.6.6. Количество $d_n(q)$ упорядоченных представлений числа n в виде суммы q степеней двойки не превосходит $(q!)^2$.

Теорема 7.6.7 (Малер). Число μ трансцендентно.

Следующая задача — удачная тема для исследовательских работ, см. п. 1.3. Пункты (a), (b), (c) аналогичны теореме Малера 7.6.7. Решение остальных пунктов мне неизвестно, но наверняка доступно сильному старшекласснику (и может быть известно специалистам). Ср. [KaS06, Обобщение].

8.2 Элементы анализа для многочленов (2)

Переменной знака в конечной последовательности $b_0, \dots, b_k$ ненулевых чисел называется такой индекс $i \in \{1, \dots, k\}$, что числа b_{i-1} и b_i имеют разные знаки. *Переменной знака* в конечной последовательности называется переменная знака в последовательности, полученной из данной вычёркиванием нулей.

8.2.1. (а) Число *положительных* решений уравнения $ax^2 + bx + c = 0$ не превосходит числа перемен знака в последовательности a, b, c .

(б) Число положительных решений уравнения $ax^3 + bx^2 + cx + d = 0$ не превосходит числа перемен знака в последовательности a, b, c, d .

8.2.2. (а) **Правило знаков Декарта.** Число положительных решений уравнения $p_n x^n + \dots + p_1 x + p_0 = 0$ не превосходит числа перемен знака в последовательности $p_0, \dots, p_n$.

(б) Как аналогично правилу знаков Декарта оценить количество *отрицательных* корней данного многочлена?

(с)* Как аналогично правилу знаков Декарта оценить количество корней данного многочлена на данном промежутке $[a, b]$?

(д) **Неравенства Маклорена.** Для $x_1, \dots, x_n > 0$ обозначим

$$M_k = \sqrt[k]{\frac{\sum_{i_1 < \dots < i_k} x_{i_1} \cdot \dots \cdot x_{i_k}}{\binom{n}{k}}}.$$

(Заметьте, что M_1 — это среднее арифметическое и M_n — среднее геометрическое.) Тогда $M_1 \geq \dots \geq M_n$.

8.2.3. (а) При чётном n многочлен $\sum_{k=0}^n \frac{x^k}{k!}$ не имеет вещественных корней, а при нечётном n имеет ровно один вещественный корень.

(б) Минимальный модуль корня многочлена $\sum_{k=0}^n \frac{x^k}{k!}$ стремится к бесконечности при $n \rightarrow \infty$.

Для решения этих и многих других задач полезно следующее понятие. *Предпроизводной* f' многочлена f называется многочлен $D_f(x, y) := \frac{f(y) - f(x)}{y - x}$ от двух переменных x, y . (Сообразите, почему это многочлен.) *Производной* многочлена f называется многочлен $f'(x) := D_f(x, x)$.

8.5 Применения компактности (4*). А. Я. Канель-Белов

В этом пункте задачи посложнее и подсказок поменьше. Однако он будет интересен читателю, так как, насколько нам известно, такая подборка интересных задач по этой важной теме впервые публикуется в неспециальной литературе.

8.5.1. Близкая идея в конечном случае. Запись числа состоит из нулей и единиц. Любой фрагмент «10» числа заменяют на «0001». Докажите, что рано или поздно заменять будет нечего.

8.5.2. Идея компактности. (а) Известно, что человечество живёт вечно, а число людей в каждом поколении конечно. Докажите, что найдётся бесконечная цепочка наследников.

(b) В бесконечном парламенте у каждого парламентария не более трёх врагов. Докажите, что парламент можно разбить на две палаты так, что у каждого парламентария будет не более одного врага в своей палате. (Для конечного парламента эта задача разбивается в [SZ, задача 7 в п. «Полуинварианты»].)

(с) Известно, что любую *конечную* карту на плоскости можно правильно раскрасить в 4 цвета. Докажите, что тогда *произвольную* карту на плоскости также можно правильно раскрасить в 4 цвета. (Страны можно считать многоугольниками. Раскраска называется *правильной*, если любые две страны с общим участком границы раскрашены в разные цвета.)

(d) (Загадка.) Прочитайте [SZ, п. «Полуинварианты»]. Какие утверждения верны для бесконечных множеств, а какие нет?

8.5.3. Для любых M и k найдётся достаточно большое v с таким свойством: если все рёбра полного графа с v вершинами покрашены в M цветов, то найдётся полный подграф с k вершинами, все рёбра которого покрашены в один цвет.

8.5.4. Из любой бесконечной последовательности целых чисел можно выбрать подпоследовательность либо так, чтобы каждый её член делился на предыдущий, либо так, чтобы ни один член не делился на другой.

9 К алгоритмам решения алгебраических уравнений

Listeners are prepared to accept unstated (but hinted) generalizations much more than they are able ... to decode a precisely stated abstraction and to re-invent the special cases that motivated it in the first place.

P. Halmos, How to talk mathematics.

9.1 Введение и формулировки результатов

9.1.1 О чём этот параграф

Знаменитые теоремы Гаусса 9.1.5, Руффини 9.2.6, Абеля, Галуа 9.1.12, 9.1.13 и Кронекера о построимости правильных многоугольников и о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений).

Определения построимости и разрешимости в радикалах, а также формулировки указанных теорем, приведены в п. 9.1.2–9.1.4. Я не привожу историю этих теорем, направляя заинтересованного читателя к текстам [Gi, Gil, Ma].

Основное содержание данного текста — изложение глубоких идей алгебры (точнее, теории Галуа) на красивых простых доказательствах этих теорем, см. п. 9.1.5 и [ZSS, § 27]. Этот текст адресован всем любителям такого изложения: старшеклассникам, студентам, учителям и профессиональным математикам. Приводимые доказательства (п. 9.2.5 и 9.4) интересны тем, что для их понимания достаточно уметь доказывать иррациональность (п. 4.1), делить многочлены с остатком (п. 4.3 и задачи 4.4.3, 4.4.4), извлекать корни из комплексных чисел (задача 4.5.4), умножать перестановки (п. 5.1) и решать системы линейных уравнений. (Для каждого одного доказательства необходима только часть этих умений.) Напомним, что несмотря на простоту этих доказательств, они иллюстрируют глубокие идеи алгебры. Разбор доказательств (или их начала) полезен для закрепления тем «иррациональность», «многочлены», «комплексные числа», «перестановки» и «основы линейной алгебры».

И тот, кто не дойдёт до полного доказательства основных результатов, получит хороший опыт по этим темам и даже сможет порешать задачи для исследования, см. п. 9.1.5 и [E2, Es, AB, Ko17, Saf] и ссылки в этих работах.

Перед доказательствами неразрешимости алгебраических уравнений мы разберем общий способ их решения — метод резольвент Лагранжа (п. 9.2). Идея Абеля и Галуа фактически заключается в том, что если уравнение разрешимо в радикалах, то его можно решить этим методом. Эта идея формализуется критерием 9.2.12.а Галуа разрешимости уравнения. Этим же методом строятся и алгоритмы — распознаваемости разрешимости уравнений в радикалах и решения в радикалах разрешимого уравнения.

Для практики приближённые методы вычисления тригонометрических функций и решения уравнений полезнее радикальных формул. Кроме того, уравнения можно решать при помощи трансцендентных функций (см. метод Виета в п. 4.2 и [PSo]; о развитии этих идей рассказывается, например, в [Sk10]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

О новизне. Приводимые доказательства не претендуют на новизну, хотя в этом тексте имеется много методических находок, см. п. 9.1.5 и 9.1.6. Однако, к сожалению, они малоизвестны. Как следствие, малоизвестно, что не только решать квадратные и кубические уравнения, но и доказывать указанные теоремы экономнее не строя и затем применяя теорию Галуа (как, например, в стандартных учебниках по алгебре, [Kh13, Kir]), а напрямую (см. ссылки в п. 9.1.6)— но при этом, конечно, открывая и используя базовые идеи этой теории.

План параграфа. Этот параграф не обязательно изучать подряд. Например, начать его изучение можно не с п. 9.1, а с решения задач в п. 9.2, 9.3, поскольку большинство из них использует предыдущий материал только в качестве мотивировки. Читатель может выбрать удобную ему последовательность изучения (или вовсе опустить некоторые пункты) на основании приводимого плана.

В п. 9.1.2–9.1.4 приведены формулировки основных результатов. Следующие три пункта введения независимы от остального текста

(т.е. они не используются в остальном тексте и для его изучения достаточно прочитать п. 9.1.2–9.1.4). В п. 9.1.7 приводится переформулировка теоремы Гаусса (упомянутая в п. 9.1.2).

План п. 9.2–9.4 приводится в их начале. Доказательства основных результатов приводятся в п. 9.2.3, 9.2.5 и 9.4. Формально они независимы от задач, подводящих к ним (п. 9.2–9.3).

Благодарности. Благодарю А. Я. Белова-Канеля, И. И. Богданова, Э. Б. Винберга, В. В. Волкова, М. Н. Вялого, А. С. Голованова, П. А. Дергача, Д. Зунга, А. Л. Канунникова, В. А. Клепцына, П. А. Козлова, Г. А. Мерзона, А. А. Пахарева, В. В. Прасолова, А. Д. Руховича, Л. М. Самойлова, М. Б. Скопенкова, Г. Р. Челнокова, Л. Э. Шабанова и В. В. Шувалова за полезные обсуждения. Этот текст основан на занятиях в Московской выездной школе по математике, на Летней Конференции Турнира Городов [ABG, ECG], в кружках «Математический семинар» и «Олимпиады и математика».

9.1.2 Построимость (1)

Замечание 9.1.1. Известно, что

$$\begin{aligned} \cos \frac{2\pi}{3} = -\frac{1}{2}, \quad \cos \frac{2\pi}{4} = 0, \quad \cos \frac{2\pi}{5} = \frac{\sqrt{5}-1}{4}, \quad \cos \frac{2\pi}{6} = \frac{1}{2}, \\ \cos \frac{2\pi}{8} = \frac{1}{\sqrt{2}}, \quad \cos \frac{2\pi}{10} = \frac{\sqrt{5}+1}{4}, \quad \cos \frac{2\pi}{12} = \frac{\sqrt{3}}{2}. \end{aligned}$$

А для каких еще n число $\cos \frac{2\pi}{n}$ выражается аналогичной формулой? Т.е. для каких n его можно получить на калькуляторе, выполняящем только четыре арифметических действия и извлечения квадратных корней?

Вещественное число называется **вещественно построимым**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству M , содержащему числа x, y ,

чисел $x + y, x - y, xy$, числа x/y при $y \neq 0$ и числа $\sqrt{x}$ при $x > 0$.

Или если это число можно получить на калькуляторе из замечания 9.1.1.

Например, вещественно построимы числа

$$\sqrt[4]{2} = \sqrt{\sqrt{2}}, \quad \sqrt{2\sqrt{3}}, \quad \sqrt{2} + \sqrt{3}, \quad \sqrt{1 + \sqrt{2}}, \quad 1 + \sqrt{3 - 2\sqrt{2}}, \quad \frac{1}{1 + \sqrt{2}},$$

числа из замечания 9.1.1 и утверждения 9.1.3.

Вещественная построимость числа равносильна его *построимости циркулем и линейкой*. Поэтому приводимые ниже результаты решают знаменитые проблемы древности о построимости циркулем и линейкой. Мы обсудим эту равносильность в п. 9.1.7; впрочем, она не используется в остальном тексте. Изучение вещественной построимости важно также как пробная задача современных теорий символьных вычислений и сложности вычислений [Ko17].

Теорема 9.1.2. Число $\sqrt[3]{2}$ не является вещественно построимым.

См. доказательство в п. 9.4.4.

Вопрос об обобщении формул из замечания 9.1.1 формализуется так: для каких n число $\cos(2\pi/n)$ вещественно построимо?

9.1.3. Число $\cos(2\pi/n)$ вещественно построимо для $n = 15, 16, 20, 24, 60$.

Лемма 9.1.4 (об умножении; вещественная версия). (a) Если число $\cos(2\pi/n)$ вещественно построимо, то число $\cos(\pi/n)$ вещественно построимо.

(b) Если числа $\cos(2\pi/n)$ и $\cos(2\pi/m)$ вещественно построимы и m, n взаимно просты, то число $\cos(2\pi/mn)$ вещественно построимо.

Теорема 9.1.5 (Гаусс). Число $\cos(2\pi/n)$ вещественно построимо тогда и только тогда, когда $n = 2^\alpha p_1 \cdot \dots \cdot p_l$, где $p_1, \dots, p_l$ — различные простые числа вида $2^{2^s} + 1$.

Построимость в теореме Гаусса доказана в п. 9.2.3 и 9.2.5 (или п. 9.2.6), а непостроимость — в п. 9.4.4.

Строго говоря, теорема Гаусса не даёт настоящего решения проблемы вещественной построимости числа $\cos(2\pi/n)$, поскольку неизвестно, какие числа вида $2^{2^s} + 1$ являются простыми. Однако теорема Гаусса даёт, например, быстрый алгоритм распознавания построимости.

Из теоремы Гаусса вытекает вещественная непостроимость числа $\cos(2\pi/9)$ (впрочем, ее проще доказать напрямую, см. задачу 9.3.14.а). Отсюда вытекает следующий результат, показывающий *невозможность трисекции угла циркулем и линейкой*.

Теорема 9.1.6. Существует такое α (например, $\alpha = 2\pi/3$), что число $\cos \alpha$ вещественно построимо, а число $\cos(\alpha/3)$ — нет.

9.1.3 Неразрешимость в вещественных радикалах (2)

Вещественное число называется **вещественно радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней из положительных чисел. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству $M \subset \mathbb{R}$, содержащему числа x, y ,

чисел $x + y, x - y, xy$, числа x/y при $y \neq 0$

и числа $\sqrt[n]{x}$ при $x > 0$ и целом $n > 0$.

Это определение можно сформулировать и на языке калькулятора аналогично замечанию 9.1.1. Стандартный термин: число лежит в некотором вещественном радикальном расширении поля $\mathbb{Q}$. Вещественная радикальность числа α равносильна существованию таких

- целых положительных чисел $s, k_1, \dots, k_s$,
- вещественных чисел $f_1, \dots, f_s$ и многочленов $p_0, p_1, \dots, p_s$ от $0, 1, \dots, s$ переменных, соответственно, с рациональными коэффи-

циентами, что

$$\begin{cases} f_1^{k_1} = p_0 \\ f_2^{k_2} = p_1(f_1) \\ \dots \\ f_s^{k_s} = p_{s-1}(f_1, \dots, f_{s-1}) \\ \alpha = p_s(f_1, \dots, f_s) \end{cases}.$$

Замечание 9.1.7. (а) Любой вещественный корень квадратного уравнения с рациональными коэффициентами вещественно радикален.

(b) Уравнение $x^3 + x + 1 = 0$ имеет ровно один вещественный корень, который вещественно радикален (п. 4.2), см. также задачу 9.2.7 (с).

(с) Уравнение $x^4 + 4x - 1 = 0$ имеет два вещественных корня, каждый из которых вещественно радикален (задача 4.2.6.b), см. также задачу 9.2.10 (d).

(d) Любое вещественно построенное число (п. 9.1.2) вещественно радикально.

(е) Существует многочлен 3-й степени с рациональными коэффициентами (например, $x^3 - 3x + 1$), ни один из корней которого не является вещественно радикальным. (Это доказано в п. (f).)

(f) Число $\cos(2\pi/9)$ не является вещественно радикальным.

Действительно, по формуле 4.1.5 (е) косинуса тройного угла каждое из чисел $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ удовлетворяет уравнению $8y^3 - 6y + 1 = 0$. По нижеприведенной теореме 9.1.8 ни одно из них не является вещественно радикальным.

(g) Трисекция угла невозможна при помощи вещественных радикалов, т.е. существует такое α (например, $\alpha = 2\pi/3$), что число $\cos \alpha$ вещественно радикально, а число $\cos(\alpha/3)$ — нет. (Это следует из п. (f).)

Теорема 9.1.8 (о разрешимости в вещественных радикалах). Следующие условия на многочлен f третьей степени с рациональными коэффициентами равносильны:

(i) многочлен f имеет либо хотя бы один рациональный корень, либо ровно один вещественный корень;

- (ii) многочлен f имеет вещественно радикальный корень;
- (iii) все вещественные корни многочлена f вещественно радикальны.

Единственность вещественного корня «укороченного» уравнения $x^3 + px + q = 0$ равносильна условию « $p = q = 0$ или $(p/3)^3 + (q/2)^2 > 0$ », см. задачу 8.1.4 (d).

Равносильность (ii) $\Leftrightarrow$ (iii) очевидна, ср. с замечанием 9.1.7.а. Разрешимость в теореме 9.1.8 (т.е. (i) $\Rightarrow$ (ii)) доказывается *методом дель Ферро*, см. теоремы, приведённые в указаниях к задачам 4.2.4 и 8.1.4 (d); см. другое доказательство в п. 9.2.2. Неразрешимость в теореме 9.1.8 (т.е. (ii) $\Rightarrow$ (i)) доказывается сложнее, см п. 9.4.5. Более просто доказывается аналогичный результат о *неразрешимости в многочленах*, см. п. 9.3.5 и п. 9.4.2.

Замечание 9.1.9. Из неразрешимости в теореме 9.1.8 тривиально следует, что *для любого $n \geq 3$ существует многочлен n -й степени, один из корней которого не является вещественно радикальным*. Более сложно доказывается аналог этого утверждения с заменой слов «один из корней» на «ни один из корней», см. теорему 9.1.10 ниже. При этом корни *некоторых* уравнений высоких степеней (например, $x^5 = 2$) вполне могут быть вещественно радикальны, см. также п. 9.2.5.

Многочлен с коэффициентами в F называется *неприводимым* над множеством F , если он не раскладывается в произведение многочленов меньшей степени с коэффициентами в F .

Теорема 9.1.10. Если многочлен простой нечётной степени с рациональными коэффициентами неприводим над $\mathbb{Q}$ и имеет более одного вещественного корня, то ни один из его корней не является вещественно радикальным.

Это вещественный аналог теоремы Кронекера 9.1.14. Доказательство приведено в п. 9.4.8.

Гипотеза 9.1.11.* (a) Каждый вещественный корень неприводимого над $\mathbb{Q}$ многочлена четвёртой степени с рациональными коэффициентами вещественно радикален тогда и только тогда, когда хотя

бы один корень его кубической резольвенты (определенной после задачи 4.2.6.b) вещественно радикален. (Ср. с задачей 9.3.13.d.)

(b) Если число $\cos(2\pi/n)$ вещественно радикально, то оно вещественно построимо. (Ср. с теоремой Гаусса 9.1.5 о построимости правильных многоугольников.)

Возможно, справедливость этих гипотез известна специалистам. Гипотезу 9.1.11.b (и ответ к задаче 9.3.3 с набросками доказательств) мне сообщил А. А. Канунников. Читатель может попробовать доказать эти гипотезы после изучения §9.3 и §9.4.

9.1.4 Неразрешимость в комплексных радикалах (2)

Перейдём к формулам, которые могут содержать комплексные числа. Оказывается, кубическое уравнение (например, $x^3 - 3x + 1$), неразрешимое в вещественных радикалах, разрешимо в комплексных.

Комплексное число называется (комплексно) **радикальным**, если его можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений корней целых положительных степеней. Т.е. если некоторое множество, его содержащее, можно получить из множества $\{1\}$, используя операции добавления к уже имеющемуся множеству M , содержащему числа x, y ,

$$\text{чисел } x + y, x - y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

и любого такого числа $r \in \mathbb{C}$, что $r^n = x$ для некоторого целого $n > 0$.

Это определение можно сформулировать и на языке калькулятора аналогично замечанию 9.1.1. (Правда, калькулятор будет необычный: он оперирует с комплексными числами и при нажатии кнопки $\sqrt[n]{}$ выдаёт все значения корня.) Стандартный термин: число лежит в некотором радикальном расширении поля $\mathbb{Q}$.

Например, любой (комплексный) корень квадратного уравнения с рациональными коэффициентами является радикальным. Аналогичные утверждения справедливы для уравнений 3-й и 4-й степени. Они доказываются *методами дель Ферро и Феррари*, см. теоремы,

приведённые в указаниях к задачам 4.2.4 и 4.2.7; см. другое доказательство в п. 9.2.2.³ Однако аналог этих утверждений для более высоких степеней неверен.

Теорема 9.1.12 (Галуа). Существует уравнение 5-й степени с рациональными коэффициентами (например, $x^5 - 4x + 2 = 0$), ни один из корней которого не является радикальным.

Знаменитую проблему о разрешимости уравнений в радикалах решили доказанные немного ранее более слабые теоремы Руффини–Абеля. Теорема Руффини 9.2.6 сложнее формулируется, но подводит нас к доказательству теоремы Галуа. Четкая формулировка теоремы Абеля еще более сложна и здесь не приводится, см. [Sk15, Замечание 7]. Экономнее решить проблему разрешимости, доказав (в п. ??) следующую теорему Галуа (более слабую и более просто доказываемую, чем теорема Галуа 9.1.12). Для $X \subset \mathbb{C}$ комплексное число называется *X-радикальным*, если его можно получить из множества $X \cup \{1\}$ при помощи операций из определения радикальности.

Теорема 9.1.13. Существуют такие $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$, что ни один корень уравнения $x^5 + a_4x^4 + \dots + a_1x + a_0 = 0$ не является $\{1, a_0, a_1, a_2, a_3, a_4\}$ -радикальным.

Analogous result (with analogous proof) holds for equations of any degree $n \geq 5$.

А более сильная теорема Галуа 9.1.12 вытекает из следующего результата.

Теорема 9.1.14 (Кронекер). Если многочлен простой степени с рациональными коэффициентами неприводим над $\mathbb{Q}$, имеет более одного вещественного корня и хотя бы один невещественный, то ни один из его корней не является радикальным.

Эта теорема интересна и нетривиальна даже для многочлена пятой степени. Она доказана в п. 9.4.7. Для её доказательства необходимо следующее обобщение теоремы Гаусса 9.1.5. Обозначим

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

³Об оценках на количество необходимых корней см. п. 9.3.9 и [ABG].

Теорема 9.1.15 (Гаусса о понижении). (а) Если q простое, то можно получить ε_q при помощи операций из определения радикальности так, чтобы корни извлекались только $(q-1)$ -й степени.

(б) Для любого q можно получить ε_q при помощи операций из определения радикальности так, чтобы корни извлекались только степеней, строго меньших q .

Часть (а) доказывается аналогично доказательству построимости в теореме Гаусса (п. 9.2.5, 9.2.6). Часть (б) выводится из (а) при помощи индукции по q . (Если $q = ab$ для некоторых целых a, b , $0 < a, b < q$, то шаг индукции следует из равенства $\varepsilon_q = \sqrt[a]{\varepsilon_b}$. Если же q простое, то шаг индукции следует из части (а).)

Справедлив комплексный аналог замечания 9.1.9 для $n \geq 5$ и теоремы Кронекера 9.1.14 вместо теоремы 9.1.10. При этом доказательство теоремы 9.1.13 легко переносится на уравнения любой степени $n \geq 5$.

Теорема 9.1.16. There is an algorithm deciding, for $a_{n-1}, \dots, a_0 \in \mathbb{Q}$, whether all the roots of the equation $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ are expressible by radicals.

Theorem 9.1.16 can be proved using Galois Solvability Criterion 9.2.12.a and an estimation 9.3.46.b of the number of operations.

9.1.5 Чем интересны приводимые доказательства

Приводимые доказательства намного проще и короче тех, которые излагаются в стандартных учебниках по алгебре. (Здесь я имею в виду доказательство «с нуля», а не вывод нужной теоремы из построенной перед этим теории, в которой фактически заключается всё доказательство.) Сравнение с доказательствами из менее стандартной более популярной литературы приведено в п. 9.1.6.

Эта простота достигается благодаря тому, что, в отличие от большинства учебников, приводимые доказательства не используют термина «группа Галуа» (даже термина «группа»). Несмотря на отсутствие этих *терминов, идеи* приводимых доказательств являются *отправными* для теории Галуа и *конструктивной теории Галуа* [E2]. Более подробно это обсуждается в [ZSS, §27 и §28].

Доказательство разрешимости основано на методе *резольвент Лагранжа*. Доказательства неразрешимости основаны на идеях *симметрии* и *сопряжения*. (Вторая идея более учёно называется идеей *автоморфизма поля*; замечательное изложение см. в [Vag].)

Основные идеи представлены на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей, и со сведением научного языка к необходимому минимуму. Хотя основные результаты касаются уравнений высших степеней, идеи демонстрируются на квадратных и кубических уравнениях. Неразрешимость доказывается сначала при условии, что *корень извлекался только один раз* (в задачах в п. 9.3.1, 9.3.3, 9.3.4). Благодаря этому основные идеи преподносятся на примере рациональных чисел (а не произвольных полей и даже не полей из башни расширений). Эти основные идеи (сопряжения, поля и другие) заключены в леммах о калькуляторе, о линейной независимости и о сопряжении (§9.3 и 9.4). При доказательстве неразрешимости в теореме Гаусса 9.1.5 используется степень *многочлена* (вместо степени *расширения поля*) Перед доказательствами неразрешимости (в теоремах 9.1.12, 9.1.13, 9.1.14 Галуа и Кронекера) доказывается неразрешимость в *многочленах* (теоремы Руффини 9.2.6, ??), а также неразрешимость в *вещественных* радикалах уравнений третьей степени (теорема 9.1.8). Важные идеи доказательств явно выделены в виде четко сформулированных на простом языке лемм (о сохранении четносимметричности 9.3.36, ??, о степенях двойки 9.4.4, о рационализации ??). Все это делает доказательства неразрешимости более доступными (за счёт введения интересных чётко выделенных промежуточных «ступенек»). Кроме того, это подводит читателя к предположению о том, что приведённые доказательства можно развить до теории (Галуа), полезной для доказательства других интересных результатов (подробнее см. [ZSS, п. 28.2]).

Мы показываем, *как можно придумать* приводимые доказательства. Пути к ним намечены в виде задач в п. 9.2.4 и 9.3. О традиции изучения материала в виде решения и обсуждения задач см. п. 1.2 и [ZSS, §26]. Хотя *придумать* доказательства непросто, *изложить* их можно коротко (см. п. 9.2.5 и 9.4). Освобождение доказательства от деталей, возникших при его придумывании, но не

нужных для него самого, — важная часть его проверки.

Многие из приведённых задач — хорошие темы исследовательских работ старшеклассников и младшекурсников, связанные с алгеброй, комбинаторикой и информатикой, см. п. 1.3. Вот работы, уже подготовленные с использованием предыдущих версий этого текста: [Saf, AB, Ko17]. А вот примеры задач для исследования: 9.1.11, 9.2.11, 9.2.12, 9.3.3, 9.1.8, 9.1.10, 9.2.11, 9.2.15, 9.3.5, 9.3.9 (h), 9.3.17 (e), 9.3.19 (b), 9.3.21 (d), 9.3.25, 9.3.39, 9.3.41, 9.3.42, 9.2.2, 9.2.5, 9.2.6, 9.3.33, 9.3.38, 9.3.44–9.3.46.

9.1.6 Исторические комментарии

Доказательство построимости в теореме Гаусса получено из [E1, § 24] некоторым упрощением (мы обходим использование леммы 2, см. подробнее абзац перед задачей 9.2.17). Оно также более простое по сравнению с доказательством из [KS]. Элементарное доказательство построимости для $n = 17$ приводится, например, в [BK, Ch, Gi, Pr07-2, Pos, PSo, Kol], [Dor, § 37] (при этом иногда приводятся явные формулы, как с доказательствами утверждений о знаках перед радикалами [Dor, § 37], [Saf], так и без [BK]). Для общего случая оно намечено в [Ga, Gi] (где ясности доказательства немного мешает построение общей теории вместо доказательства конкретного результата). Подход из [Ki] даёт ответ на вопрос «почему», и было бы интересно довести его до полного доказательства.

Доказательство непостроимости в теореме Гаусса основано на [Dor, Supplement to § 35–37]. Оно более простое по сравнению с доказательствами из [KS].

Мне неизвестно, опубликовано ли короткое прямое доказательство теорем 9.1.8, 9.1.10 о неразрешимости в вещественных радикалах. Доказательство теоремы Руффини 9.2.6, ?? следует приведенному в замечательной книге [Kol] (я не смог разобрать приведенного там доказательства, пока не переоткрыл его, явно выделив лемму о сохранении четносимметричности 9.3.36, ??). Доказательство теоремы 9.1.13 следует приведенному в замечательной книге [PSo] (я смог убедиться в правильности предложенных там идей только переписав доказательство, явно выделив лемму о рационализации ??). Другое доказательство теоремы Абеля приведено в [Al], [FT,

Lecture 5], [Sk11]⁴. Доказательство теоремы Кронекера 9.1.14 основано на замечательных статье [T] и книгах [Dor, § 25], [Pr07-2, дополнение 8] (здесь исправлены неточности, см. сноски ?? и 12).

Другие элементарные изложения приводятся, например, в [Ber, Br, Had, Vi, Ka, Ler, Pe, Ro, St94]. Note that proofs in some of these sources are incomplete, see [Sk15, Discussion].

Вышеупомянутые элементарные изложения были для меня полезнее (несмотря на указанные недостатки), чем формальные изложения (в стандартных учебниках, излагающих теории), которые начинаются с нескольких сотен страниц определений и следствий, роль которых в доказательстве теоремы о неразрешимости неясна на момент их формулировки.

9.1.7 Связь с построениями циркулем и линейкой (1)

9.1.17. (a) Используя отрезки длины x и y , можно построить с помощью циркуля и линейки отрезок длины $\sqrt{3xy + y^4 xy^3}$.

(b) Используя отрезки длины a , b и c , можно построить с помощью циркуля и линейки отрезки длины $a + b$, $a - b$, ab/c , $\sqrt{ab}$.

Ввиду утверждения 9.1.17.b если на плоскости задан отрезок длины 1, то отрезок вещественно построимой длины можно построить циркулем и линейкой. Этот простой результат был известен ещё древним грекам. Оказывается, верно и обратное.

Теорема 9.1.18 (Основная теорема о построениях циркулем и линейкой). Если отрезок длины a можно построить циркулем и линейкой, имея отрезок длины 1, то число a вещественно построимо.

Этот несложный результат (доказанный лишь в XIX веке) показывает, что из непостроимости числа $\cos(2\pi/n)$ вытекает непостроимость правильного n -угольника циркулем и линейкой. Для доказательства этого результата можно рассмотреть все возможные случаи появления новых объектов (точек, прямых, окружностей)

⁴Доказательство из [Al] более коротко и понятно изложено в [FT, Lecture 5] и, возможно, в [Sk11]. Большая часть [Al] посвящена изложению теории, не нужной для доказательства теоремы Абеля. Однако автору книги [Al] удалось избежать немотивированного изложения части этой теории.

9.2 Решаем уравнения: метод резольвент Лагранжа

Метод резольвент Лагранжа на простейших примерах иллюстрируется в п. 9.2.2. Его применение к доказательству построимости в теореме Гаусса иллюстрируется на примерах и задачах в п. 9.2.4. Построимость в теореме Гаусса доказана в п. 9.2.3 и п. 9.2.5. При этом в п. 9.2.3 приводится более простая часть доказательства, не использующая резольвент Лагранжа; этот пункт не зависит от предыдущих. Материал п. 9.2.6 не используется далее.

Определение вещественной построимости и радикальности чисел см. в п. 9.1.2, 9.1.4. In this section equality signs involving polynomial f (or f_j) mean equality of polynomials (покоэффициентное). Напомним, что

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

9.2.1 Определение радикальности многочлена (2)

Всегда ли можно, зная $x + y$ и xy , однозначно найти x ? Вот простейшая формализация этого вопроса: *существует ли функция $q: \mathbb{R}^2 \rightarrow \mathbb{R}$, для которой $q(x + y, xy) = x$ при любых $x, y \in \mathbb{R}$?* (Т.е. разрешимо ли функциональное уравнение $q(x + y, xy) = x$?) Ответ: не существует (действительно, рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$).

Аналогично, зная

$$\sigma_1 := x + y + z, \quad \sigma_2 := xy + yz + zx \quad \text{и} \quad \sigma_3 := xyz,$$

невозможно однозначно найти $(x - y)(y - z)(z - x)$ (действительно, рассмотрите тройки $x = 1, y = 2, z = 3$ и $x = 2, y = 1, z = 3$).

9.2.1. (2), (3), (k) Для каких k разрешима следующая система функциональных уравнений

$$\begin{cases} f^k(x, y) = p(x + y, xy) \\ x = q(x + y, xy, f(x, y)) \end{cases} \quad ?$$

9.2.2. (3), (2), (k) Для каких k разрешима следующая система функциональных уравнений

$$\begin{cases} f^k(x, y, z) = p(\sigma_1, \sigma_2, \sigma_3) \\ x = q(\sigma_1, \sigma_2, \sigma_3, f(x, y, z)) \end{cases} \quad ?$$

9.2.3. Система функциональных уравнений

$$\begin{cases} f_1^2 = p_0(\sigma_1, \sigma_2, \sigma_3) \\ f_2^3 = p_1(\sigma_1, \sigma_2, \sigma_3, f_1) \\ x = p_2(\sigma_1, \sigma_2, \sigma_3, f_1, f_2) \end{cases}$$

- (а) неразрешима в вещественных функциях $\mathbb{R}^n \rightarrow \mathbb{R}$;
 (б) разрешима в комплексных функциях $\mathbb{C}^n \rightarrow \mathbb{C}$ и даже в многочленах с комплексными коэффициентами. (Подсказкой являются следующие задачи 9.2.8.а и 9.2.9.с. См. решение в п. 9.2.2.)

Обобщение вышеприведенных задач на любое количество шагов формализуется следующим определением радикальности.

Обозначим элементарные симметрические многочлены

$$\sigma_1(x_1, \dots, x_n) := x_1 + \dots + x_n, \quad \dots, \quad \sigma_n(x_1, \dots, x_n) = x_1 \cdot \dots \cdot x_n.$$

Если число n и аргументы $x_1, \dots, x_n$ ясны из контекста, то они пропускаются из обозначений.

Многочлен $p \in \mathbb{R}[x_1, \dots, x_n]$ называется **вещественно радикальным** (или выразимым в вещественных радикалах), если p можно добавить в набор $\{\sigma_1, \dots, \sigma_n\} \cup \mathbb{R}$ многочленов цепочкой операций следующего вида:

- добавить в набор сумму или произведение уже имеющихся многочленов;
- если многочлен из набора равен f^k для некоторых $f \in \mathbb{R}[x_1, \dots, x_n]$ и целого $k > 1$, то добавить в набор многочлен f .

Замечание 9.2.4. (а) Например, к многочленам $x^2 + 2y$ и $x - y^3$ операциями первого типа можно добавить многочлен $-5(x^2 + 2y)^2 + 3(x^2 + 2y)(x - y^3)^6$. А к многочлену $x^2 - 2xy + y^2$ операцией второго типа можно добавить многочлен $x - y$ (или $y - x$).

(б) Операции первого типа добавляют многочлен с вещественными коэффициентами от уже имеющихся.

(с) Радикальность многочлена x_1 равносильна существованию таких

- целых положительных чисел $s, k_1, \dots, k_s$,

• многочленов $f_1, \dots, f_s$ от n переменных и $p_0, p_1, \dots, p_s$ от $n, n+1, \dots, n+s$ переменных, соответственно, с вещественными коэффициентами, что

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \dots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \dots, \sigma_n, f_1) \\ \dots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \dots, \sigma_n, f_1, \dots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \dots, \sigma_n, f_1, \dots, f_s) \end{cases}.$$

В этих равенствах мы опускаем переменные $(x_1, \dots, x_n)$ многочленов $\sigma_1, \dots, \sigma_n, f_1, \dots, f_s$.

(d) Примеры в начале пункта показывают, что радикальность многочлена не дает его «выразимости» в указанном там смысле.

(e) По теореме Виета $\sigma_1, \dots, \sigma_n$ есть коэффициенты многочлена

$$t^n - \sigma_1 t^{n-1} + \dots + (-1)^{n-1} \sigma_{n-1} t + (-1)^n \sigma_n \in \mathbb{C}[x_1, \dots, x_n][t]$$

с корнями $x_1, \dots, x_n$. Поэтому радикальность многочлена x_1 означает выразимость в радикалах (в указанном в определении радикальности смысле) корня многочлена через его коэффициенты.

Решение задачи 9.2.1.(2) показывает, что многочлен x вещественно радикален для $n = 2$.

Теорема 9.2.5. Многочлен x не является вещественно радикальным для $n = 3$.

Теорема 9.2.5 есть еще одна формализация того, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*, ср. с замечанием 9.1.7.e.

Определение (комплексной) **радикальности** получается из его вещественного аналога заменой вещественных коэффициентов на комплексные. Решения задач 9.2.1.(2), 9.2.3.b и 9.2.10.d показывают, что многочлен x_1 радикален для $n \leq 4$.

Теорема 9.2.6 (Руффини). Ни для какого целого $n \geq 5$ многочлен x_1 не радикален.

Из доказательства будет вытекать, что даже многочлен $x_1 x_2 + x_2 x_3 + x_3 x_4 + x_4 x_5 + x_5 x_1$ не радикален для $n = 5$.

Указания, ответы и решения

9.2.1. (2) Решение квадратного уравнения $t^2 + bt + c = 0$ можно выразить формулами

$$(x-y)^2 = (x+y)^2 - 4xy = b^2 - 4c \quad \text{и} \quad x = \frac{x+y+(x-y)}{2} = \frac{-b+(x-y)}{2}.$$

Поэтому системе уравнений удовлетворяют, например, многочлены

$$f(x, y) = x - y, \quad p(u, v) = u^2 - 4v \quad \text{и} \quad q(u, v, w) = \frac{u + w}{2}.$$

(3) Подставьте $(x, y) = (1, 2)$ и $(x, y) = (2, 1)$.

9.2.5. При $n = 3$ множество вещественно радикальных многочленов содержится в множестве циклически симметрических многочленов. Это утверждение доказывается при помощи индукции по количеству операций из определения радикальности. Шаг индукции вытекает из леммы 9.3.31 о сохранении циклической симметричности.

Поскольку многочлен x не является циклически симметрическим, то он не является вещественно радикальным.

9.2.2 Решение уравнений малых степеней (2)

9.2.7. Следующие многочлены вещественно радикальны для $n = 3$

$$(a) (x-y)(y-z)(z-x); \quad (b) x^9y + y^9z + z^9x.$$

В задаче 9.2.7 и далее используйте основную теорему о симметрических многочленах 4.6.3.

9.2.8. Многочлен $f \in \mathbb{R}[u_1, u_2, \dots, u_n]$ называется **циклически симметрическим**, если $f(u_1, u_2, \dots, u_n) = f(u_2, u_3, \dots, u_{n-1}, u_n, u_1)$.

(а) Найдите хотя бы одну пару $\alpha, \beta \in \mathbb{C}$, для которой многочлен $(u + v\alpha + w\beta)^3$ циклически симметрический, а многочлен $u + v\alpha + w\beta$ — нет.

(б) Получите многочлен $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ операциями из определения радикальности из некоторых *циклически симметрических* многочленов от $x_1, x_2, \dots, x_{10}$.

9.2.9. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

$$(a) \quad \begin{cases} x + y + z + t = a, \\ x + y - z - t = b, \\ x - y + z - t = c, \\ x - y - z + t = d; \end{cases} \quad (b) \quad \begin{cases} x + y + z + t = a, \\ x + iy - z - it = b, \\ x - y + z - t = c, \\ x - iy - z + it = d; \end{cases}$$

$$(c) \quad \begin{cases} x + y + z = a, \\ x + \varepsilon_3 y + \varepsilon_3^2 z = b, \\ x + \varepsilon_3^2 y + \varepsilon_3 z = c. \end{cases}$$

9.2.10. Какие из следующих многочленов радикальны для $n = 4$?

- (a) $(x - y)(x - z)(x - t)(y - z)(y - t)(z - t)$;
 (b) $xy + zt$; (c) $x + y - z - t$; (d) x .

Выражения из задачи 9.2.9 называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в следующем смысле.

Решение кубического уравнения при помощи резольвент Лагранжа (доказательство утверждения 9.2.3 (b)). Для нахождения корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 9.2.9 (c). (Заметим, что метод дель Ферро из задачи 4.2.2 фактически приводит к тому же.) По теореме Виета $a = a(x, y, z)$ — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлен $b = b(x, y, z)$ переходит в $\varepsilon_3 c$, а $c = c(x, y, z)$ в $\varepsilon_3^2 b$ (проверьте!). Значит, многочлены bc и $b^3 + c^3$ не меняются при этой замене. Аналогично они не меняются при замене $z \leftrightarrow y$. Поэтому многочлены bc и $b^3 + c^3$ *симметрические*, т. е. не меняются при любой перестановке переменных. Тогда из теоремы Виета и теоремы о представимости симметрического многочлена в виде многочлена от элементарных симметрических многочленов (утверждение 4.6.3 (c)) следует, что эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая квадратное уравнение, можно получить b^3 и c^3 . Далее легко получить сами b и c .

Решение уравнения 4-й степени при помощи резольвент Лагранжа (решение задачи 9.2.10. d). Для нахождения корней x, y, z, t уравнения 4-й степени достаточно найти выражения a, b, c, d от корней

из задачи 9.2.9.а. По теореме Виета a — коэффициент уравнения. При замене $x \leftrightarrow y$ многочлены c^2 и d^2 меняются местами, а многочлен b^2 переходит в себя. При циклической замене $x \rightarrow y \rightarrow z \rightarrow t \rightarrow x$ многочлены b^2 и d^2 меняются местами, а многочлен c^2 переходит в себя. Значит, многочлены b^2, c^2, d^2 переставляются при любой перестановке переменных. Поэтому виетовские многочлены от них, т. е.

$$b^2 + c^2 + d^2, \quad b^2c^2 + b^2d^2 + c^2d^2, \quad b^2c^2d^2,$$

симметрические. Тогда эти многочлены от x, y, z представляются в виде многочленов от коэффициентов уравнения. Теперь, решая кубическое уравнение, можно получить сами b^2, c^2, d^2 . Далее легко получить b, c, d .

Ввиду теоремы Руффини 9.2.6 метод резольвент Лагранжа, продемонстрированный на примере решения уравнений 3-й и 4-й степени (задачи 9.2.3 (b) и 9.2.10 (d)), не работает для уравнения 5-й степени. Сообразите, почему!

Обозначим через Σ_q множество перестановок q -элементного множества. For a permutation $\alpha \in \Sigma_q$ denote

$$\vec{u}_\alpha := (u_{\alpha(1)}, \dots, u_{\alpha(q)}).$$

Определим *резольвенту Лагранжа* как

$$t(u_1, \dots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \dots + \varepsilon_q^q u_q.$$

Определим *резольвенту Галуа* как

$$Q(u_1, \dots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \dots, u_q, y].$$

9.2.11. (a) Имеем $Q(\varepsilon_q u_1, \dots, \varepsilon_q u_q, y) = Q(u_1, \dots, u_q, y)$.

(b) Для некоторого $R_Q \in \mathbb{Q}[\varepsilon_q][z]$ имеем $Q(u_1, \dots, u_q, y) = R_Q(u_1, \dots, u_q, y^q)$.

(c) Если $x_1, \dots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ и даже $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[y]$.

Многочлен $R_Q(x_1, \dots, x_5, z) \in \mathbb{Q}[z]$ называется *разрешающим многочленом* для f .

(d)* Все корни разрешающего многочлена для $f(x) = x^5 + 15x + 11$ (а значит, и самого многочлена f) радикальны.

Using (a version of) критерия Галуа разрешимости 9.2.12.a below one can prove that *при $a, b \in \mathbb{R}$ все корни уравнения $x^5 + ax + b = 0$ радикальны тогда и только тогда, когда $a = \frac{15 \pm 20c}{c^2 + 1}$ и $b = \frac{44 \mp 8c}{c^2 + 1}$ для некоторого $c \in \mathbb{Q}$, $c \geq 0$* [PSo].

9.2.12. (a) Критерий Галуа разрешимости (гипотеза). Для любых $a_{n-1}, \dots, a_0 \in \mathbb{Q}$ все корни уравнения $A(x) := x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ радикальны тогда и только тогда, когда некоторый набор многочленов степени 1 с коэффициентами в $\mathbb{Q}$ может быть получен из $\{A\}$ при помощи следующих операций:

- (факторизация) если один из многочленов равен P_1P_2 для некоторых $P_1, P_2 \in \mathbb{Q}[x]$, не являющихся константами, то заменим P_1P_2 на P_1 и P_2 ;
- (извлечение корня) если один из наших многочленов равен $P(x^q)$ для некоторого $P \in \mathbb{Q}[x]$, то заменим $P(x^q)$ на $P(x)$;
- (взятие резольвенты Галуа) заменим один из наших многочленов P на многочлен $Q(y_1, \dots, y_q, y)$, где $y_1, \dots, y_q$ – все корни многочлена P . (По утверждению 9.2.11.c $Q(y_1, \dots, y_q, y) \in \mathbb{Q}[y]$.)

(b) Докажите часть «тогда» критерия (a).

(c) Сформулируйте и докажите вещественный аналог критерия (a).

(d) Сформулируйте и докажите аналог критерия (a) for equations solvable using one radical, cf. [AB, ABG].

(e)* Does the analogue of (a) hold for every $a_{n-1}, \dots, a_0 \in \mathbb{C}$ with ‘expressible by radicals’ replaced by ‘expressible by radicals from $\{1, a_{n-1}, \dots, a_0\}$ ’?

Доказательство части «только тогда» в критерии (a) аналогично теореме 9.1.13, см. также теорему Галуа 9.1.12 и §9.3.9. I would be grateful if a specialist in algebra could confirm that criterion (a) is correct (and is equivalent to the Galois Solvability Criterion in its usual textbook formulation, please give a reference), or describe required changes. (I asked some specialists since July 2017, but so far obtained no answer.)

Указания, ответы и решения

9.2.7. (а) $(x - y)^2(y - z)^2(z - x)^2$ — симметрический многочлен. (Пункт (а) можно также свести к (b).)

(b) Обозначим

$$M = x^9y + y^9z + z^9x \quad \text{и} \quad N = y^9x + x^9z + z^9y.$$

Тогда многочлены $M + N$ и MN симметрические. Значит, они являются многочленами от элементарных симметрических многочленов $\sigma_1, \sigma_2, \sigma_3$. (Конкретное выражение приведено в [ABG].) Само же M выражается через $M + N$ и MN по «формуле корней квадратного уравнения», см. формулы в начале п. 9.2.1.

9.2.8. (а) $x + y\varepsilon_3 + z\varepsilon_3^2$.

(b) Обозначим

$$M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1 \quad \text{и}$$

$$N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2.$$

Далее аналогично задаче 9.2.7.b.

9.2.10. (а) Квадрат $(x - y)^2(x - z)^2(x - t)^2(y - z)^2(y - t)^2(z - t)^2$ симметричен, см. 9.2.7.a.

(b) Положим

$$M = xy + zt, \quad N = xz + yt, \quad K = xt + yz.$$

По утверждению 9.2.3 (b) M «выразим в радикалах при помощи многочленов»

$$M + N + K, \quad MN + MK + NK, \quad MNK.$$

Аналогично решениям задач 9.2.3 (b) выше и 9.2.10.d ниже, эти многочлены симметрические. Поэтому $M = xy + zt$ радикален.

(с) Положим

$$M = (x + y - z - t)^2, \quad N = (x + z - y - t)^2, \quad K = (x + t - y - z)^2.$$

Повторяя решение пункта (b), получим $M = (x + y - z - t)^2$. Теперь легко получить и $x + y - z - t$.

9.2.9. Используйте равенства $1 + \varepsilon + \varepsilon^2 = 0$ и $1 + i + i^2 + i^3 = 0$.

9.2.11. Для наглядности приведем решения при $q = 5$.

(а) Имеем

$$t(\varepsilon_5 \vec{u}_\alpha) = t(u_{\alpha(5)}, u_{\alpha(1)}, u_{\alpha(2)}, u_{\alpha(3)}, u_{\alpha(4)}) = t(\vec{u}_{\alpha \circ (54321)}).$$

Следовательно,

$$\begin{aligned} Q(\varepsilon_5 u_1, \dots, \varepsilon_5 u_5, y) &= \prod_{\alpha \in \Sigma_5} (y - t(\varepsilon_5 \vec{u}_\alpha)) = \\ &= \prod_{\alpha \in \Sigma_5} (y - t(\vec{u}_{\alpha \circ (54321)})) = Q(u_1, \dots, u_5, y). \end{aligned}$$

Здесь

- $(54321) \in \Sigma_5$ – это цикл, который отправляет 5 в 4, 4 в 3, ..., 1 в 5.

- последнее равенство справедливо, потому что когда α пробегает Σ_5 , то же делает и $\alpha \circ (54321)$.

(б) Для каждого $k = 0, 1, 2, \dots, 120$ найдётся однородный многочлен $P_k \in \mathbb{Q}[\varepsilon_5][u_1, \dots, u_5]$ («степени» $120 - k$) такой, что коэффициент при y^k в Q равен $P(u_1, \dots, u_5)$, т.е.

$$Q(u_1, \dots, u_5, y) = \sum_{k=0}^{120} P_k(u_1, \dots, u_5) y^k.$$

По (а) и из однородности имеем

$$P_k(u_1, \dots, u_5) = P_k(\varepsilon_5 u_1, \dots, \varepsilon_5 u_5) = \varepsilon_5^{-k} P_k(u_1, \dots, u_5).$$

Если k не кратно 5, то $P_k(u_1, \dots, u_5) = 0$, что и требовалось.

(с) Многочлен $Q(u_1, \dots, u_5, y)$ симметричен по $u_1, \dots, u_5$. Значит, все коэффициенты (P_k из пункта (б)) соответствующего многочлена из $\mathbb{Q}[\varepsilon_5, u_1, \dots, u_5][y]$ симметричны по $u_1, \dots, u_5$. Теперь $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ ввиду основной теоремы о симметрических многочленах, формул Виета и того факта, что коэффициенты многочлена f рациональны.

Теперь утверждение $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[y]$ доказывается аналогично леммам о рациональности 9.3.18.f and 9.3.22.d.

9.2.12. (б) Это доказывается методом резольвент Лагранжа, разобранным в этом пункте.

9.2.18. (а) Обозначим

$$\beta := \varepsilon_6 = \frac{1 + i\sqrt{3}}{2} \quad \text{и} \quad T(x) := x + \beta x^3 + \beta^2 x^9 + \beta^3 x^{27} + \beta^4 x^{81} + \beta^5 x^{243}.$$

Докажите, что $T(x) \equiv \beta T(x^3) \pmod{x^7 - 1}$.

(b) Обозначим

$$\beta := \varepsilon_{10} \quad \text{и} \quad T(x) := x + \beta x^2 + \beta^2 x^4 + \beta^3 x^8 + \beta^4 x^{16} + \dots + \beta^9 x^{512}.$$

Докажите, что $T(x) \equiv \beta T(x^2) \pmod{x^{11} - 1}$.

Решения задач 9.2.16 (d, e) и 9.2.18 аналогичны приведённому доказательству построимости числа ε_5 . Подробности см. в п. 9.2.5.

9.2.5 Доказательство построимости в теореме Гаусса (3)

Напомним, что формально приводимое доказательство независимо от п. 9.2.4, а из п. 9.2.3 используется только лемма 9.2.14 о комплексификации.

Лемма 9.2.19 (об умножении). (а) Если ε_n построимо, то ε_{2n} построимо.

(b) Если ε_n и ε_m построимы и m, n взаимно просты, то ε_{mn} построимо.

Доказательство получается из формул $\varepsilon_{2n} \in \sqrt{\varepsilon_n}$ и $\varepsilon_{mn} = \varepsilon_m^x \varepsilon_n^y$, где x и y — целые числа, для которых $nx + my = 1$. $\square$

При решении задач 9.2.16 (а) мы использовали различность остатков от деления чисел $2, 2^2, 2^3, 2^4$ на 5. При решении задач 9.2.16 (d, e) и 9.2.18 (а) мы использовали аналогичное свойство чисел 2 и 11, 6 и 17, 3 и 7. Для общего случая необходимо следующее обобщение.

Теорема 9.2.20 (о первообразном корне). Для любого простого p существует число g , для которого остатки от деления на p чисел $g^1, g^2, g^3, \dots, g^{p-1}$ различны.

Указание к доказательству для $p = 2^m + 1$ (только этот случай нужен для теоремы Гаусса). Если первообразного корня нет, то

сравнение $x^{2^{m-1}} \equiv 1 \pmod{p}$ имеет $p - 1 = 2^m > 2^{m-1}$ решений. Это противоречит теореме Безу.

Заинтересованный читатель может получить и полное доказательство, см. п. 3.5.

Доказательство построимости в теореме Гаусса 9.1.5. По лемме 9.2.14 о комплексификации и по лемме 9.2.19 об умножении достаточно доказать, что ε_n построимо для любого простого $n = 2^{2^s} + 1$. Так как $n - 1 = 2^m$, то по лемме 9.2.19 об умножении $\beta := \varepsilon_{n-1}$ построимо. Обозначим

$$\mathbb{Z}[\beta] := \{a_0 + a_1\beta + a_2\beta^2 + \dots + a_{n-2}\beta^{n-2} \mid a_0, \dots, a_{n-2} \in \mathbb{Z}\}.$$

Обозначим через g первообразный корень по модулю n . Для $r = 0, 1, 2, \dots, n - 2$, обозначим

$$T_r(x) := x + \beta^r x^g + \beta^{2r} x^{g^2} + \dots + \beta^{(n-2)r} x^{g^{n-2}} \in \mathbb{Z}[\beta][x].$$

Тогда $(T_0 + T_1 + \dots + T_{n-2})(\varepsilon) = (n - 1)\varepsilon$. Кроме того, $T_0(\varepsilon) = -1$. Поэтому достаточно доказать построимость каждого из чисел $T_r(\varepsilon)$, $r = 1, 2, \dots, n - 2$. Имеем

$$\begin{aligned} \beta^r T_r(x^g) \equiv_{x^n-1} T_r(x) &\implies T_r^{n-1}(x^g) \equiv_{x^n-1} T_r^{n-1}(x) \implies \\ \implies T_r^{n-1}(x^k) &\equiv_{x^n-1} T_r^{n-1}(x) \text{ для любого } k. \end{aligned}$$

Возьмём многочлен $a_0 + a_1x + a_2x^2 + \dots + a_{n-1}x^{n-1}$ с коэффициентами в $\mathbb{Z}[\beta]$, сравнимый с $T_r^{n-1}(x)$ по модулю $x^n - 1$. Тогда $a_1 = a_2 = \dots = a_{n-1}$. Поэтому $T_r^{n-1}(\varepsilon) = a_0 - a_1 \in \mathbb{Z}[\beta]$. Значит, $T_r(\varepsilon)$ построимо. $\square$

9.2.6 Эффективные доказательства построимости (4*)

Здесь приводятся другие доказательства построимости в теореме Гаусса 9.1.5 и теоремы Гаусса о понижении 9.1.15 (а). Они сложнее приведённого в п. 9.2.5, но дают более быстрые алгоритмы вычисления [ВК, Saf, Ko17]. Именно они принадлежат Гауссу.

Эффективное доказательство построимости в теореме Гаусса 9.1.5 для $n = 5$. It suffices to prove that $\varepsilon := \varepsilon_5$ is constructible. Сразу

9.3 Задачи о неразрешимости в радикалах

В этом пункте мы на простых примерах демонстрируем идеи доказательств теорем о неразрешимости из п. 9.1. Этот пункт независим от предыдущего. Более того, он почти независим от п. 9.1, поскольку большинство приводимых здесь задач касается непредставимости чисел в некотором специальном виде и не использует определений и формулировок из п. 9.1. Непредставимость, хоть она и кажется очень естественной, может доказываться нетривиально!

К теореме 9.1.2 и непостроимости в теореме Гаусса 9.1.5 (п. 9.4.4) подводят задачи из п. 9.3.1–9.3.2. К неразрешимости в вещественных радикалах из теоремы 9.1.8 (п. 9.4.5), к теореме 9.1.10 (п. 9.4.8), и к теореме Кронекера 9.1.14 (п. 9.4.7) подводят задачи из п. 9.3.1–9.3.4. К теореме 9.1.13 и неразрешимости в критерии 9.2.12.а (п. 9.4.3 и ??) подводят задачи из п. 9.3.1–9.3.6. К теореме 9.1.16 подводят задачи всего этого пункта, включая п. 9.3.9.

Таким образом, п. 9.3.1–9.3.4 развивают идею сопряжения, а 9.3.7–9.3.9 — идею симметрии. Заметим, что в п. 9.3 эти идеи раскрываются в обратном порядке (поскольку, в противоположность первым шагам, окончательная реализация идеи сопряжения более сложна, чем идеи симметрии).

В этом пункте «многочлен с рациональными коэффициентами» коротко называется *многочленом*. Числа $v_1, \dots, v_n \in \mathbb{C}$ называются *линейно зависимыми над $\mathbb{Q}$* , если найдутся $\lambda_1, \dots, \lambda_n \in \mathbb{Q}$, не все равные нулю, для которых $\lambda_1 v_1 + \dots + \lambda_n v_n = 0$. Напомним, что

$$\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q).$$

9.3.1 Одно извлечение квадратного корня (1-2)

Перед решением задач этого подпункта полезно прорешать п. 4.1.

9.3.1. Представимо ли следующее число в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$:

- (a) $\sqrt{3 + 2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$; (c) $\sqrt[3]{7 + 5\sqrt{2}}$; (d) $\sqrt[3]{2}$;
 (e) $\sqrt{2} + \sqrt[3]{2}$; (f) $\sqrt{2 + \sqrt{2}}$; (g) $\sqrt{2} + \sqrt{3} + \sqrt{5}$.

Задачи 9.3.1 и 9.3.3 интересны в связи с неразрешимостью в радикалах, поскольку нам нужно придумать многочлен, корни ко-

торого не радикальны, а числа из задач 9.3.1 являются корнями многочленов (подумайте, каких). См. также утверждение 7.6.2.

Лемма 9.3.2 (о расширении). Пусть число можно получить из числа 1 при помощи нескольких операций сложений, вычитаний, умножений, делений на ненулевые числа, и одной операции извлечения квадратного корня из положительного числа (т.е. число вещественно построимо с извлечением корня только один раз). Тогда оно имеет вид $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ и $b > 0$.

9.3.3.* Для каких n число $\cos(2\pi/n)$ представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$? В качестве отдельных пунктов засчитываются случаи $n = 16, 24, 20, 15, 9, 7, 17, 25$.

(Ответ на этот вопрос нужен, например, для изучения *внешних бильярдов*. Ср. с задачей 4.1.7.а, замечанием 9.1.1, утверждением 9.1.3 и теоремами 4.8.5, 9.1.5.)

Лемма 9.3.4. Пусть $r \in \mathbb{R} - \mathbb{Q}$ и $r^2 \in \mathbb{Q}$.

- (а) **О неприводимости.** Многочлен $x^2 - r^2$ неприводим над $\mathbb{Q}$.
- (б) **О линейной независимости.** Если $a, b \in \mathbb{Q}$ и $a + br = 0$, то $a = b = 0$.
- (с) Если многочлен P имеет корень r , то P делится на $x^2 - r^2$.
- (д) **О сопряжении.** Если многочлен имеет корень r , то корнем этого многочлена является также число $-r$.
- (е) **О сопряжении.** Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.
- (ф) Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

Теорема 9.3.5. Если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

Из теоремы 9.3.5 и леммы 9.3.2 о расширении вытекает, что *если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не является вещественно радикальным с извлечением корня только один раз, причём второй степени*. Справедлив и комплексный аналог этого утверждения. Это наше первое продвижение

к теоремам о неразрешимости из §9.1. Аналогичные продвижения в следующих подпунктах (сформулируйте их самостоятельно) вытекают из аналогичных теорем и лемм.

9.3.6. (а) Решите уравнение $x^6 - 2x^4 - 12x^3 - 2x^2 + 1 = 0$.

(б) Число $\cos(2\pi/7)$ является корнем многочлена, полученного из функции $x^3 + x^2 + x + 1 + x^{-1} + x^{-2} + x^{-3}$ заменой Жуковского $z = \frac{1}{2}(x + \frac{1}{x})$.

9.3.7. Приводим ли многочлен $x^5 - 4x^3 + 6x^2 + 4x + 2$

(а) над $\mathbb{Z}$; (б) над $\mathbb{Q}$?

9.3.8. (а) Найдите неприводимый над $\mathbb{Q}$ многочлен, корнем которого является число $\varepsilon_q := \cos(2\pi/q) + i \sin(2\pi/q)$ для $q = 5, 7, 11, 9, 25, 15, 16, 20$.

(б) То же с заменой ε_q на $\cos(2\pi/q)$.

Подсказки

9.3.2. Было бы достаточно доказать, что множество чисел такого вида замкнуто относительно сложения, вычитания, умножения и деления. Это, естественно, не так: $(1 + \sqrt{2}) + (1 + \sqrt{3})$ не представимо в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$ (докажите!).

9.3.4. (а) Если многочлен $x^2 - r^2$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(б) Если $b \neq 0$, то $r = -a/b \in \mathbb{Q}$, что невозможно. Поэтому $b = 0$, а значит, $a = 0$.

(с) Поделим многочлен с остатком⁸ на $x^2 - r^2$:

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Подставляя $x = r$, по лемме о линейной независимости (см. п. (б)) получаем, что остаток нулевой.

(д) Из п. (с) следует, что если $R^2 = r^2$, то R есть корень многочлена.

Указание к другому решению. Отображение $u \mapsto \bar{u}$ множества $\mathbb{Q}[r] := \{a + br : a, b \in \mathbb{Q}\}$ в себя корректно определено формулой

⁸Это деление с остатком — то же самое, что «замена» x^2 на r^2 .

9.3.5 Неразрешимость «в вещественных многочленах» (2)

In this and the following subsubsection equality signs involving polynomial f (or f_j) mean equality of polynomials (покоэффициентное). В этом пункте аргументы (x, y, z) многочленов в формулах часто пропускаются.

9.3.28. Существуют ли многочлены с вещественными коэффициентами, удовлетворяющие системе из задачи 9.2.3 с заменой f_2^3 на f_2^2 ?

Для решения полезны следующее понятие и утверждение. Многочлен $g \in \mathbb{R}[x, y, z]$ называется **циклически симметрическим**, если $g(x, y, z) = g(y, z, x)$.

9.3.29. Если $f \in \mathbb{R}[x, y, z]$ и многочлен

- (a) f^3 ; (b) f^2

циклически симметрический, то f циклически симметрический.

9.3.30. Пусть $f, g \in \mathbb{R}[x, y, z]$.

- (a) **Лемма.** Если $fg = 0$, то $f = 0$ или $g = 0$.

Предостережения: существуют функции $F, G : \mathbb{R} \rightarrow \mathbb{R}$, для которых $FG = 0$, $F \neq 0$, $G \neq 0$; существуют два разных многочлена от двух переменных, равные в бесконечном множестве точек; не пользуйтесь без доказательства равенством многочленов от двух переменных, значения которых совпадают в любой точке.

- (b) Если $f^2 = g^2$, то $f = g$ или $f = -g$.
 (c) Если $f^2 + fg + g^2 = 0$, то $f = 0$ и $g = 0$.
 (d) Если $f^3 = g^3$, то $f = g$.
 (e) Если $f^5 = g^5$, то $f = g$.
 (f) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$.

Теорема 9.2.5 вытекает из следующей леммы.

Лемма 9.3.31 (о сохранении циклической симметричности). Если $q > 0$ целое, $f \in \mathbb{R}[x, y, z]$ и многочлен f^q циклически симметрический, то f циклически симметрический.

9.3.32. Аналоги каких утверждений этого пункта справедливы для

- (a) многочленов с комплексными коэффициентами?

(b) с заменой многочлена f на функцию $f : \mathbb{R}^3 \rightarrow \mathbb{R}$ (не предполагаемую непрерывной).

9.3.6 Неразрешимость «в многочленах» (3)

Теорема Руффини 9.2.6 вытекает из леммы 9.3.36. Самое трудное и интересное — придумать формулировку этой леммы. Для этого докажем следующие более простые факты.

9.3.33. Многочлен x_1 не радикален для $n = 3$ так, что вторая операция из определения радикальности применяется только для

- (а) $k = 2$ (*подсказка*: см. задачу 9.3.32); (b) $k = 3$.

9.3.34. Какие из следующих утверждений верны для любого $f \in \mathbb{C}[x_1, \dots, x_5]$?

(а) Если f^5 циклически симметрический, то f циклически симметрический.

(b) Если f^3 циклически симметрический, то f циклически симметрический.

(с) Если f^2 симметрический, то f симметрический.

(d) Если f^3 симметрический, то f симметрический.

Циклом длины 3 называется перестановка n -элементного множества, переставляющая некоторые 3 элемента по циклу и оставляющая на месте каждый из оставшихся элементов. Многочлен $f \in \mathbb{C}[x_1, \dots, x_n]$ называется **четносимметрическим**, если $f(x_1, x_2, \dots, x_n) = f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)})$ для любого цикла α длины 3.

9.3.35. Придумайте циклически симметрический многочлен, не являющийся четносимметрическим.

Лемма 9.3.36 (о сохранении четносимметричности). Если $q > 0$ целое, $f \in \mathbb{C}[x_1, \dots, x_5]$ и многочлен f^q четносимметрический, то f четносимметрический.

9.3.37. Пусть $f \in \mathbb{C}[x_1, \dots, x_n]$ — многочлен.

(а) Если многочлен f^7 четносимметрический, то f четносимметрический.

(b) Если $n \geq 5$ и многочлен f^3 четносимметрический, то f четносимметрический.

(с) Если $n \geq 5$, то любой цикл длины 3 на n -элементном множестве разлагается в произведение перестановок вида $(ab)(cd)$ с различными a, b, c, d (т.е. в произведение композиций транспозиций с непересекающимися носителями).

9.3.7 Единственность способа решения квадратного уравнения (2)

9.3.39. Решите систему уравнений в многочленах $f(x, y)$, $p(u, v)$ и $q(u, v, w)$ с вещественными коэффициентами:

$$\begin{cases} f^2(x, y) = p(x + y, xy) \\ x = q(x + y, xy, f(x, y)) \end{cases}.$$

Многочлен f от двух переменных x, y называется *антисимметрическим*, если $f(x, y) = -f(y, x)$.

9.3.40. (а) **Лемма.** Если $f \in \mathbb{R}[x, y]$ — многочлен с вещественными коэффициентами от двух переменных и многочлен f^2 симметрический, то f либо симметрический, либо антисимметрический.

(б) Если $f \in \mathbb{R}[x, y]$ антисимметрический, то существует симметрический многочлен $a \in \mathbb{R}[x, y]$, для которого $f = (x - y)a$.

Приведем обобщение утверждения из решения задачи 9.3.39 на любое количество шагов из определения радикальности (п. 9.2.1).

9.3.41. *Рациональной функцией* называется «формальное отношение многочленов», т.е. пара $f/g := (f, g)$ многочленов, в которой $g \neq 0$, с точностью до следующей эквивалентности: $f/g \sim f'/g'$ при $fg' = f'g$. При этом многочлен f отождествляется с парой $(f, 1)$.

(а) Дайте определения суммы и произведения рациональных функций. Проверьте их корректность.

(б) Возьмем систему из замечания 9.2.4.(с) для $n = 2$, в которой f_j и p_j рациональные функции, а не обязательно многочлены, и которая *минимальна*, т.е. нет системы с меньшим s и f_j^k не представляется в виде рациональной функции от $x + y, xy, f_1, \dots, f_{j-1}$ ни для каких $j = 1, \dots, s$ и $k < k_j$. Тогда $s = 1$, $k_1 = 2$ и существует рациональная функция $a \in \mathbb{R}(u, v)$, для которой $f_1(x, y) = (x - y)a(x + y, xy)$.

(с)* Сформулируйте и докажите аналог п. (б) с заменой рациональных функции $f_1, \dots, f_s$ на функции $\mathbb{R}^2 \rightarrow \mathbb{R}$ ($p_0, \dots, p_s$ по-прежнему рациональные функции), и равенств рациональных функций — на равенства функций, определенных для всех $(x, y) \in \mathbb{R}^2$.

9.3.42. (Загадка) Кубическое уравнение можно решить только одним способом. (Для решения полезны п. 9.3.1 и 9.3.3.)

9.3.30.be, 9.3.40. Если k нечетно, то из утверждения 9.3.40.b получаем, что f симметрический, что противоречит равенству $x = q(x + y, xy, f(x, y))$. Если $k = 4$, то по утверждению 9.3.40.a многочлен f^2 либо симметрический, либо антисимметрический. Первый случай сводится к п. (a). Во втором $f^2(x, y) + f^2(y, x) = 0$. Аналогично разбирается случай произвольного четного k .

(c) Аналогично п. (a) получаем $x = a + bf$. Поэтому f — дробно-рациональная функция. Тогда решение аналогично п. (a).

9.3.40. (a) Так как f^2 симметрический, то $f(x, y)^2 = f(y, x)^2$. Отсюда по утверждению 9.3.30.b $f(x, y) = \pm f(y, x)$.

(b) См. указание к 9.3.30.f.

9.3.8 Неразрешимость «в комплексных числах» (4*)

См. англ версию.

9.3.9 Выразимость с данным числом радикалов (4*)

Определения радикальности числа и многочлена приведены в п. 9.1.4 и 9.2.1, соответственно.

9.3.43. Корни уравнений 3-й и 4-й степени с рациональными коэффициентами радикальны с извлечением корня только

(a) два раза, причём один раз третьей степени и один раз второй — для 3-й степени;

(b) четыре раза, причём один раз третьей степени и три раза второй — для 4-й степени.

(«Один раз» означает «однократное использование в программе». Например, в программе $u := \sqrt[3]{a}$, $v := u + u$ кубический корень используется один раз.)

9.3.44. Корни кубического уравнения (как многочлены) не являются радикальными с извлечением только

(a) одного корня;

(b) квадратных корней;

(c) кубических корней;

(d)* «одноэтажных» корней, т.е. корней из выражений, не содержащих корней.

9.3.45. Являются ли корни уравнения 4-й степени (как многочлены) радикальными с извлечением только

- (а) квадратных корней; (b) кубических корней;
(с) двух корней; (d) трех корней?

9.3.46. Если корни уравнения n -й степени с рациональными коэффициентами радикальны, то они радикальны с извлечением не более, чем

- (а) 5 корней для $n = 5$; (b) $n \log_2 n$ корней для любого n .

Для решения этих задач нужны следующие простые элементы теории Галуа. В этом пункте (в отличие от остальных) обозначим $\mathbb{Z}_q := \{1, \varepsilon_q, \varepsilon_q^2, \dots, \varepsilon_q^{q-1}\}$. Подгруппой в S_n называется подмножество, замкнутое относительно операций взятия композиции и обратного элемента. Для подгруппы $G \subset S_n$ и целого q отображение $G \rightarrow \mathbb{Z}_q$ называется гомоморфизмом (или *характером*), если оно переводит композицию в произведение: $\chi(\alpha\beta) = \chi(\alpha)\chi(\beta)$.

9.3.47. (а) Если $q > 0$ целое и ненулевой многочлен f^q четносимметрический, то для любой четной перестановки α существует и единственно такое

$$\chi_f(\alpha) \in \mathbb{Z}, \quad \text{что} \quad f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = \varepsilon_q^{\chi_f(\alpha)} f(x_1, x_2, \dots, x_n).$$

(b) Построенное в п. (а) отображение $\chi_f : A_n \rightarrow \mathbb{Z}_q$ из множества A_n всех четных перестановок является гомоморфизмом.

9.3.48. Существует ли простое q и непостоянный гомоморфизм

- (а) $A_3 \rightarrow \mathbb{Z}_q$? (b) $A_4 \rightarrow \mathbb{Z}_q$?

В доказательстве леммы 9.3.36 о сохранении четносимметричности фактически доказано, что при целом $n \geq 5$ и простом q любой гомоморфизм $\chi : A_n \rightarrow \mathbb{Z}_q$ переводит каждую перестановку в 1.

9.3.49. (а) Существуют ли целое q и инъективный (=взаимно-однозначный) гомоморфизм $S_3 \rightarrow \mathbb{Z}_q$?

(b) Существуют ли целые p, q и гомоморфизмы $\chi : S_4 \rightarrow \mathbb{Z}_q$ и $\varphi : \chi^{-1}(1) \rightarrow \mathbb{Z}_p$, из которых второй инъективен?

9.3.50. (a) Существуют ли целые p, q и гомоморфизмы $\chi : S_4 \rightarrow \mathbb{Z}_q$ и $\varphi : \chi^{-1}(1) \rightarrow \mathbb{Z}_p$, из которых второй инъективен?

(b) Существуют ли целые p, q, r и гомоморфизмы $\chi : S_4 \rightarrow \mathbb{Z}_q$, $\varphi : \chi^{-1}(1) \rightarrow \mathbb{Z}_p$ и $\gamma : \varphi^{-1}(1) \rightarrow \mathbb{Z}_r$, из которых последний инъективен?

(c) Существуют ли цепочка из четырех гомоморфизмов, аналогичная п. (b)?

9.3.51. (a) Для любого многочлена $f(x_1, x_2, \dots, x_n)$ множество

$$\text{st}_f := \{\alpha \in S_n \mid f(x_{\alpha(1)}, x_{\alpha(2)}, \dots, x_{\alpha(n)}) = f(x_1, x_2, \dots, x_n)\}$$

является подгруппой в S_n .

(b) Перечислите все подгруппы в S_3 .

(b') Какие из них могут быть прообразами единицы при гомоморфизме $S_3 \rightarrow \mathbb{Z}_q$ для некоторого q ?

(c) Перечислите все подгруппы в S_4 .

(c') Какие из них могут быть прообразами единицы при гомоморфизме $S_4 \rightarrow \mathbb{Z}_q$ для некоторого q ?

The estimation 9.3.46 can be extracted from the idea of proof of the Ruffini Theorem 9.2.6. The idea is that the ‘symmetry subgroup’ st_f of S_n cannot be changed more than $\log_2(n!) < n \log_2 n$ times.

9.4.4 Непостроимость в теореме Гаусса (3*)

Теорема 9.1.2 (вещественная непостроимость числа $\sqrt[3]{2}$) вытекает из вещественного аналога леммы 9.4.1.а о башне расширений и следующей леммы.

Лемма 9.4.3. Пусть $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^2 \in F$.

- (а) Тогда $F[r]$ — поле.
- (б) Если $\sqrt[3]{2} \notin F$, то $\sqrt[3]{2} \notin F[r]$.

Доказательство части (а). Нужно доказать, что $F[r]$ замкнуто относительно сложения, вычитания, умножения и деления на ненулевое число. Это не очевидно только в случае деления, который следует из равенства $\frac{1}{a+br} = \frac{a}{a^2-b^2r^2} - \frac{b}{a^2-b^2r^2}r$. $\square$

Доказательство части (б). Предположим, напротив, что $\sqrt[3]{2} \in F[r]$. Тогда $\sqrt[3]{2} = a + br$ для некоторых $a, b \in F$. Получаем

$$2 = (\sqrt[3]{2})^3 = (a^3 + 3ab^2r^2) + (3a^2b + b^3r^2)r.$$

Так как $\sqrt[3]{2} \notin F$, то $b \neq 0$ и $r \notin F$. В частности, $r \neq 0$. Поэтому $3a^2 + b^2r^2 > 0$. Так как $2 \in \mathbb{Q} \subset F$, то $r \in F$. Противоречие. $\square$

Перейдем к доказательству непостроимости в теореме Гаусса 9.1.5.

Лемма 9.4.4 (о степенях двойки). Если неприводимый над $\mathbb{Q}$ многочлен P с рациональными коэффициентами имеет построимый корень, то $\deg P$ есть степень двойки.

Эта лемма вытекает из леммы 9.4.1.а о башне расширений и части (б) следующей леммы. Доказательство ее части (а) оставляем читателю в качестве упражнения.

Лемма 9.4.5 (о сопряжении). Пусть $F \subset \mathbb{C}$ — поле, $r \in \mathbb{C} - F$ и $r^2 \in F$.

(а) Определим отображение сопряжения $\bar{\cdot} : F[r] \rightarrow F[r]$ формулой $\overline{x + yr} := x - yr$. Это отображение корректно определено, $\overline{z + w} = \bar{z} + \bar{w}$ и $\overline{zw} = \bar{z} \cdot \bar{w}$.

(б) Если многочлены $P \in F[x]$ и $Q \in F[r][x]$ имеют общий корень и неприводимы над F и над $F[r]$, соответственно, то $\deg P \in \{\deg Q, 2 \deg Q\}$.

Доказательство части (б). По комплексному аналогу леммы 9.4.3.а $F[r]$ поле. Будем рассматривать делимость, неприводимость и НОД в $F[r]$, если не указано другое. Так как P и Q имеют общий корень и Q неприводим, то P делится на Q . Тогда по п. (а) $P = \overline{P}$ делится на $\overline{Q}$. Так как Q неприводим и делится на $D := \gcd(Q, \overline{Q})$, то либо $D = Q$, либо $D = 1$.

Если $D = Q$, то из $\overline{D} = D$ получаем $Q = D \in F[x]$. Отсюда, так как P неприводим над F , получаем $P = Q$.

Если $D = 1$, то P делится на $M := Q\overline{Q}$. Так как $\overline{M} = M$, получаем $M \in F[x]$. Так как P неприводим над F , получаем $P = M$. Значит, $\deg P = 2 \deg Q$. $\square$

Лемма 9.4.6 (признак Эйзенштейна). Пусть p простое. Если для многочлена с целыми коэффициентами старший коэффициент не делится на p , остальные делятся на p , а свободный член не делится на p^2 , то этот многочлен неприводим над $\mathbb{Z}$.

Лемма 9.4.7 (Гаусс). Если многочлен с целыми коэффициентами неприводим над $\mathbb{Z}$, то он неприводим и над $\mathbb{Q}$.

И признак Эйзенштейна, и лемма Гаусса легко доказываются переходом к многочленам с коэффициентами $\mathbb{Z}_p$. (Для леммы Гаусса рассмотрим разложение $P = P_1 P_2$ данного многочлена P над $\mathbb{Q}$, возьмём такие целые n_1 и n_2 , что и $n_1 P_1$, и $n_2 P_2$ имеют целые коэффициенты, и возьмём простой делитель p числа $n_1 n_2$. For the Eisenstein criterion see solution of Problem 9.3.1.f.)

Доказательство непостроимости в теореме Гаусса 9.1.5. Так как $\varepsilon_n = \varepsilon_{nk}^k$, то из построимости числа ε_{nk} вытекает построимость числа ε_n . Поэтому достаточно показать, что ε_n непостроимо для

- (А) простого числа n , не представимого в виде $2^m + 1$;
- (В) квадрата простого числа, т. е. $n = p^2$.

Непостроимость числа ε_n следует из леммы 9.4.4 о степенях двойки для корня ε_n многочлена

- $P(x) := x^{n-1} + x^{n-2} + \dots + x + 1$ в случае (А) и
- $P(x) := x^{p(p-1)} + x^{p(p-2)} + \dots + x^p + 1$ в случае (В).

Неприводимость этих многочленов над $\mathbb{Q}$ вытекает из их неприводимости над $\mathbb{Z}$ и леммы 9.4.7 Гаусса. Неприводимость этих многочленов $P(x)$ над $\mathbb{Z}$ вытекает из неприводимости многочленов $P(x+1)$ над $\mathbb{Z}$. Последняя неприводимость доказывается применением признака 9.4.6 Эйзенштейна. Выполнение предположений признака Эйзенштейна для многочленов $P(x+1)$ легко проверяется с помощью сравнения $(a+b)^p \equiv a^p + b^p \pmod{p}$. $\square$

9.4.5 Неразрешимость «в вещественных числах» (3*)

Импликация $(ii) \Rightarrow (i)$ в теореме 9.1.8 вытекает из вещественного аналога леммы 9.4.1.b о башне расширений и части (а) следующей леммы.

Лемма 9.4.8. Пусть q простое, $F \subset \mathbb{R}$ — поле, $r \in \mathbb{R} - F$ и $r^q \in F$.

(а) If a polynomial with coefficients in F has degree 3, has three real roots none of which lies in F , then none of the roots lies in $F[r]$.

(b) **О неприводимости.** Многочлен $t^q - r^q$ неприводим над $F[\varepsilon_q]$.

(с) **О линейной независимости.** Если $P(r) = 0$ для некоторого многочлена $P \in F[\varepsilon_q][t]$ степени меньше q , то $P = 0$.

(d) **О сопряжении.** Если $P \in F[\varepsilon_q][t]$ и $P(r) = 0$, то $P(r\varepsilon_q^k) = 0$ для любого $k = 0, 1, \dots, q-1$.

Доказательство части (b). Пусть, напротив, многочлен $t^q - r^q$ приводим над $F[\varepsilon_q]$, т.е. имеет собственный делитель $P \in F[\varepsilon_q][t]$. Все корни многочлена $t^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \dots, r\varepsilon_q^{q-1}$. Свободный член многочлена P равен произведению некоторых k из этих корней. Тогда $r^k \in F[\varepsilon_q]$. Так как q простое, то $kx + qy = 1$ для некоторых целых x, y . Тогда $r = (r^k)^x (r^q)^y \in F[\varepsilon_q]$.

Поэтому¹⁰ $r^2, r^3, \dots, r^{q-1} \in F[\varepsilon_q]$. Составим таблицу $a_{kl} \in F$ размера $q \times (q-1)$ из разложений чисел r^k по степеням числа ε_q :

$$r^k = \sum_{l=0}^{q-2} a_{kl} \varepsilon_q^l, \quad 0 \leq k \leq q-1.$$

¹⁰ Другая запись этого абзаца с использованием понятия размерности: тогда $\dim_F F[r] \leq \dim_F F[\varepsilon_q] \leq q-1$.

При помощи нескольких операций прибавления к одной строке другой, умноженной на число из F , можно получить таблицу с нулевой строкой.

Значит, имеется ненулевой многочлен $Q \in F[t]$ степени меньше q с корнем r . Тогда $\gcd(t^q - r^q, Q)$ имеет корень r и степень k , $0 < k \leq \deg Q < q$. Поэтому многочлен $t^q - r^q$ приводим над F .

Тогда аналогично первому абзацу этого доказательства получаем, что $r \in F$. Противоречие. $\square$

Part (c) follows by part (b) analogously to the last but one paragraph of the proof of (b).

Доказательство части (d). Так как $P(r) = 0$, то остаток от деления многочлена $P(t)$ на $t^q - r^q$ принимает значение 0 в точке r . Since the degree of this remainder is less than q , по части (c) этот остаток равен нулю. Thus P is divisible by $t^q - r^q$. For every $j = 0, 1, \dots, q-1$ since $(r\varepsilon_q^j)^k = r^k$, we obtain $P(r\varepsilon_q^j) = 0$. $\square$

Доказательство части (a). Пусть, напротив, некоторый корень x_0 многочлена A лежит в $F[r]$. Тогда $x_0 = H(r)$ для некоторого многочлена H с коэффициентами в F степени больше 0 и меньше q . Применим п. (d) к многочлену $P(t) := A(H(t))$. Так как $A(H(r)) = 0$, то $H(r\varepsilon_q^k)$ является корнем многочлена A для любого $k = 0, 1, \dots, q-1$. Если $H(r\varepsilon_q^k) = H(r\varepsilon_q^l)$ для некоторых k, l , $0 \leq k < l \leq q-1$, то по п. (c) получим, что $\deg H = 0$ — противоречие. Итак, числа $H(r\varepsilon_q^k)$, $0 \leq k \leq q-1$, — попарно различные корни многочлена A . Значит, $q \leq 3$.

Если $q = 2$, то по теореме Виета третий корень многочлена A лежит в F — противоречие. Поэтому $q = 3$. Так как $\overline{\varepsilon_3} = \varepsilon_3^2$, то $\overline{H(r\varepsilon_3)} = H(r\varepsilon_3^2)$. Так как последние два числа различны, то ни одно из них не вещественно. $\square$

9.4.6 Неразрешимость «в числах» (4*)

См. [Sk15].

Литература

- [Al] *Алексеев В. Б.* Теорема Абеля. М.: Наука, 1976.
- [AB] *Akhtyamov D., Bogdanov I.* Solvability of cubic and quartic equations using one radical.
<http://arxiv.org/abs/1411.4990>.
- [ABG] Solving equations using one radical, presented by D. Akhtyamov, I. Bogdanov, A. Glebov, A. Skopenkov, E. Streltsova and A. Zykin. <http://www.turgor.ru/lktg/2015/4/index.htm>.
- [Ar84] *Арнольд В.И.* Обыкновенные дифференциальные уравнения, М. Наука, 1984.
- [Ber] *Bergen J.* A Concrete Approach to Abstract Algebra: From the Integers to the Insolvability of the Quintic, 2010.
- [BK] *Бурда Ю., Кадец Л.* Семнадцатиугольник и закон взаимности Гаусса // Мат. Просвещение. 2013, № 17.
- [Br] J. Brown, Abel and the insolvability of the quintic, <http://www.math.caltech.edu/~jimlb/abel.pdf>.
- [Ch] *Чеботарёв Н. Н.* Основы теории Галуа. Часть 1. Л., М.: Гостехиздат, 1934.
- [CR] *Курант Р., Роббинс Дж.* Что такое математика. М.: МЦНМО, 2004.

- [Dor] *Dörrie H.* 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.
- [E1] *Edwards H. M.* Galois Theory. Springer Verlag, 1984.
- [E2] *Edwards H. M.* The construction of solvable polynomials // Bull. Amer. Math. Soc. 2009. V. 46. P 397–411. Errata: Bull. Amer. Math. Soc. 46 (2009), 703–704.
- [ECG] Toward algorithms of solving algebraic equations, presented by A. Enne, A. Chilikov, A. Glebov, A. Skopenkov, B. Vukorepa, <https://www.turgor.ru/lktg/2018/5/index.html>.
- [Es] *Esterov A.* Galois theory for general systems of polynomial equations, <https://arxiv.org/abs/1801.08260>
- [FT] *Табачников С. Л., Фукс Д. Б.* Математический дивертисмент, М.: МЦНМО, 2011.
- [Ga] *Гаусс К. Ф.* Арифметические исследования. Труды по теории чисел. М.: Изд-во АН СССР, 1959. С. 9–580.
- [Gi] *Гиндикин С.* Дебют Гаусса // Квант. 1972. № 1. С. 2–11.
- [Gi1] *Гиндикин С.* Великое искусство // Квант. 1976. № 9. С. 2–10.
- [Had] *Hadlock Ch. R.* Field Theory and its Classical Problems. The Mathematical Association of America, 1978. (Carus Mathematical Monographs, № 19.)
- [Ka] *Канунников А. Л.* Начала теории Галуа: разрешимость алгебраических уравнений в радикалах. <http://www.mathnet.ru/conf1015>.
- [Ki] *Кириллов А. А.* О правильных многоугольниках, функции Эйлера и числах Ферма // Квант. 1977. № 7. С. 2–9; 1994. № 6. С. 15–18.
- [Kir] *Кириченко В. А.* Построения циркулем и линейкой и теория Галуа. <http://www.mccme.ru//dubna/2005/courses/kirichenko.html>.

- [Ko17] *Коган Е.* Множественная сложность построения правильного многоугольника, <https://arxiv.org/abs/1711.05807>.
- [Kol] *Колосов В. А.* Теоремы и задачи алгебры, теории чисел и комбинаторики. М.: Гелиос, 2001.
- [KS] *Козлов П., Скопенков А.* В поисках утраченной алгебры: в направлении Гаусса (подборка задач) // Мат. Просвещение. 2008. № 12. С. 127–144;
[http://arxiv.org/abs/0804.4357\(v1\)](http://arxiv.org/abs/0804.4357(v1)).
- [Kh13] *Хованский А. Г.* Построения циркулем и линейкой // Мат. Просвещение. 2013. № 17.
- [Ler] *Lerner L.* Galois Theory without abstract algebra.
<http://arxiv.org/abs/1108.4593>.
- [Ma] *Манин Ю. И.* О разрешимости задач на построение с помощью циркуля и линейки // В кн.: Энциклопедия элементарной математики. Книга четвёртая (геометрия) / Под редакцией П. С. Александрова, А. И. Маркушевича и А. Я. Хинчина. М.: Физматгиз, 1963.
- [Pe] P. Pesic, Abel's Proof, The MIT Press, 2004, Cambridge, Massachusetts, London, England.
- [Pos] *Постников М. М.* Теория Галуа. М.: Физматлит, 1963.
- [Pr07-2] *Прасолов В. В.* Задачи по алгебре, арифметике и анализу. М.: МЦНМО, 2007.
- [PSo] *Прасолов В. В., Соловьев Ю. П.* Эллиптические функции и алгебраические уравнения. М.: Факториал, 1997.
- [Ro] M. I. Rosen, Niels Hendrik Abel and Equations of the Fifth Degree, Amer. Math. Monthly, 102:6 (1995) 495-505.
- [Saf] *Сафин А.* Программа для построения правильных многоугольников циркулем и линейкой (доклад на ММКШ-2008). <http://www.mccme.ru/mmks/dec08/Safin.pdf>.

- [Sk08] *Скопенков А.* Ещё несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах.
<http://arxiv.org/abs/0804.4357>.
- [Sk10] *Скопенков А.* Базисные вложения и 13-я проблема Гильберта // Мат. Просвещение. 2010. № 14. С. 143–174;
<http://arxiv.org/abs/1001.4011>.
- [Sk11] *Скопенков А.* Простое доказательство теоремы Абеля о неразрешимости уравнений в радикалах // Мат. Просвещение. 2011. № 15. С. 113–126;
<http://arxiv.org/abs/1102.2100>.
- [Sk15] *Skopenkov A.* A short elementary proof of the insolvability of the equation of degree 5. <http://arxiv.org/abs/1508.03317>.
- [St94] *Stillwell J.* Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.
- [T] *Тихомиров В. М.* Абель и его великая теорема // Квант. 2003. № 1. С. 11–15.
- [Vag] *Вагутен Н.* Сопряжённые числа // Квант. 1980. № 2. С. 26–32.
- [Vi] *Винберг Э. Б.* Алгебра многочленов. М.: Просвещение, 1980.
- [W] *Ван дер Варден Б. Л.* Алгебра. М.: Наука, 1976.

11 О преподавании

11.1 Олимпиады и математика

To him a thinking man's job was not to deny one reality
at the expense of the other, but to include and to connect

*U. K. Le Guin. The Dispossessed*²¹

Перед школьниками, их учителями и руководителями кружков встаёт вопрос: готовиться к олимпиадам или к «серьёзной» математике? Некоторые думают, что для первого надо прорешивать задачи последних олимпиад, для второго надо читать вузовские учебники, и что ввиду принципиальной разницы первого и второго бессмысленно пытаться достичь и того, и другого. Я придерживаюсь распространённого мнения о том, что эти подходы недостаточно эффективны и приводят к вредным «побочным эффектам»: школьники либо чрезмерно увлекаются *спортивным* элементом в решении задач, либо изучают *язык* математики вместо её содержания²².

По моему мнению, основу математического образования должно составлять *решение и обсуждение интересных ученику задач, в процессе которых он знакомится с важными математическими идеями и теориями*. Это одновременно подготовит школьника и к математической науке, и к олимпиадам и не нанесёт вред его развитию в целом. Это будет более эффективно и для достижения успеха только в олимпиадах или только в науке (если не учитывать большого количества других факторов, кроме разумной организации занятий).

Как и при естественном развитии самой математики, каждая следующая задача должна быть мотивирована либо практикой, ли-

²¹Для него работой мыслителя было не отрицание одной реальности за счёт другой, а взаимовключение и взаимосвязь. *У. К. Ле Гуин, «Обделённые»* (пер. автора).

²²Имеется обширная литература, в которой в первую очередь излагается содержание, а язык появляется по ходу дела. Однако часто такая *популярная* литература недооценивается ввиду её «недостаточной серьёзности» по сравнению с учебниками *для университета*. Подробнее см. § 11.2 «Начинать с языка или содержания?».

Кроме того, даже чтение хороших книг без решения задач, как правило, неэффективно.

бо уже решёнными задачами (см. подробнее § 11.2 «Начинать с языка или содержания?» и 11.3 «О необходимости мотивировок»). Ученик, занимающийся «мотивированной для него» математикой (обычно более элементарной, но содержательной и потому сложной) вместо «немотивированной для него» математики (обычно менее элементарной, но языковой и потому тривиальной), имеет преимущество в дальнейшей учёбе и научной работе. А. Н. Колмогоров говорил, что до тридцати лет математику разумнее всего заниматься решением конкретно поставленных задач. А значит, умение решать сложные задачи является одним из важнейших для молодого математика.

Олимпиадных задач очень много; большинство из них интересны школьнику, и среди них много математически содержательных. Такие задачи могут составить основу изучаемого материала. Однако решение олимпиадных задач без изучения математических идей и теорий недостаточно эффективно для подготовки к олимпиадам (на долгих — год и более — промежутках времени, как и вообще решение сиюминутных задач без фундаментального развития). А решение олимпиадных задач *вместе* с изучением стоящих за ними математических идей и теорий более эффективно. Это также позволит по-настоящему разобраться в идеях и теориях.

Кроме того, большинству людей легче достичь успеха на олимпиадах в том случае, когда они не считают успех главной целью. Задачу легче решить, если спокойно думать о самой задаче, а не о награде, которая последует за её решением. Поэтому школьник, мотивированный более высокой целью, чем успех на олимпиаде, имеет на этой олимпиаде психологическое преимущество.

См. также п. 1.2 «Изучение путём решения и обсуждения задач».

11.2 Начинать с языка или содержания?

По моему мнению, именно с *новых идей*, изложенных на уже имеющемся языке, а не с *введения нового языка*, полезно начинать изучение любой теории. Удачно представлять основные идеи на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей. Как правило, такие идеи наибо-

лее ярко выражаются доказательствами, подобными приведённым в § 9, 10 и других частях этой книги. Имеется много других ярких примеров, упомянем только фейнмановские лекции по физике (там приводятся физические рассуждения, а не доказательства).

«Мы стараемся свести к минимуму число понятий, откладывая определения до момента, когда они напрашиваются сами собой, и избегая задач на понимание и применение формальных определений (типа „является ли множество целых чисел группой по сложению?“)» [Shen].

«При изложении материала нужно ориентироваться на объекты, которые основательнее всего укореняются в человеческой памяти. Это — отнюдь не системы аксиом и не логические приёмы в доказательстве теорем. Изящное решение красивой задачи, формулировка которой ясна и доступна, имеет больше шансов удержаться в памяти студента, нежели абстрактная теория. Скажем больше, именно по такому решению, при наличии некоторой математической культуры, студент впоследствии сможет восстановить теоретический материал. Обратное же, как показывает опыт, практически невозможно» [Kol, предисловие].

Такой стиль изложения не только делает материал более доступным, но позволяет сильным ученикам (для которых доступно даже абстрактное изложение) приобрести математический вкус и стиль. Это означает разумный выбор проблем для исследования и их мотивировки. Например, математик, понимающий, что теория Галуа мотивируется более важными и более сложными проблемами, чем построимость правильных многоугольников и разрешимость алгебраических уравнений в радикалах, вряд ли станет мотивировать созданную им теорию приложениями, которые можно получить и без его теории. Вкус и стиль означают также ясное изложение собственных открытий, не скрывающее ошибку или известность полученного результата за чрезмерным формализмом. К сожалению, такое — обычно непреднамеренное — сокрытие ошибки часто происходит с математиками, воспитанными на чрезмерно формальных курсах. Происходило это и с автором этих строк; к счастью, все мои серьёзные ошибки исправлялись *перед* публикациями.

Мода на искусственно формализованное изложение привела к сле-

11.3.1 «За» и «против» мотивировок

Решение задачи (неважно, учебной или научной) может прийти не сразу. При размышлении над ним выдвигаются естественные гипотезы, для доказательства которых нужны новые гипотезы, и т. д. В результате может быть построена целая теория. А решение исходной задачи может получиться при доказательстве утверждений, связь которых с исходной задачей неочевидна. В таких случаях разбиение материала на утверждения, каждое из которых легко доказать, доказав только *предыдущие*, нарушает естественную мотивированность изложения (хотя оно необходимо при написании формального доказательства). Однако многие учебники и курсы по «высшей» математике устроены именно так. Формулировки красивых результатов и важных проблем, ради которых была придумана теория, приводятся только *после* продолжительного изучения этой теории (или не приводятся совсем). Это способствует появлению представления о математике как науке, изучающей немотивированные понятия и теории. Такое представление принижает ценность математики.

О необходимости мотивировок говорили классики математики [Kl], [Poi1, гл. 2], [Poi2, с. 455–475].

*«...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде $f(gh) = (fg)h$. Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвящённым овладение своей наукой и тем самым повысить её авторитет»*²³ (В. И. Арнольд) [Ar84, с. 49, комментарий к задаче 5].

²³ Думаю, в последнем предложении несколько сгущены краски. Имеется традиция мотивированного изложения математики. Например, мои собственные попытки вернуть мотивировки в изложение были поддержаны математическим сообществом (по крайней мере, пока я не говорил о необходимости мотивировок явно и не приводил этой цитаты В. И. Арнольда). См. список литературы; для меня было также важно устное поощрение математиков.

Необходимость мотивировок выглядит банальностью. Однако на практике в большинстве курсов и учебников по математике «университетского» уровня либо мотивировок нет, либо приводятся общие слова без ссылок на чёткие формулировки результатов, доступные ученику или неспециалисту, а не скрытые под толщей обозначений и терминов. В тех ситуациях, когда эти общие слова удаётся проверить, они иногда оказываются неадекватными, см. п. 11.3.2. Для разных людей мотивировки разные: для одних новое определение само по себе интересно, а для других необходима его полезность для уже имеющейся математики и её приложений. Подробнее о «естественно-научном» и «философском» аспектах математики см. в [PS15, конец § 2].

О необходимости мотивировок высказываются открыто, а желание их пропустить не осознают или не афишируют. Судить о том, почему мотивированное изложение не принимается, приходится его сторонникам.

«Часто имеются непреодолимые трудности к мотивированности определений в курсе. Такое изложение требует высокого уровня общематематической подготовки и мотивированности его слушателей (а обычно большая часть слушателей хочет выучить и сдать). Преподавателю часто жалко времени на мотивировку определений...» (И. С. Рубанов, из письма).

Думаю, большинство математиков согласны с необходимостью мотивировок. Однако трудно понимать, какие утверждения ученику неизвестны, когда преподавателю известно больше. Ещё труднее понимать, какие вещи для ученика не мотивированы его знаниями, когда знаниями преподавателя мотивировано гораздо больше. Тем более что ученик мотивирован не только знаниями, но доверием преподавателю, оценкой, etc. Может быть не только трудно, но даже неприятно посмотреть на материал с точки зрения неспециалиста и осознать немотивированность изложения, особенно привычного, своего или уважаемого автора. Знаю это по собственному опыту. Поэтому часто необходимость мотивировок *вообще* признаётся, но *в данном конкретном случае* находятся причины неприятия мотивированного изложения. Эти причины не продумываются, поскольку продумывание может привести к неприятному осозна-

11.4 Кружки и олимпиады как путь в математику и как спорт. *А. Я. Канель-Белов, А. И. Буфетов*

11.4.1 Введение

Внешкольные занятия математикой, которым посвящена находящаяся в руках у читателя книга, играют в математическом образовании в нашей стране важнейшую роль, которую трудно переоценить. При этом значительное число занятий так или иначе оказываются связанными с олимпиадами. Школьников и их учителей часто сводят вместе математические олимпиады (например, в 1993 году А. Я. был членом жюри московской олимпиады, а девятиклассник А. И. участником — так мы и познакомились).

Многие школьники, особенно на периферии, получают математическое образование, нацеленное в первую очередь на подготовку к олимпиадам. С этим необходимо считаться научным руководителям и организаторам учебного процесса. Даже те, кто не занимается подготовкой к олимпиадам в тренерском смысле этого слова, активно используют идеи и задачный материал олимпиад.

У истоков олимпиадного движения стояли великие ученые, однако позже олимпиадный мир стал жить собственной жизнью. По всему миру проводятся математические конкурсы и олимпиады. Появились специалисты по их проведению, возникла олимпиадная математика со своей методикой работы и своей литературой. С некоторой долей условности можно сказать, что в олимпиадном мире сложились две ценностные ориентации: «научная» и «спортивная». Эти различные взгляды на олимпиады проявляются в подборе задач, выработке критериев оценок, в кадровых вопросах, в организации математических лагерей.

В нашей заметке мы кратко противопоставляем эти подходы.

11.4.2 Спортивный подход

Несколько сгущая краски, попробуем передать спортивный подход фразой: «олимпиада — это спорт по решению головоломок». Такая ориентация влечет за собой многое: усиливается тренерство, ужесточаются формальные требования и, соответственно, критерии оценок. Так, если спортсмен переступит черту на 10 см, а прыгнет

Глава 1

Геометрия

В этой главе, если задачу можно решать разными методами, она приводится в пункте, посвящённом одному из них, а о возможности других решений говорится в комментарии. Помимо обозначений, принятых во всей книге, в данной главе везде, где не оговорено обратное, используются принятые в геометрии обозначения элементов треугольника, описанные в начале параграфа «Треугольник».

12 Треугольник

Всюду в данной главе, кроме специально оговорённых случаев, используются следующие обозначения: ABC — данный треугольник, $A_i, B_i, C_i, i = 1, 2, \dots$, — точки на сторонах BC, CA и AB соответственно (или на продолжениях этих сторон, если это оговорено в условии задачи); ω — вписанная окружность, I — её центр, r — её радиус; Ω — описанная окружность, O — её центр, R — её радиус; G — точка пересечения медиан (центр тяжести, центроид), H — точка пересечения высот (ортоцентр). Проведём биссектрисы AI, BI, CI до пересечения с Ω в точках A', B', C' соответственно. Таким образом, A', B', C' — середины дуг AB, BC, CA . *Ортотреугольник* — треугольник с вершинами в основаниях высот, *серединный треугольник* — треугольник с вершинами в серединах сторон данного треугольника. Перпендикуляр, опущенный из точки A на BC , обозначается $h(A, BC)$.

Окружностью ABC называется окружность, описанная вокруг треугольника ABC .

12.1 Принцип Карно (1). *В. Ю. Протасов, А. А. Гаврилюк*

12.1.1. Теорема Карно. В точках A_1, B_1, C_1 , лежащих на сторонах треугольника ABC или на их продолжениях, восставлены перпендикуляры к этим сторонам. Докажите, что они пересекаются в одной точке тогда и только тогда, когда

$$C_1A^2 - C_1B^2 + A_1B^2 - A_1C^2 + B_1C^2 - B_1A^2 = 0.$$

12.1.2. Сформулируйте и докажите обобщённую теорему Карно для произвольных точек плоскости A_1, B_1, C_1 , не обязательно лежащих на прямых, содержащих стороны треугольника ABC .

12.1.3.° В каком из следующих случаев перпендикуляры, восставленные к сторонам треугольника в указанных точках, могут не пересекаться в одной точке:

- 1) A_1, B_1, C_1 — точки касания сторон с вписанной окружностью;
- 2) A_2, B_2, C_2 — точки касания сторон с соответствующими внеписанными окружностями;
- 3) A_3, B_3, C_3 — основания биссектрис треугольника?

12.1.4. На плоскости даны три пересекающиеся окружности. Докажите, что три их общие хорды пересекаются в одной точке.

Примечание. Это утверждение обычно доказывают, используя понятие степени точки (см. п. 13.4). Однако его легко вывести и из обобщённой теоремы Карно.

12.1.5. Пользуясь принципом Карно, получите ещё одно доказательство теоремы о пересечении трёх высот треугольника.

12.1.6. Охарактеризуйте все треугольники, у которых перпендикуляры к сторонам, восставленные в точках пересечения сторон с биссектрисами противоположных углов, пересекаются в одной точке.

12.3.8. В вершинах остроугольного треугольника проведены касательные к его описанной окружности. Докажите, что центр описанной окружности треугольника, образованного этими тремя касательными, лежит на прямой Эйлера исходного треугольника.

Указания, ответы и решения

12.3.3. Угол C должен быть острым, так как в противном случае точки O и H лежат по разные стороны от AB . Так как расстояние от O до AB равно $R \cos C$, а высота, проведённая из вершины C , равна $AC \sin A = 2R \sin A \sin B$, параллельность прямой Эйлера и прямой AB равносильна равенству $3 \cos C = 2 \sin A \sin B$. Учитывая, что $\cos C = -\cos(A + B) = \sin A \sin B - \cos A \cos B$, получаем утверждение задачи.

12.3.6. Из условия следует, что степени точки O относительно этих окружностей равны R^2 . Кроме того, если AA' и BB' — высоты треугольника, то четырёхугольник $ABA'B'$ вписанный, и, значит, $HA \cdot HA' = HB \cdot HB'$. Поэтому степени точки H относительно всех трёх окружностей также равны, т. е. прямая OH является их общей радикальной осью.

12.4 Формула Карно (2*). А. Д. Блинков

Формула Карно (по имени французского математика, физика и политического деятеля Лазаря Карно, 1753–1823) утверждает, что в остроугольном треугольнике сумма расстояний от центра описанной окружности до сторон треугольника равняется сумме радиусов описанной и вписанной окружностей, т. е. $OM_1 + OM_2 + OM_3 = R + r$, где M_1, M_2, M_3 — середины BC, CA, AB соответственно. Её доказательство с помощью теоремы Птолемея приводится в п. 13.6 «Теоремы Птолемея и Кези». Здесь мы рассмотрим её применения и ещё один способ её доказательства, в процессе которого будут получены другие важные факты.

12.4.1. Пусть биссектриса угла A пересекает окружность, описанную около треугольника ABC , в точке W , а точка D диаметрально противоположна точке W . Докажите, что

- (a) $M_1W = (r_a - r)/2$;
 (b) $M_1D = (r_b + r_c)/2$, где r, r_a, r_b, r_c — радиусы вписанной и невписанных окружностей.

12.4.2. Докажите формулу Карно.

Рассмотрим теперь несколько задач на применение формулы Карно. Если явно не оговорено обратное, то треугольник, заданный в условии, остроугольный.

12.4.3. Докажите, что сумма расстояний от вершин треугольника до ортоцентра равна сумме диаметров его вписанной и описанной окружностей.

12.4.4. Докажите, что в треугольнике ABC выполняются неравенства

- (a) $AH + BH + CH \leq 3R$;
 (b) $3OH \geq R - 2r$.

12.4.5. (a) Докажите, что $m_a + m_b + m_c \leq \frac{9}{2}R$, где m_a, m_b и m_c — длины медиан треугольника.

(b) Пусть в треугольнике ABC биссектрисы углов A, B и C пересекают описанную окружность в точках W_1, W_2 и W_3 соответственно. Докажите, что $AW_1 + BW_2 + CW_3 \leq 6,5R - r$.

12.4.6. (a) Докажите, что для углов треугольника выполняется неравенство

$$\frac{3r}{R} \leq \cos A + \cos B + \cos C \leq \frac{3}{2}.$$

(b) Пусть AH_1, BH_2 и CH_3 — высоты треугольника ABC . Выразите сумму диаметров окружностей, описанных около треугольников AH_2H_3, BH_1H_3 и CH_1H_2 , через R и r .

12.4.7. В окружность радиуса R вписан треугольник, а в каждый сегмент, ограниченный стороной треугольника и меньшей из дуг окружности, вписана окружность наибольшего возможного радиуса. Найдите сумму диаметров трёх получившихся окружностей и радиуса окружности, вписанной в треугольник.

12.4.8. (а) Докажите, что в треугольнике ABC выполняется равенство

$$a(OM_2 + OM_3) + b(OM_1 + OM_3) + c(OM_1 + OM_2) = 2pR.$$

(b) **Неравенство Эрдёша.** Пусть h_a — наибольшая высота треугольника ABC . Докажите, что $h_a \geq R + r$.

12.4.9. (а) Выведите аналоги формулы Карно для прямоугольного и тупоугольного треугольников.

(b) Четырёхугольник $ABCD$ вписанный. Пусть r_1 и r_2 — радиусы окружностей, вписанных в треугольники ABC и ADC , а r_3 и r_4 — радиусы окружностей, вписанных в треугольники ABD и CBD . Докажите, что $r_1 + r_2 = r_3 + r_4$.

12.4.10. Пусть d , d_1 , d_2 и d_3 — расстояния от центра O окружности, описанной около треугольника, до центров его вписанной и невписанных окружностей. Докажите, что

$$R^2 = \frac{d^2 + d_1^2 + d_2^2 + d_3^2}{12}.$$

12.4.11. (а) Докажите, что если точка принадлежит отрезку, соединяющему основания двух биссектрис треугольника, то сумма расстояний от этой точки до двух сторон треугольника равна расстоянию от неё до третьей стороны.

(b) Пусть центр окружности, описанной около треугольника, лежит на отрезке, соединяющем основания двух биссектрис. Докажите, что расстояние от ортоцентра треугольника до одной из его вершин равно $R + r$.

Указания, ответы и решения

12.4.1. (а) Пусть точки I и I_a соответственно — центры вписанной окружности и невписанной окружности, касающейся стороны BC , K и P — точки касания этих окружностей с BC , L — точка пересечения I_aP с прямой, проходящей через I и параллельной BC , Q — середина IL . Так как W — середина отрезка II_a (следствие из теоремы о трезубце, см. задачу 12.7.3 п. 12.7 «Биссектрисы, высоты

12.8 «Полувписанная» окружность (3^*). П. А. Кожевников

Пусть A' и A'' — середины дуг BC описанной окружности Ω , соответственно не содержащей и содержащей точку A ; B' и B'' , C' и C'' определяются аналогично.

Рассмотрим окружность S_A (назовём её *полувписанной*), касающуюся сторон AB , AC и окружности Ω (внутренним образом). Основными в этой серии являются следующие факты:

- прямая, проходящая через точки касания полувписанной окружности со сторонами, содержит точку I ;
- точка касания полувписанной окружности с окружностью Ω лежит на прямой $A''I$.

Основная серия-1

Докажите следующие утверждения.

12.8.1. Пусть перпендикуляр к биссектрисе AI , проведённый через точку I , пересекает AB и AC в точках K и L соответственно. Тогда окружности BKI , CLI и Ω пересекаются в одной точке T .

12.8.2. Точки T , I , A'' лежат на одной прямой.

12.8.3. Точки T , K , C' лежат на одной прямой.

12.8.4. Точки K , L и T являются точками касания окружности S_A с прямыми AB , AC и окружностью Ω .

12.8.5. (а) Прямая CC' касается окружности $TBKI$.

(б) Точка T — центр поворотной гомотетии, переводящей треугольник BKI в треугольник ILC .

Основная серия-2

12.8.6. Прямая AT проходит через центр гомотетии с положительным коэффициентом, переводящей окружность ω в Ω .

12.8.7. Пусть A_1 и A_2 — точки касания вписанной и невписанной окружностей со стороной BC соответственно. Тогда

- (a) AA' — биссектриса угла TAA_2 ;
- (b) $\angle BTA_1 = \angle ABC$. (Задача 4.7.7 из [GZ].)

12.8.8. Пусть AT пересекает KL в точке Z . Тогда $\angle BZK = \angle CZL$. (Задача 4.7.5 из [GZ].)

12.8.9. Прямые KL , TA' и BC пересекаются в одной точке или параллельны. (И. Шарыгин.)

12.8.10. Точка пересечения Y_A из предыдущей задачи и точки Y_B , Y_C , определённые аналогичным образом, лежат на одной прямой.

Дополнительные задачи-1

12.8.11. Пусть P — произвольная точка на дуге $BA'C$.

(a) Пусть $P_b = BB' \cap PC'$, $P_c = CC' \cap PB'$. Тогда окружность PP_bP_c проходит через T . ([Za14], задача 8.8, 2013 г.)

(b) Пусть J_b и J_c — центры вписанных окружностей треугольников PAB и PAC . Тогда окружность PJ_bJ_c проходит через T . (Задача 4.7.9 из [GZ].)

(c) Пусть касательные к ω из точки P пересекают BC в точках U_1 и U_2 . Тогда окружность PU_1U_2 проходит через T . (Задача 4.7.10 из [GZ].)

(d) Пусть прямые, проходящие через I параллельно биссектрисам углов между прямыми AP и BC пересекают прямую BC в точках V_1 и V_2 . Тогда окружность PV_1V_2 проходит через T . (См. частный случай задачи 4.7.18 из [GZ].)

Дополнительные задачи-2

Следующие задачи — про «обобщённые полувписанные» окружности, т. е. окружности, касающиеся двух прямых и окружности.

12.8.12. Пусть D — точка на стороне AC треугольника ABC , и пусть S_1 — окружность, касающаяся окружности Ω внутренним образом в точке R , а также отрезков BD и AD в точках M и N соответственно.

- (a) Докажите, что точки B , M , I , R лежат на одной окружности.
- (b) **Лемма Саваямы.** Прямая MN проходит через центр I вписанной окружности ω треугольника ABC .

12.8.13. Пусть D — точка на отрезке AC треугольника ABC ; S_1 — окружность, касающаяся отрезков BD и AD , а также окружности Ω внутренним образом; S_2 — окружность, касающаяся отрезков BD и CD , а также окружности Ω внутренним образом.

(а) **Теорема Тебо.** Линия центров окружностей S_1 и S_2 проходит через I .

(б) Докажите, что окружности S_1 и S_2 равны тогда и только тогда, когда $D = B_2$.

12.8.14. Найдите аналоги предложенных задач для «полувписанных» и «обобщённых полувписанных» окружностей, касающихся Ω внешним образом.

Указания, ответы и решения

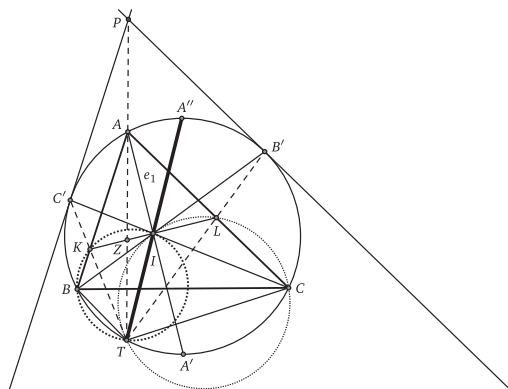


Рис. 1.5:

12.8.1. Это частный случай следующего известного факта: если точки X' , Y' , Z' лежат на прямых YZ , ZX , XY соответственно, то окружности $XY'Z'$, $YZ'X'$, $ZX'Y'$ проходят через одну точку. В данном случае точки B , C , I лежат на прямых, содержащих стороны треугольника AKL , следовательно, окружности BKI , CLI и ABC пересекаются в одной точке.

12.8.2. Из окружностей $TBKI$, $TCLI$ получаем (см. рис. 1.5), что $\angle BTI = \angle AKI = \angle ALI = \angle CTI$. Это означает, что TI — биссектриса угла BTC , поэтому TI проходит через середину дуги A'' .

12.8.14. Комментарий. Есть «алгебраические» причины, по которым, например, вписанная и невписанная окружности обладают похожими свойствами. Уравнение окружности, касающейся трёх данных прямых, — это уравнение либо вписанной, либо одной из невписанных окружностей, разница лишь в геометрическом расположении. Поэтому факты для вписанной окружности зачастую имеют своего «близнеца» для невписанной окружности.

12.9 Обобщённая теорема Наполеона (2*). П. А. Кожевников

Классическая теорема Наполеона гласит, что центры правильных треугольников, построенных на сторонах произвольного треугольника вне его, являются вершинами равностороннего треугольника.

Теорема Наполеона является частным случаем утверждения задачи 16.1.7, п. «Комплексные числа и геометрия». В этом пункте мы докажем другое обобщение теоремы Наполеона.

Предлагаем для решения серию задач, внешне не имеющих никакой связи с теоремой Наполеона. Можно решать задачи любыми методами, а затем познакомиться с обобщением теоремы Наполеона и получить решения задач как следствия этого сильного факта.

Вводные задачи

12.9.1. Докажите, что центры квадратов, построенных на сторонах параллелограмма вне его, являются вершинами квадрата.

12.9.2. На боковых сторонах трапеции $ABCD$ построены треугольники ABE и CDF так, что $AE \parallel CF$ и $BE \parallel DF$. Докажите, что если E лежит на стороне CD , то F лежит на стороне AB .

12.9.3. (а) Две окружности пересекаются в точках A и B . Через точку A проведена прямая, вторично пересекающая первую окружность в точке C , а вторую — в точке D (можно считать, что точки C и D лежат по разные стороны от точки A). Пусть M и N — середины дуг BC и BD , не содержащих точку A , а K — середина отрезка

Формулировка и доказательство обобщённой теоремы Наполеона

Через $\angle(\vec{a}, \vec{b})$ будем обозначать угол поворота от вектора $\vec{a} \neq \vec{0}$ до вектора $\vec{b} \neq \vec{0}$, отсчитываемый против часовой стрелки. Этот угол определён с точностью до прибавления $2\pi k$, $k \in \mathbb{Z}$. Например, равенство $\angle(\vec{a}, \vec{b}) \equiv 0 \pmod{2\pi}$ означает, что $\angle(\vec{a}, \vec{b}) = 2k\pi$ для некоторого $k \in \mathbb{Z}$.

12.9.9.* Обобщённая теорема Наполеона. Пусть на сторонах треугольника ABC построены такие треугольники (возможно, вырожденные) BCA_1 , CAB_1 , ABC_1 , что выполнены следующие условия:

- 1) $\angle(\overrightarrow{A_1B}, \overrightarrow{A_1C}) + \angle(\overrightarrow{B_1C}, \overrightarrow{B_1A}) + \angle(\overrightarrow{C_1A}, \overrightarrow{C_1B}) \equiv 0 \pmod{2\pi}$;
- 2) $AB_1 \cdot BC_1 \cdot CA_1 = BA_1 \cdot CB_1 \cdot AC_1$.

Тогда углы треугольника $A_1B_1C_1$ находятся из равенств

$$\begin{aligned}\angle(\overrightarrow{A_1C_1}, \overrightarrow{A_1B_1}) &\equiv \angle(\overrightarrow{BC_1}, \overrightarrow{BA}) + \angle(\overrightarrow{CA}, \overrightarrow{CB_1}) \pmod{2\pi}; \\ \angle(\overrightarrow{B_1A_1}, \overrightarrow{B_1C_1}) &\equiv \angle(\overrightarrow{CA_1}, \overrightarrow{CB}) + \angle(\overrightarrow{AB}, \overrightarrow{AC_1}) \pmod{2\pi}; \\ \angle(\overrightarrow{C_1B_1}, \overrightarrow{C_1A_1}) &\equiv \angle(\overrightarrow{AB_1}, \overrightarrow{AC}) + \angle(\overrightarrow{BC}, \overrightarrow{BA_1}) \pmod{2\pi}.\end{aligned}$$

Примечание. В теореме предполагается, что точка A_1 отлична от B , C , B_1 , C_1 и т. д. Однако допускается, что вершины каких-то из треугольников BCA_1 , CAB_1 , ABC_1 и $A_1B_1C_1$ лежат на одной прямой. В этом случае говорят, что соответствующий треугольник является вырожденным, а его углы считают равными (с точностью до 2π) 0 , 0 и π .

Таким образом, в теореме утверждается, что при выполнении условий 1 и 2 углы треугольника $A_1B_1C_1$ зависят лишь от углов треугольников, построенных на сторонах треугольника ABC , и не зависят от углов самого треугольника ABC . Условие теоремы может быть описано также таким изящным образом (см. [Bel]): пусть даны точки M, N, P, T и на сторонах треугольника ABC строятся треугольники ABC_1 , BCA_1 , CAB_1 , подобные с сохранением ориентации соответственно треугольникам MNT , NPT , PMT . Действительно, выполнение условий 1 и 2 в этом случае проверяется непосредственно. С другой стороны, если треугольники ABC_1 ,

13.6 Теоремы Птолемея и Кези (3*). А. Д. Блинков, А. А. Заславский

13.6.1 Теорема Птолемея

13.6.1. (а) Докажите, что для любых четырёх различных точек A, B, C, D выполнено *неравенство Птолемея*

$$AB \cdot CD + AD \cdot BC \geq AC \cdot BD.$$

(b) **Теорема Птолемея.** Это неравенство обращается в равенство тогда и только тогда, когда $ABCD$ — вписанный четырёхугольник.

13.6.2. В остроугольном треугольнике ABC обозначим $|BC| = a$, $|AC| = b$. Найдите $|AB|$, если радиус окружности, описанной около $\triangle ABC$, равен R .

13.6.3. Биссектриса угла A треугольника ABC пересекает описанную около него окружность в точке W .

(а) Выразите отношение AW/IW , где I — центр окружности, вписанной в треугольник ABC , через длины сторон треугольника.

(b) Докажите, что $AW > \frac{AB+AC}{2}$.

13.6.4. На гипотенузе AB прямоугольного треугольника ABC во внешнюю сторону построен квадрат, O — его центр. Найдите $|OC|$, если a и b — катеты треугольника.

13.6.5. Дан правильный треугольник ABC и точка P .

(а) Докажите, что если точка P лежит на описанной около треугольника окружности, то расстояние от неё до одной из вершин треугольника равно сумме расстояний до двух других вершин.

(b) **Теорема Помпейю.** Для любой точки P , не лежащей на описанной окружности, из отрезков PA, PB, PC можно составить треугольник.

13.6.6. Сумма расстояний от точки X , выбранной вне квадрата, до двух его ближайших соседних вершин равна m . Найдите наибольшее значение суммы расстояний от X до двух других вершин квадрата.

13.6.7. Точки M и N — середины диагоналей AC и BD вписанного четырёхугольника $ABCD$. Известно, что $\angle ABD = \angle MBC$. Докажите, что $\angle BCA = \angle NCD$. (*Кубок Колмогорова, 1999 г.*)

13.6.8. (а) Точки A, B, C и D — четыре последовательные вершины правильного семиугольника. Докажите, что $\frac{1}{AB} = \frac{1}{AC} + \frac{1}{AD}$.

(б) Докажите, что $\frac{1}{\sin(\pi/7)} = \frac{1}{\sin(2\pi/7)} + \frac{1}{\sin(3\pi/7)}$.

13.6.9. В выпуклом шестиугольнике $ABCDEF$ известно, что $AB = BC = a$, $CD = DE = b$, $EF = FA = c$. Докажите, что $\frac{a}{BE} + \frac{b}{AD} + \frac{c}{CF} \geq \frac{3}{2}$.

13.6.10. Стороны вписанного четырёхугольника равны a, b, c, d . Найдите его диагонали.

13.6.11. Выведите из теоремы Птолемея формулу Карно (см. п. 12.4 «Формула Карно»).

13.6.2 Теорема Кези

13.6.12. Обобщённая теорема Птолемея, или теорема Кези.

(а) Даны четыре непересекающихся круга, ограниченных окружностями $\alpha, \beta, \gamma, \delta$. Докажите, что окружность, касающаяся их внешним образом, или прямая, касающаяся их всех так, что круги лежат относительно неё в одной полуплоскости, существует тогда и только тогда, когда

$$l_{\alpha\beta}l_{\gamma\delta} + l_{\alpha\delta}l_{\beta\gamma} = l_{\alpha\gamma}l_{\beta\delta},$$

где $l_{\alpha\beta}$ — длина общей внешней касательной к окружностям α, β и т. д.

(б) Сформулируйте теорему Кези для случая, когда искомая окружность касается некоторых из данных окружностей внутренним образом.

13.6.13. Сформулируйте утверждение, аналогичное теореме Кези, для случая, когда

- (а) одна;
- (б) две из данных окружностей вырождаются в прямые;
- (с) какие-то из данных окружностей вырождаются в точки.

13.6.14. Пусть на сторонах AC и BC треугольника ABC взяты такие точки X , Y , что $XY \parallel AB$. Докажите, что существует окружность, проходящая через X , Y и касающаяся одинаковым образом вневписанных окружностей треугольника, вписанных в углы A и B .

13.6.15. Докажите **теорему Фейербаха**: окружность, проходящая через середины сторон треугольника, касается его вписанной и вневписанных окружностей.

13.6.16. Докажите, что три окружности, каждая из которых касается внутренним образом одной из вневписанных окружностей треугольника и внешним образом двух других, пересекаются в одной точке.

13.6.17. Даны две окружности, лежащие одна вне другой. Произвольная окружность, касающаяся их одинаковым образом, пересекает одну из их общих внутренних касательных в точках A и A' , а другую — в точках B и B' . Докажите, что среди прямых AB , AB' , $A'B$, $A'B'$ найдутся две, параллельные общим внешним касательным к данным окружностям.

13.6.18. Даны две концентрические окружности a_1 и a_2 . Каждая из окружностей b_1 и b_2 касается внешним образом окружности a_1 и внутренним — a_2 , а каждая из окружностей c_1 и c_2 касается внутренним образом обеих окружностей a_1 и a_2 . Оказалось, что окружности b_1 , b_2 пересекают c_1 , c_2 в восьми точках. Докажите, что эти точки лежат на двух окружностях или прямых, отличных от b_1 , b_2 , c_1 , c_2 . (*В. Протасов, III Олимпиада им. И. Ф. Шарыгина.*)

Указания, ответы и решения

13.6.1. Сделайте инверсию с центром A и воспользуйтесь утверждениями задач 14.10.2, 14.10.5. Заметим, что неравенство Птолемея верно даже для точек, не лежащих в одной плоскости.

13.6.2. Ответ: $\frac{a\sqrt{4R^2-b^2}+b\sqrt{4R^2-a^2}}{2R}$.

Проведите диаметр CD и примените к полученному четырёхугольнику теорему Птолемея.

14 Геометрические преобразования

В данном параграфе задачи расположены так, чтобы сначала новые понятия (геометрических преобразований) использовались для решения интересных задач, формулируемых без этих понятий, и только потом эти новые (но уже мотивированные) понятия изучались сами по себе.

Подробнее о геометрических преобразованиях см., например, [Za03] (теорема Шаля — § 1.2, подобие и гомотетия — § 1.3, аффинные преобразования — гл. 2, проективные преобразования — гл. 3, инверсия — гл. 4, комплексная интерпретация движений и подобий — § 6.1, комплексная интерпретация инверсии — § 6.2), [Pr95] и [Ya75].

14.1 Применения движений. (1) А. Д. Блинков

Поворотом вокруг точки O на угол φ называется преобразование плоскости, оставляющее точку O на месте и переводящее любую отличную от O точку X в такую точку X' , что $|OX| = OX'$ и ориентированный угол между векторами $\overrightarrow{OX}$ и $\overrightarrow{OX'}$ равен φ . Поворот на 180° называется *центральной симметрией*.

Параллельным переносом на вектор $\vec{m}$ называется преобразование плоскости, переводящее любую точку X в такую точку X' , что $\overrightarrow{XX'} = \vec{m}$.

Осевой симметрией относительно прямой l называется преобразование плоскости, переводящее любую точку X в такую точку X' , что $XX' \perp l$ и точки X, X' лежат по разные стороны от прямой l и равноудалены от неё.

14.1.1.° Параллелограмм имеет ровно четыре оси симметрии. Какое из следующих утверждений верно?

- 1) это прямоугольник, отличный от квадрата;
- 2) это ромб, отличный от квадрата;
- 3) это квадрат;
- 4) такого параллелограмма не существует.

14.1.2.° Треугольник имеет центр симметрии. Какое из следующих утверждений верно?

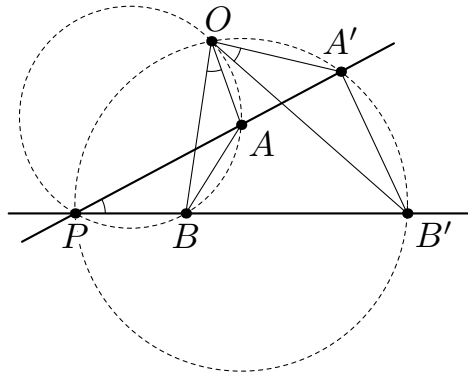


Рис. 1.41:

Это означает, что существует поворотная гомотетия, переводящая отрезок AA' в $[BB']$, причём O — её центр.

Пусть P — точка пересечения данных прямых, а α — угол между ними. Так как при поворотной гомотетии с центром O образом точки A является точка B , отрезок AB должен быть «виден» из точки O под углом α . Следовательно, O лежит на дуге окружности, описанной около треугольника APB . Аналогично отрезок $A'B'$ должен быть «виден» из точки O под углом α , значит, точка O лежит на дуге окружности, описанной около треугольника $A'PB'$. Таким образом, O — вторая точка пересечения этих окружностей.

Если построенные окружности касаются, значит, обе точки проходят через P одновременно. В этом случае точка P сама будет искомой.

14.5 Поворотная гомотетия (2). П. А. Кожевников

14.5.1 Вводные задачи: немного о велосипедистах

14.5.1. По двум окружностям, пересекающимся в точках P и Q , одновременно начали движение из точки P по часовой стрелке с равными угловыми скоростями два велосипедиста A и B .

- (а) Докажите, что прямая AB всё время проходит через Q .
- (б) Докажите, что треугольники PAB всё время подобны друг другу и треугольнику PO_1O_2 , где O_1 и O_2 — центры окружностей.
- (с) Найдите ГМТ (траекторию движения) середин отрезков AB ; центров вписанных окружностей треугольников PAB ; любых соот-

ветственных точек подобных треугольников PAB .

(d) **Задача о велосипедистах.** Докажите, что A и B всё время равноудалены от фиксированной точки. (См. [VSh].)

14.5.2. По трём окружностям, имеющим общую точку O и попарно различные точки пересечения P , Q и R , одновременно начали движение из точки O по часовой стрелке с равными угловыми скоростями три велосипедиста A , B и C .

(a) Докажите, что все треугольники ABC подобны между собой и треугольнику $O_1O_2O_3$, где O_1 , O_2 и O_3 — центры окружностей.

(b) Какова траектория движения центра масс треугольника ABC ?

14.5.3. Два велосипедиста P и Q едут равномерно по двум прямым, пересекающимся в точке O .

(a) Найдите траекторию середины отрезка PQ .

(b) Докажите, что если скорости велосипедистов равны, то середина дуги (одной из дуг) PQ окружности OPQ неподвижна.

(c) Докажите, что если велосипедисты проходят O не одновременно, то окружности OPQ имеют вторую общую точку, отличную от O .

14.5.4. Дан фиксированный треугольник ABC . По прямым BC , CA , AB едут соответственно велосипедисты P , Q , R так, что углы между RP и PQ , PQ и QR , QR и RP фиксированные.

(a) Докажите, что точка пересечения окружностей RAQ , RBP , PCQ неподвижна.

(b) Найдите ГМТ центров вписанных окружностей треугольников PQR .

14.5.2 Основные задачи

14.5.5. Три велосипедиста P , Q и R едут равномерно по трём прямым. Известно, что в некоторые два момента времени треугольник PQR был подобен с сохранением ориентации фиксированному треугольнику XYZ . Докажите, что это условие будет выполняться в любой момент времени.

14.5.6. В треугольник ABC вписан подобный ему треугольник PQR ($P \in BC$, $Q \in CA$, $R \in AB$, $\angle P = \angle A$, $\angle Q = \angle B$, $\angle R = \angle C$).

(а) Докажите, что центр описанной окружности треугольника ABC совпадает с ортоцентром треугольника PQR .

(б) Найдите максимальное значение выражения $\frac{S_{ABC}}{S_{PQR}}$.

(с) Докажите, что центр описанной окружности треугольника PQR равноудалён от центра описанной окружности и ортоцентра треугольника ABC .

14.5.7. Через вершины треугольника ABC проводятся три произвольные параллельные прямые d_a, d_b, d_c . Прямые d'_a, d'_b, d'_c , симметричные d_a, d_b, d_c относительно BC, CA, AB соответственно, образуют треугольник XYZ . Найдите геометрическое место центров вписанных окружностей таких треугольников.

14.5.8. Дан выпуклый четырёхугольник $ABCD$, стороны BC и AD которого равны, но не параллельны. Пусть E и F — внутренние точки отрезков BC и AD соответственно, удовлетворяющие условию $BE = DF$. Прямые AC и BD пересекаются в точке P , прямые BD и EF пересекаются в точке Q , прямые EF и AC пересекаются в точке R . Докажите, что для всевозможных способов выбора точек E, F окружности PQR имеют общую точку, отличную от P . (См. [IMO], 2005 г.)

14.5.9. Пусть O и I — центры описанной и вписанной окружностей треугольника ABC соответственно. Точки D, E и F выбраны на сторонах BC, CA и AB соответственно так, что $BD + BF = CA$ и $CD + CE = AB$. Описанные окружности треугольников BDF и CDE пересекаются в точках D и P . Докажите, что $OP = OI$. (См. [IMO], 2012 г.)

14.5.3 Дополнительные задачи

14.5.10. Впишите в данный остроугольный треугольник равносторонний треугольник с минимальной стороной.

14.5.11. На пол положили правильный треугольник ABC , выпиленный из фанеры. В пол вбили три гвоздя (по одному вплотную к каждой стороне треугольника) так, что треугольник невозможно повернуть, не отрывая от пола. Первый гвоздь делит сторону AB

в отношении $1 : 3$, считая от вершины A , а второй делит сторону BC в отношении $2 : 1$, считая от вершины B . В каком отношении делит сторону AC третий гвоздь? (*Московская математическая олимпиада 1998 г.*)

14.5.12. Выпуклый многоугольник M можно поместить в треугольник T . Докажите, что это можно сделать так, чтобы одна из сторон многоугольника M лежала на стороне треугольника T .

Поворотной гомотетией называют преобразование $H_O^{k,\varphi} := H_O^k \circ R_O^\varphi$.

14.5.13. (а) Окружности α и β пересекаются в точках A и B . Пусть H — поворотная гомотетия с центром в точке A , переводящая α в β . Докажите, что для любой точки $X \in \alpha$ точка $H(X)$ получена пересечением прямой BX с окружностью β . (См. [Pr95, 19.27].)

(б) Окружности $S_1, \dots, S_n$ проходят через точку O . Кузнечик из точки $X_i \in S_i$ прыгает в точку $X_{i+1} \in S_{i+1}$ так, что прямая $X_i X_{i+1}$ проходит через вторую точку пересечения окружностей S_i и S_{i+1} . Докажите, что после n прыжков (с S_1 на $S_2, \dots$, с S_n на S_1) кузнечик вернётся в исходную точку. (См. [Pr95, 19.28].)

(с) Пусть концы отрезков AB и CD попарно различны, а P — точка пересечения прямых AB и CD . Центром поворотной гомотетии, переводящей AB в CD , является (отличная от P) точка пересечения описанных окружностей треугольников ACP и BDP . (См. [Pr95, 19.41 (б)].)

Указания, ответы и решения

14.5.1. (а) Из равенства угловых скоростей следует, что $\angle(PQ, QA) = \angle(PQ, QB)$.

(б) Угол $\angle(BA, AP) = \angle(QA, AP)$ постоянный и равен $\angle(O_2 O_1, O_1 P)$.

(с) Если M — середина AB , то $\angle(QM, MP)$ постоянный, поэтому M движется по окружности Γ , проходящей через P и Q .

Пусть N — любая точка треугольника PAB (в некоторый фиксированный момент). Рассмотрим поворотную гомотетию (см. определение перед задачей 14.5.13) с центром P , переводящую A в N .

15.3 Полярное соответствие (2). А. А. Гаврилюк, П. А. Кожеников

Традиционно при изучении полярного соответствия существенно используются свойства проективных преобразований. Мы же делаем попытку познакомиться с полярным соответствием и применением его свойств без привлечения проективной геометрии.

Введём нужные нам определения и обозначения. Пусть на плоскости фиксированы точка O и окружность ω радиуса R с центром в O .

Для каждой точки $X \neq O$ на луче OX строим такую точку X' , что $OX \cdot OX' = R^2$. (Говорят, что X' и X *инверсны* относительно окружности ω .) Через точку X' проведём прямую x , перпендикулярную OX' . Прямая x называется *полярной* точки X , а точка X называется *полюсом* прямой x . Соответствие $X \leftrightarrow x$ является взаимно однозначным соответствием между точками, отличными от O , и прямыми, не проходящими через O . Это соответствие и называется *полярным соответствием*.

Ниже мы обозначаем точки, отличные от O (полюсы), большими латинскими буквами, а их поляры — соответствующими маленькими буквами: $A \leftrightarrow a$, $B \leftrightarrow b$, $C \leftrightarrow c$, ...

Основные свойства и вводные задачи

Установите два основных свойства полярного соответствия.

П1. Двойственность. Включение $A \in b$ выполняется тогда и только тогда $B \in a$, т. е. поляра любой точки является геометрическим местом полюсов проходящих через неё прямых.

П2.* Пусть две прямые m и l , проходящие через произвольную точку $A \notin \omega$, пересекают ω в точках M_1, M_2 и L_1, L_2 . Тогда $M_1L_1 \cap M_2L_2 \in a$ или $M_1L_1 \parallel M_2L_2 \parallel a$.

Докажите следующие факты.

В1. Если $A \in \omega$, то a — это касательная к ω , проведённая через A .

В2. Если точка A расположена вне окружности ω , то a проходит через точки касания с ω касательных, проведённых через A .

В3. Если O, A, B не лежат на одной прямой, то $a \cap b \leftrightarrow AB$.

В4. Точки A, B, C лежат на одной прямой тогда и только тогда, когда a, b, c проходят через одну точку или параллельны.

Основные задачи

15.3.1.° Даны окружность и её хорда AB . Где лежит точка пересечения поляр точек A и B ?

- 1) внутри окружности; 2) вне окружности; 3) на окружности.

15.3.2.° Пусть C — середина хорды AB . Тогда поляр точки C

- 1) параллельна AB ;
2) перпендикулярна AB ;
3) касается окружности.

15.3.3.° При полярном соответствии относительно вписанной окружности треугольник переходит

- 1) в серединный треугольник;
2) в ортотреугольник;
3) в треугольник, образованный точками касания сторон с вписанной окружностью.

15.3.4. Даны окружность ω и прямая l , не имеющие общих точек. Из точки X , которая движется по прямой l , проводятся касательные XA, XB к ω . Докажите, что все хорды AB имеют общую точку.

15.3.5. Симметричная бабочка. (а) Дана точка A на диаметре BC полуокружности ω . Точки X, Y на ω таковы, что $\angle XAB = \angle YAC$. Докажите, что прямые XY проходят через одну точку или параллельны.

(б) Точки A и A' инверсны относительно окружности ω , причём точка A' расположена внутри ω . Через A' проводятся хорды XY . Докажите, что центры вписанной и одной из невписанных окружностей треугольника AXY фиксированны. (*С. Маркелов, см. [Sh97].*)

15.3.6. Основное свойство симедианы. Касательные к описанной окружности треугольника ABC , проведённые через точки B

и C , пересекаются в точке P . Докажите, что AP — симедиана (т. е. прямая, симметричная медиане AM относительно биссектрисы угла A).

15.3.7. Гармонический четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность ω . Известно, что касательные к ω , проведённые в точках A и C , пересекаются на прямой BD или параллельны BD . Докажите, что касательные к ω , проведённые в точках B и D , пересекаются на прямой AC или параллельны AC .

В следующих трёх задачах дан четырёхугольник $ABCD$, у которого диагонали пересекаются в точке P , продолжения сторон AB и CD — в точке R , продолжения сторон BC и DA — в точке Q .

15.3.8. Вписанный четырёхугольник. Пусть четырёхугольник $ABCD$ вписан в окружность с центром O . Докажите, что четвёрка точек O, P, Q, R ортоцентрическая (т. е. каждая точка является ортоцентром треугольника с вершинами в оставшихся трёх точках).

15.3.9. Описанный четырёхугольник. Пусть четырёхугольник $ABCD$ описан около окружности; K, L, M, N — точки касания с окружностью сторон AB, BC, CD, DA соответственно; прямые KL и MN пересекаются в точке S , а прямые LM и NK — в точке T .

(а) Докажите, что точки Q, R, S, T лежат на одной прямой.

(б) Докажите, что KM и LN пересекаются в точке P .

15.3.10. Вписанно-описанный четырёхугольник. Четырёхугольник $ABCD$ описан около окружности ω с центром I и вписан в окружность Ω с центром O .

(а) Докажите, что O, I, P лежат на одной прямой.

(б) Зафиксируем ω и Ω и рассмотрим всевозможные четырёхугольники $ABCD$, описанные около окружности ω и вписанные в окружность Ω . Докажите, что для всех таких четырёхугольников точки P совпадают, а также что прямые QR совпадают.

Комментарий. Согласно теореме Понселе если существует хотя бы один четырёхугольник, описанный около окружности ω и вписанный в окружность Ω , то существует бесконечно много таких четырёхугольников.

16.1 Комплексные числа и элементарная геометрия.

Пусть на плоскости задана система координат. Тогда комплексному числу $z = x + yi$ соответствует точка плоскости Z с координатами (x, y) . При этом модуль числа z равен расстоянию от Z до начала координат O , а аргумент равен ориентированному углу между положительным направлением оси Ox и вектором $\overrightarrow{OZ}$, т. е. углу, на который надо повернуть против часовой стрелки ось Ox , чтобы совместить её положительное направление с направлением вектора $\overrightarrow{OZ}$. Оси Ox и Oy называют *действительной* и *мнимой* осями.

16.1.1. (Загадка.) Выясните геометрический смысл сложения комплексных чисел.

16.1.2. (а) Каким геометрическим преобразованием комплексной плоскости получается число iz из числа z ?

(б) (Загадка.) Обозначим $e^{i\varphi} := \cos \varphi + i \sin \varphi$. Каков геометрический смысл умножения на $e^{i\varphi}$? А на $re^{i\varphi}$, где r — вещественное число (см. определение тригонометрической формы комплексного числа в п.4.5)

(с) Выразите число w , полученное из числа z поворотом на угол φ против часовой стрелки относительно центра z_0 , через z , z_0 и φ .

(d) Докажите, что композиция поворотов плоскости (с различными центрами) — поворот или параллельный перенос.

(е) Докажите, что точки z_1, z_2, z_3 лежат на одной прямой тогда и только тогда, когда отношение $(z_3 - z_1)/(z_2 - z_1)$ вещественно.

Комментарий. Задача 16.1.2 (b) легко решается с помощью тригонометрических формул сложения. Однако можно поступить наоборот: решить эту задачу геометрически, доказать, что при умножении комплексных чисел их модули перемножаются, а аргументы складываются, а затем, используя этот результат, получить доказательство формул сложения, не требующее перебора различных случаев.

16.1.3.° Какое преобразование плоскости задаётся формулой $z \mapsto 2z + 2$?

Теперь воспользуемся тем, что аффинное преобразование однозначно определяется образами трёх точек, не лежащих на одной прямой. Пусть точки $0, 1$ и i переходят в z_0, z_1, z_2 соответственно. Тогда данное преобразование задаётся формулой требуемого вида, в которой $c = z_0$, $a = (z_1 + z_2 - 2z_0)/2$, $b = (z_1 - z_2)/2$. Из того, что z_0, z_1, z_2 не лежат на одной прямой, следует, что $|a| \neq |b|$.

16.1.7. Пусть $\varepsilon = \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$. Тогда точки $1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{n-1}$ являются вершинами правильного n -угольника. Согласно предыдущей задаче можно считать, что вершинами данного многоугольника являются точки $a\varepsilon^k + b\varepsilon^{-k}$, $k = 0, 1, \dots, n-1$. Значит, центр k -го правильного n -угольника z_k удовлетворяет равенству $a\varepsilon^{k+1} + b\varepsilon^{-k-1} - z_k = \varepsilon(a\varepsilon^k + b\varepsilon^{-k} - z_k)$. Отсюда легко получить, что z_k образуют геометрическую прогрессию с знаменателем ε , т. е. являются вершинами правильного n -угольника.

16.2 Комплексные числа и круговые преобразования.

Преобразование круговой плоскости, сохраняющее обобщённые окружности, называется *круговым*. Произвольное отличное от тождества круговое преобразование может быть представлено как композиция инверсии и движения.

16.2.1.° Четвёрка комплексных чисел z_1, z_2, z_3, z_4 удовлетворяет равенству $\frac{(z_1 - z_3)(z_2 - z_4)}{(z_1 - z_4)(z_2 - z_3)} = 2$. Что можно сказать о четвёрке точек плоскости, соответствующих числам z_1, z_2, z_3, z_4 ?

- 1) Они являются вершинами параллелограмма.
- 2) Они лежат на одной прямой или на одной окружности.
- 3) Площадь треугольника $0z_1z_2$ равна площади треугольника $0z_3z_4$ (точка 0 — начало координат).

16.2.2. Докажите, что преобразование комплексной плоскости является круговым тогда и только тогда, когда оно задаётся дробно-линейной функцией вида $f(z) = (az + b)/(cz + d)$ или $f(z) = (a\bar{z} + b)/(c\bar{z} + d)$, где $ad - bc \neq 0$.

16.2.3. Докажите, что для любых шести различных точек A, B, C, A', B', C' существует ровно два круговых преобразования, переводящих A в A' , B в B' , C в C' .

Двойным отношением четырёх комплексных чисел a, b, c, d , где $a \neq d, b \neq c$, называется комплексное число $(a, b, c, d) = \frac{(a-c)(b-d)}{(a-d)(b-c)}$.

16.2.4. Докажите, что для данных восьми различных точек $A, B, C, D; A', B', C', D'$ круговое преобразование, переводящее A в A', B в B', C в C', D в D' , существует тогда и только тогда, когда для соответствующих комплексных чисел выполняется равенство $(a, b, c, d) = (a', b', c', d')$ или $\overline{(a, b, c, d)} = (a', b', c', d')$.

16.2.5. Даны два треугольника ABC и $A'B'C'$. Докажите, что существует инверсия, переводящая треугольник ABC в треугольник, равный $A'B'C'$.

16.2.6. Дан четырёхугольник $ABCD$. Докажите, что существует инверсия, переводящая его вершины в вершины параллелограмма, причём все параллелограммы, полученные в результате таких инверсий, подобны.

См. также задачу 14.10.4(с) п. «Инверсия».

Дополнительные задачи

16.2.7. (а) Пусть a, b, c — комплексные числа, соответствующие не лежащим на одной прямой точкам A, B, C ; $f(z) = (z-a)(z-b)(z-c)$. Докажите, что две точки, соответствующие корням производной $f'(z)$, изогонально сопряжены относительно треугольника ABC .

(б)* *Эллипсом Штейнера* треугольника ABC называется эллипс наибольшей площади, лежащий внутри треугольника. Докажите, что фокусы эллипса Штейнера соответствуют корням производной $f'(z)$.

16.2.8. Пусть a, b, c — комплексные числа, соответствующие точкам A, B, C , причём $|a| = |b| = |c| = 1$. Докажите, что точки Z_1, Z_2 изогонально сопряжены относительно треугольника ABC тогда и только тогда, когда соответствующие комплексные числа удовлетворяют соотношению

$$z_1 + z_2 + abc\bar{z}_1\bar{z}_2 = a + b + c.$$

сторонах четырёхугольника, проходящий через середины его диагоналей, за исключением концов.

Для параллелограмма ответ очевиден.

Пусть P и Q — середины диагоналей AC и BD данного четырёхугольника, отличного от параллелограмма (см. рис. 1.54 б). Тогда $S_{ABP} + S_{CDP} = S_{ABQ} + S_{CDQ} = S_{ABCD}/2$.

Если точка M лежит внутри $ABCD$ на PQ , то $S_{APM} = S_{CPM}$ (так как точки A и C равноудалены от PM) и $S_{BPM} = S_{DPM}$ (так как точки B и D равноудалены от PM). Таким образом, $S_{ABM} + S_{CDM} = S_{ABP} + S_{CDP} + S_{APM} + S_{BPM} - S_{CPM} - S_{DPM} = S_{ABP} + S_{CDP} = S_{ABCD}/2 = S_{ADM} + S_{BCM}$.

Если точка M не лежит на указанном отрезке, то, действуя аналогично, проверяем, что указанное в условии равенство не выполняется.

17.3 Построения. Ящик инструментов (2). А. А. Гаврилюк

При изучении материала этого раздела желательно знакомство с § 13 «Окружность» и рекомендованной в нем литературой.

17.3.1. (а) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его пополам.

(б) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки удвойте его.

(с) Даны две параллельные прямые, на одной из которых дан отрезок. С помощью одной линейки разделите его на n равных частей.

Ср. с задачей 14.9.5 п. «Центральная проекция и проективные преобразования».

17.3.2. Даны окружность ω , её диаметр AB и точка X . С помощью одной линейки постройте перпендикуляр из точки X на AB , если точка X лежит

(а) не на окружности; (б) на окружности.

17.3.3. Даны окружность ω и точка X . С помощью одной линейки постройте (все возможные) касательные, проведённые из точки X к окружности, если точка X лежит

(а) вне окружности; (б) на окружности.

17.3.4. При помощи только циркуля постройте образ данной точки X при инверсии относительно данной окружности ω .

17.3.5. Дана окружность на плоскости. С помощью двусторонней линейки постройте её центр. (С помощью двусторонней линейки можно проводить прямую через две точки, проводить прямую, параллельную проведённой ранее прямой и отстоящую от неё на расстояние, равное ширине линейки, а также проводить через две точки, расстояние между которыми не меньше ширины линейки, две параллельные прямые, расстояние между которыми равно ширине линейки.)

17.3.6. Даны прямая l и отрезок OA , ей параллельный. С помощью двусторонней линейки постройте точки пересечения прямой l с окружностью радиуса OA и с центром в точке O .

17.3.7. При помощи только циркуля постройте окружность, проходящую через три данные точки.

17.3.8. Задача Аполлония. Постройте окружность, касающуюся трёх данных, при помощи циркуля и линейки.

В последующих задачах этого пункта *построением* будем называть некоторую последовательность следующих элементарных операций:

- с помощью линейки провести прямую через две данные или ранее построенные точки;
- с помощью циркуля построить окружность с центром A и радиусом BC , где A, B, C — данные или ранее построенные точки;
- найти точки пересечения двух данных или ранее построенных линий (прямых или окружностей).

В последующих теоремах никакие другие операции не разрешаются (в отличие от предыдущих задач, где разрешена, например, операция «взять произвольную точку уже построенного множества»). В частности, если изначально не даны хотя бы две точки, ничего построить нельзя.

17.3.9.* Теорема. Отрезок длины a можно построить циркулем и линейкой, имея отрезок длины 1, тогда и только тогда, когда число a можно получить из числа 1 при помощи сложений, вычитаний, умножений, делений на ненулевые числа и извлечений квадратных корней из положительных чисел.

17.3.10.* Теорема (Мор—Маскерони). Любое построение, осуществимое циркулем и линейкой, можно осуществить одним циркулем (прямая считается построенной, если построены две различные лежащие на ней точки, см. [Fu87]).

17.3.11.* Теорема (Штейнер). Любое построение, осуществимое циркулем и линейкой, можно осуществить одной линейкой, если начерчена одна окружность и отмечен её центр (окружность считается построенной, если построены её центр и лежащая на ней точка, см. [Smo]).

Следующая задача предназначена для закрепления материала.

17.3.12.° Пользуясь теоремами Мора—Маскерони и Штейнера, определите, какие инструменты необходимы для построения центра данной окружности.

1) циркуль и линейка; 2) только линейка; 3) только циркуль.

Указания, ответы и решения

17.3.1. (а) Пусть AB — данный отрезок. Возьмём точку X вне полосы, ограниченной данными прямыми, и найдём точки C и D пересечения прямых XA и XB с прямой, отличной от AB . Пусть Y — точка пересечения диагоналей трапеции $ABCD$. Тогда прямая XY делит основания трапеции пополам.

(b) Возьмите на другой прямой произвольный отрезок и разделите его пополам.

(с) Возьмите на другой прямой произвольный отрезок и, повторив несколько раз предыдущее построение, увеличьте его в n раз.

17.3.2. Если прямые XA , XB вторично пересекают окружность в точках B' , A' , то точка пересечения прямых AA' и BB' — ортоцентр треугольника XAB .

- [fest] Шесть фестивалей (материалы Российских фестивалей юных математиков). Краснодар: ГИНМЦ, 1996.
- [Fu87] *Фукс Д.* Построения одним циркулем // Квант. 1987. № 7. С. 34–37.
- [Smo] *Смогоржевский А. С.* Линейка в геометрических построениях. М.: Гостехиздат, 1956.

18 Стереометрия

Чужбина так же сродственна отчизне,
Как тупику соседствует пространство.

И. Бродский.

18.1 Задачи на пространственное воображение

М. А. Корчемкина, И. А. Пушкарёв

Задачи о траекториях придуманы по мотивам [Do, SE], а многие задачи о фигурах из кубиков — по мотивам [Ag], см. также [R].

18.1.1 Фигуры из кубиков

Будем рассматривать три (ортогональные) проекции пространственной фигуры — вид спереди, сверху и справа (см. пример на рис. 1.56).

18.1.1. Существует ли фигура, не являющаяся кубом, проекция которой на каждую грань некоторого куба совпадает с проекцией всего этого куба?

Игрушкой будем называть фигуру, склеенную из одинаковых кубиков (границы склеиваются целиком), если из каждого кубика можно добраться до любого другого, переходя из кубика в кубик только через соприкасающиеся грани. Если у Вас есть кубики, то перед рисованием игрушки можете сделать ее модель.

18.1.2. (a,b) Нарисуйте игрушку по трём её проекциям на рис. 1.56.

(c) (Загадка) Однозначно ли игрушка восстанавливается по трём её проекциям?

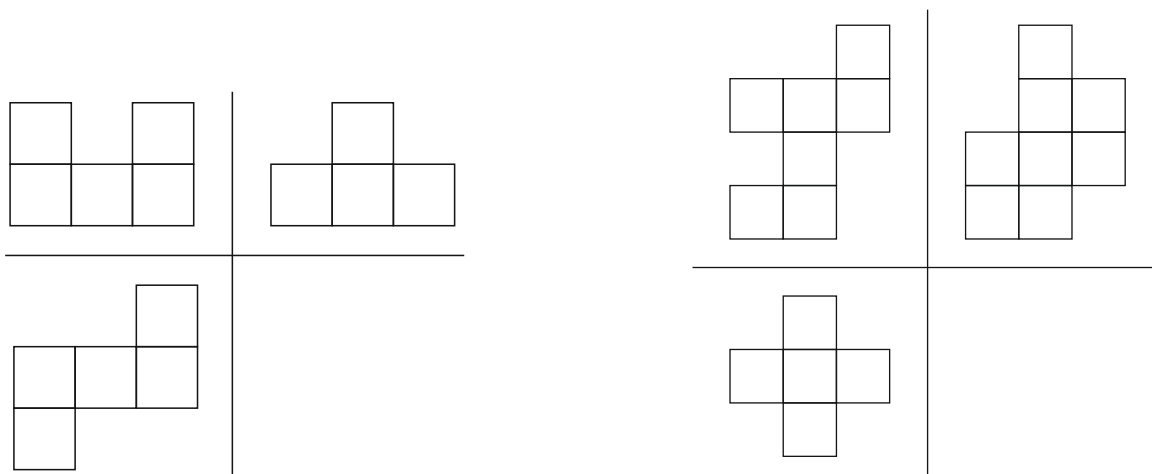


Рис. 1.56: Три проекции

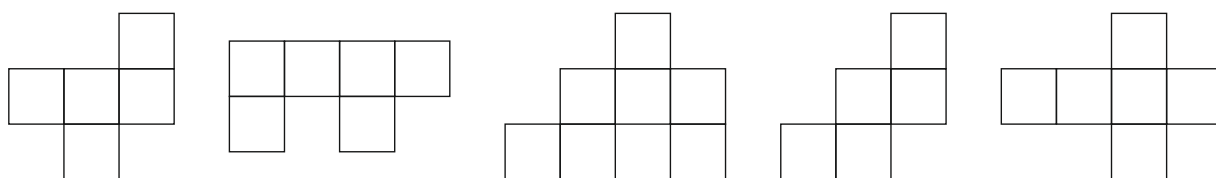


Рис. 1.57: Клетчатые фигуры

18.1.3. (а) Из клетчатых фигур на рис. 1.57 выберите три, которые могут быть тремя проекциями одной и той же игрушки (вращать клетчатые фигурки нельзя). Нарисуйте эту игрушку.

(б) Для какой-нибудь другой тройки клетчатых фигур из приведенных (на Ваш выбор) объясните, почему она не может образовывать набор трех проекций одной и той же игрушки.

18.1.2 Траектории

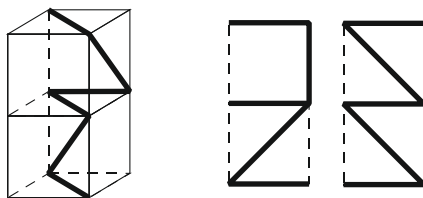


Рис. 1.58: Линия в параллелепипеде



Рис. 1.59: Восстановите линию в параллелепипеде по ее проекциям

18.1.4. (а) В параллелепипеде размера $1 \times 1 \times 2$ нарисовали линию, см. рис. 1.58 слева. Изобразите её вид спереди и справа.

(b,c) Восстановите линию в параллелепипеде размера $1 \times 1 \times 2$ по её видам спереди и справа, см. рис. 1.59.

(d) (Загадка) Однозначно ли восстанавливается линия по двум её проекциям?

18.1.3 Рисование

18.1.5. (a,b) На поверхности стеклянного куба нарисовали линию, см. рис. 1.60 (представьте себе, что по поверхности куба проползла улитка, оставляя за собой заметный след). Изобразите её вид спереди, сверху и справа.

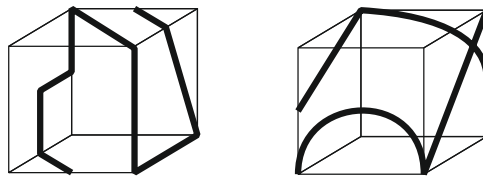


Рис. 1.60: Линии на поверхности стеклянного куба

18.1.6. (a,b) По видам спереди, сверху и справа на рис. 1.61 восстановите линию в кубе (т.е. проходящую по поверхности или внутри куба; представьте себе, что куб заполнен водой и внутри получившегося аквариума или вдоль его стенок может плавать рыбка).

вид спереди вид сверху вид справа

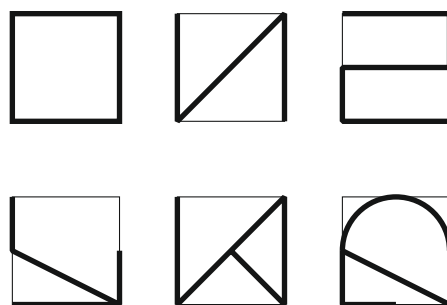


Рис. 1.61: Проекции линии в кубе

18.2 Рисование. А. Б. Скопенков (1-2)

Предмет математики настолько серьезен, что полезно не упускать случаев делать его немного занимательным.

Б. Паскаль.

Пространственное воображение необходимо в разных областях знания и техники, прежде всего в математике, программировании и физике. Более того, эти науки часто работают с многомерным пространством! Поэтому полезно и рано начинать развитие пространственного воображения, и не пропускать это развитие, даже если не получилось начать рано. Пространственное воображение является важным предварительным умением, а его развитие — одной из сверхзадач школьного курса стереометрии и даже базовых университетских курсов геометрии и топологии.³

При этом многие задачи в этом тексте являются скорее занимательными, чем математическими. Для их решения не требуется предварительных знаний по стереометрии. Они использовались для 6-11 классников на кружках «Олимпиады и математика» в школе «Интеллектуал» и МЦНМО, а также в Московской летней математической школе. Благодарю А.И. Сгибнева за обсуждения.

18.2.1. Нарисуйте сечение куба плоскостью, которое является

³Например, несколько первых занятий курсов топологии на ФИВТ и ФОПФ МФТИ отведены на такие задачи [Ку]. Из приведенных ниже задач используются лишь немногие, в основном разбираются «топологические» наглядные задачи [Sk, §2], см. также [Fr].

- (а) правильным треугольником; (b) квадратом;
- (с) правильным шестиугольником.

Сообразите, почему сечение куба плоскостью не может быть правильным n -угольником при $n \geq 7$. Оно не может быть и правильным пятиугольником. Но чтобы доказать это, нужны минимальные знания по стереометрии.

18.2.2. Из 27 одинаковых кубиков составлен куб $3 \times 3 \times 3$. Нарисуйте

- (а) ежа (т.е. объединение центрального кубика и кубиков, имеющих с ним общую грань);
- (b) то, что получается при выкидывании угловых кубиков из куба;
- (с) то, что получается при выкидывании ежа из куба.

18.2.3. Можно ли пространство заполнить попарно непересекающимися ежами?

18.2.4. Нарисуйте пространственную фигуру, три проекции которой являются («заполненными», т.е. двумерными) треугольником, квадратом и кругом, соответственно.

18.2.5. (а) Нарисуйте пересечение правильного тетраэдра с тетраэдром, полученным из него поворотом на 90° относительно прямой, соединяющей середины противоположных рёбер.

(b) То же для объединения.

(с)* Нарисуйте объединение куба с кубом, полученным из него поворотом на 60° относительно большой диагонали.

(d)* Для каждой грани тетраэдра проведем две параллельные ей плоскости, делящие каждое ребро, не лежащее в этой грани, на три равных отрезка. На сколько частей разбивают тетраэдр проведенные плоскости?

18.2.6. (а) Как на двух гвоздях, вбитых в плоскую стену, повесить замкнутую веревку (с тяжелой медалью), чтобы веревка не падала, но после вынимания любого гвоздя падала?

(b) Нарисуйте в пространстве три резиновые кольца, которые нельзя расцепить, но после разрезания любого из них они расцеплялись бы.

18.3.21. (а) Укажите два вращения правильного додекаэдра, композициями которых можно получить любое другое.

(б) Постройте биекцию, сохраняющую композицию, между множеством вращений додекаэдра и множеством чётных перестановок пяти элементов.

18.4 Многомерье (4^*). А. Я. Канель-Белов

18.4.1 Простейшие многогранники в многомерном пространстве. Ю. М. Бурман, А. Я. Канель-Белов

Хорошо известно, что точке плоскости можно сопоставить пару чисел — её декартовых координат (для этого нужно предварительно выбрать систему координат, то есть начало координат и оси). Тем самым плоскость можно понимать просто как множество всевозможных пар (x_1, x_2) действительных чисел. Аналогично трёхмерное пространство можно считать просто множеством всевозможных троек (x_1, x_2, x_3) . Накладывая на числа различные ограничения, мы получим описание разнообразных подмножеств плоскости и пространства (плоских фигур и трёхмерных тел).

18.4.1.° Даны три набора условий на числа x_1, x_2, x_3 :

1) $x_1 = x_2 = 2x_3$;

2) $x_1 + 2x_2 + 3x_3 = 0$, $3x_1 + 2x_2 + x_3 = 1$;

3) $x_1^2 + x_2^2 - 2x_3 = -1$.

Какие из них задают прямую в трёхмерном пространстве?

Когда измерений больше, чем три, координатный подход становится ведущим: удобно *определить*, скажем, четырёхмерное пространство как множество всевозможных наборов (x_1, x_2, x_3, x_4) из четырёх действительных чисел.

В этом пункте *отрезком* мы будем называть множество $[-1, 1] = \{x: |x| \leq 1\}$ чисел, по модулю не превосходящих 1; *квадратом* — множество $[-1, 1]^2 = \{(x_1, x_2): |x_1|, |x_2| \leq 1\}$ пар чисел, каждое из которых по модулю не превосходит 1; *кубом* — множество $[-1, 1]^3 = \{(x_1, x_2, x_3): |x_1|, |x_2|, |x_3| \leq 1\}$ троек таких чисел; *четырёхмерным кубом* — четвёрок и т. д. См. рисунок 1.65.

18.4.18. Докажите, что любое n -мерное сечение $(n + 1)$ -мерного куба, перпендикулярное диагонали и проходящее через вершину, комбинаторно эквивалентно «зоне» в n -мерном кубе между двумя аналогичными сечениями. Точнее, пусть $L_n(a, b) = \{(x_1, \dots, x_n) \mid x_i \in [0, 1], a \leq x_1 + \dots + x_n \leq b\}$. Докажите, что $L_{n+1}(k, k)$ комбинаторно эквивалентно $L_n(k - 1, k)$. Начните со случая $n = 3, k = 2$.

18.4.19. Пусть (гипер)плоскость $\sum_{i=1}^n a_i x_i = c$, где $n > 2, a_i > 0$, числа a_i взаимно простые в совокупности, пересекает единичную решётку, состоящую из кубов. Докажите, что количество возникающих частей с точностью до параллельных переносов равно $\sum_{i=1}^n a_i$.

18.4.20. Дан n -мерный куб с центром в начале координат, координаты вершин которого равны ± 1 . Число n мы будем называть *адамаровым*, если можно указать набор из n попарно ортогональных векторов с координатами ± 1 . Докажите, что числа 1, 2, 4, 8 хорошие, а числа 3, 5, 6 — нет.

18.4.21. Докажите, что адамарово число, большее 2, имеет вид $4k$.

18.4.22. Докажите что все степени двойки — адамаровы числа.

18.4.23. Докажите, что число 12 адамарово.

18.4.24. Докажите, что число 20 адамарово.

Очень важная открытая проблема: верно ли, что все числа вида $4k$ адамаровы? См. подробнее [GDI, п. 7.2] и приведенные там ссылки.

18.4.2 Многомерные объёмы

Объём n -мерного многогранника определяется аналогично площади фигуры на плоскости (см. п. 26.5 «Принцип Дирихле и его применения в геометрии»).

Объёмом n -мерных многогранников называется заданная на множестве многогранников неотрицательная функция V , удовлетворяющая следующим условиям:

— если многогранник M_1 можно движением перевести в многогранник M_2 , то $V(M_1) = V(M_2)$;

- $V(M_1 \cup M_2) = V(M_1) + V(M_2) - V(M_1 \cap M_2)$;
- объём любого подмножества $(n - 1)$ -мерной гиперплоскости равен нулю;
- объём куба с ребром a равен a^n .

Используя эти свойства и при необходимости верхние и нижние оценки, можно найти объём любого многогранника. Например, объём n -мерной пирамиды задаётся формулой $V = \frac{1}{n}Sh$, где S — $(n - 1)$ -мерный объём основания пирамиды, а h — её высота. Можно также находить объёмы некоторых n -мерных тел (т. е. ограниченных подмножеств n -мерного пространства), не являющихся многогранниками.

18.4.25. У 100-мерного арбуза (шара) радиус равен 1 метру, а толщина корки — 1 см. Какой процент его объёма занимает мякоть?

18.4.26. Докажите, что в единичный куб достаточно большой размерности можно поместить здание МГУ, т. е. существует трёхмерная плоскость, в пересечение которой с кубом можно поместить это здание.

18.4.27. Укажите какое-нибудь такое n , что в n -мерный единичный куб можно поместить круг радиуса R .

18.4.28. Укажите какое-нибудь такое n , что в n -мерный единичный куб можно поместить шар радиуса R .

18.4.29. Укажите какое-нибудь такое n , что в n -мерный единичный куб можно поместить n -мерный шар радиуса R .

18.4.30. К чему стремится объём n -мерного шара радиуса 2015 при $n \rightarrow \infty$?

Известно, что объём n -мерного шара радиуса R равен

$$B_n = \frac{\pi^{n/2}}{\Gamma(n/2 + 1)},$$

где $\Gamma(z) = \int_0^\infty y^z e^{-y} dy$, $z > 0$ — знаменитая *гамма-функция* Эйлера.

Она доопределяет факториал на комплексную плоскость: $\Gamma(k) =$

$(k+1)!$ при целом k и $\Gamma(z) = \Gamma(z-1)z$. Последнее равенство позволяет доопределить $\Gamma(z)$ также и при $\operatorname{Re}(z) < 0$. Известно, что $\Gamma(x)\Gamma(1-x) = \pi/\sin(\pi x)$, в частности $\Gamma(1/2) = \sqrt{\pi}/2$.

18.4.31. Найдите площадь поверхности n -мерного шара единичного объёма.

18.4.32. Найдите объём n -мерного симплекса с единичным ребром. Найдите ребро n -мерного симплекса с единичным объёмом. (Определения n -мерных симплекса и октаэдра приведены в п. 18.4.1 «Комбинаторная геометрия в многомерном пространстве».)

Диаметром ограниченного подмножества M n -мерного пространства называется $\sup\{|XY|, X, Y \in M\}$, где $\operatorname{dist}(X, Y)$ — расстояние между точками X и Y .

18.4.33. Найдите объём n -мерного октаэдра с единичным ребром. Найдите диаметр n -мерного симплекса с единичным объёмом.

18.4.3 Объёмы и сечения

$$\text{Обозначим } x_+ = \max(x, 0) = \begin{cases} x & \text{при } x \geq 0, \\ 0 & \text{при } x < 0. \end{cases}$$

Открытой полуплоскостью называется множество точек плоскости, лежащих строго по одну сторону от некоторой прямой. *Замкнутой полуплоскостью* называется объединение открытой полуплоскости и её граничной прямой. Прямая, заданная уравнением $ax + by + c = 0$, разбивает плоскость на две полуплоскости (замкнутую и открытую), координаты точек которых удовлетворяют неравенствам $ax + by + c \geq 0$ и $ax + by + c < 0$. Аналогично определяются открытое и замкнутое *полупространство* в n -мерном пространстве.

В задачах этого пункта слова «открытое» и «замкнутое» будут опускаться, поскольку несущественно, какое именно подпространство рассматривается.

18.4.34. Обозначим через $S(a, b, d)$ площадь пересечения единичного квадрата $K = \{(x, y) : 0 \leq x, y \leq 1\}$ с полуплоскостью $ax + by \leq d$,

Задачи на пространственное воображение

- [Ag] *Агаханов С.* Проекции фигур // Квантик. 2015. № 2. С. 11-13.
- [Dor] *Дориченко С.* Стереометрия для всех // Квантик. 2012. № 1. С. 28.
- [R] *В. Красноухов,* Недетские кубики-2, // Квантик. 2018. № 10. С. 15
- [ShEr] *Шарыгин И. Ф., Ерганжиева Л. Н.* Математика. Наглядная геометрия. (второе издание). М.: 2015. 192 с.
- [Nik] *Никитин Б. П.* Интеллектуальные игры. (шестое издание). Обнинск.: “Световид”. 2009. 216 с. <http://nikitiny.ru/Kirpichiki>

Рисование

- [BKK+] *И. Богданов, А. Каибханов, Ю. Кудряшов, А. Скопенков, А. Сосинский и Г. Челноков.* Новые способы плетения корзинок <http://www.turgor.ru/lktg/2004/lines.ru/index.htm>.
- [Fr] Дж. Франсис, Книжка с картинками по топологии (как рисовать математические картинки). Москва, Мир, 1991.
- [GSS+] *А. А. Гайфуллин, А. Б. Скопенков, М. Б. Скопенков и А. В. Шаповалов.* Проекция скрещивающихся прямых. <http://www.turgor.ru/lktg/2001/index.php>.
- [Ku] Курсы топологии в исполнении А.Б. Скопенкова, <http://www.mcsme.ru/circles/oim/home/combtop13.htm>
- [PS] В.В. Прасолов и И.Ф. Шарыгин. Задачи по стереометрии. Москва, Наука, 1989.
- [Sk] А.Б. Скопенков, Алгебраическая топология с геометрической точки зрения. Москва, МЦНМО, 2015. Часть книги: <http://www.mcsme.ru/circles/oim/home/combtop13.htm#photo>

Глава 2

Комбинаторика

20 Подсчеты в комбинаторике

Этот параграф посвящен в основном вопросу «Сколько существует объектов с данными свойствами?». В нем собраны материалы для самого первого знакомства с подсчетами в комбинаторике. Продолжить их изучение мы рекомендуем по главе 1 книги [GDI].

20.1 Подсчеты числа способов (1). *А. А. Гаврилюк, Д. А. Пермяков*

Этот пункт не требует никаких знаний и подходит для первого знакомства с комбинаторикой.

20.1.1. (а) Назовем натуральное число *симпатичным*, если в его записи встречаются только четные цифры. Выпишите все двузначные симпатичные числа и подсчитайте их количество.

(b) Сколько существует пятизначных симпатичных чисел?

(c) Сколько существует шестизначных чисел, в записи которых есть хотя бы одна четная цифра?

(d) Каких семизначных чисел больше: тех, в записи которых есть единица, или остальных?

20.1.2. Из двух математиков и десяти экономистов надо составить комиссию из восьми человек. Сколькими способами можно составить комиссию, если в нее должен входить хотя бы один математик?

20.1.3. (a) Найдите сумму всех семизначных чисел, которые можно получить всевозможными перестановками цифр $1, \dots, 7$.

(b) Из цифр $1, 2, 3, \dots, 9$ составлены все четырехзначные числа, не содержащие повторяющихся цифр. Найдите сумму этих чисел.

(c) Найдите сумму всех четырехзначных чисел, не содержащих повторяющихся цифр.

20.1.4. (a) На двух клетках шахматной доски стоят черный и белый короли. За один ход можно пойти любым королем (короли дружат, так что могут стоять в соседних клетках, но не в одной и той же). Могут ли в результате их передвижений встретиться все возможные варианты расположения этих королей, причем ровно по одному разу?

(b) Тот же вопрос, если короли разучились ходить по диагонали.

20.1.5. (a) Найдите сумму всех 6-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6$.

(b) Найдите сумму всех 10-значных чисел, получаемых при всех перестановках цифр $4, 5, 5, 6, 6, 6, 7, 7, 7, 7$.

20.1.6. (a) Тому Сойеру поручили покрасить забор из 8 досок в белый цвет. В силу своей лени он покрасит не более 3 досок. Сколько у него способов это сделать?

(b) А сколько способов покрасить не более 5 досок?

(c) А сколько способов покрасить любое количество досок?

Указания, ответы и решения

20.1.1. *Ответы:* (b) 2500; (c) 884 375; (d) в которых есть единица.

(b) *Решение* (написано А. Колоченковым). Первой цифрой симпатичного числа может быть 2, 4, 6, или 8 — всего 4 варианта. Для каждой цифры со второй по пятую есть 5 вариантов: 0, 2, 4, 6, 8. Значит, всего симпатичных чисел $4 \cdot 5 \cdot 5 \cdot 5 \cdot 5 = 2500$.

Это рассуждение в комбинаторике называется *правилом произведения* и подробно обсуждается в статье [Vi71].

(c) *Решение* (написано А. Колоченковым). Вычтем из общего количества шестизначных чисел количество шестизначных чисел,

нет). Если нет, то предположим, без ограничения общности, что $2007 \notin X_1$ и что $2, \dots, 52 \in X_1$. Тогда для всех $j = 2, \dots, 52$ пересечение $X_j \cap X_{2007}$ должно состоять ровно из одного элемента, причём разного для разных j (так как любые два множества по условию имеют ровно один общий элемент). Но это невозможно, поскольку X_{2007} состоит всего из 40 элементов, что меньше 51.

20.2.5. *Ответ:* да.

20.2.6. *Ответ:* да.

20.2.7. *Ответ:* $(N + 1)! - 1$.

20.3 Формула включений и исключений (2). Д. А. Пермяков

Этот пункт посвящен доказательству и использованию формулы включений и исключений. Она позволяет отвечать на вопрос «Сколько существует объектов с данными свойствами?» во многих непростых случаях. Потребуются базовые навыки решения задач по комбинаторике. В частности, нужно уметь приводить строгие доказательства с использованием взаимно однозначных соответствий, правил суммы и произведения. Например, полезно прорешать п. 20.1 «Подсчеты числа способов» или задачи из статьи [Vi71].

20.3.1. Сколькими способами можно переставить числа от 1 до n , чтобы

- (a) и 1, и 2 не оказались на своем месте;
- (b) ровно одно из чисел 1, 2 и 3 оказалось на своем месте;
- (c) каждое из чисел 1, 2 и 3 оказалось не на своем месте;
- (d) каждое из чисел 1, 2, 3 и 4 оказалось не на своем месте?

Обозначим через $\varphi(n)$ функцию Эйлера, т. е. количество чисел от 1 до n , взаимно простых с числом n .

20.3.2. (a) Найдите количество целых чисел от 1 до 1001, не делящихся ни на одно из чисел 7, 11, 13.

(b) Найдите $\varphi(1)$, $\varphi(p)$, $\varphi(p^2)$, $\varphi(p^\alpha)$, где p — простое число, $\alpha > 2$.

(c) Докажите, что $\varphi(n) = n \left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_s}\right)$, где $n = p_1^{\alpha_1} \cdot \dots \cdot p_s^{\alpha_s}$ — каноническое разложение числа n .

20.3.3. (a) На полу комнаты площадью 24 м^2 расположены три ковра (произвольной формы) площадью 12 м^2 каждый. Тогда площадь пересечения некоторых двух ковров не меньше 4 м^2 .

(b) На кафтане расположено пять заплат (произвольной формы). Площадь каждой из них больше трех пятых площади кафтана. Тогда площадь общей части некоторых двух заплат больше одной пятой площади кафтана.

(c)* То же, что в п. (b), если площадь каждой заплаты больше *половины* площади кафтана.

В этом пункте предлагаются задачи следующего типа: даны конечное множество U и набор свойств (подмножеств) $A_k \subset U$, $k = 1, \dots, n$. Требуется найти количество элементов, для которых выполнено хотя бы одно из свойств A_k (т. е. $|A_1 \cup \dots \cup A_n|$), либо количество элементов, для которых не выполнено ни одно из свойств A_k (т. е. $|U - (A_1 \cup \dots \cup A_n)|$). Для этого используются два варианта формулы включений и исключений (см. задачу 20.3.5 (b)). При этом если во всех пересечениях множеств набора число элементов зависит только от количества пересекаемых множеств, то формулу можно упростить (см. задачу 20.3.5 (a)).

20.3.4. Рассмотрим подмножества A_1, A_2, A_3, A_4 конечного множества U . Докажите равенства

$$(a) \quad A_1 \cup A_2 = (A_1 \setminus A_2) \sqcup (A_1 \cap A_2) \sqcup (A_2 \setminus A_1);$$

$$(b) \quad |A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|;$$

$$(c) \quad |A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3| - |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|.$$

(d) Количество элементов в U , не принадлежащих ни одному из подмножеств A_1, A_2, A_3 , равно

$$|U| - |A_1| - |A_2| - |A_3| + |A_1 \cap A_2| + |A_2 \cap A_3| + |A_1 \cap A_3| - |A_1 \cap A_2 \cap A_3|.$$

(е) Для $k = 1, 2, 3, 4$ обозначим

$$M_k := \sum_{1 \leq i_1 < \dots < i_k \leq 4} |A_{i_1} \cap A_{i_2} \cap \dots \cap A_{i_k}|.$$

Докажите, что количество элементов в A , не принадлежащих ни одному из A_i , равно $|U| - M_1 + M_2 - M_3 + M_4$.

(f) В условиях п. (е) количество элементов, принадлежащих ровно одному из множеств A_i , равно $M_1 - 2M_2 + 3M_3 - 4M_4$.

20.3.5. Формула включений и исключений. Рассмотрим подмножества $A_1, \dots, A_n$ конечного множества U . Положим по определению $\left| \bigcap_{j \in \emptyset} A_j \right| := U$.

(а) Пусть число $\alpha_{|S|} := \left| \bigcap_{j \in S} A_j \right|$ зависит только от размера $|S|$ набора $S \subset \{1, \dots, n\}$ индексов, а не от самого набора. Тогда

$$\begin{aligned} |A_1 \cup \dots \cup A_n| &= \sum_{k=1}^n (-1)^{k+1} \binom{n}{k} \alpha_k, \\ |U - (A_1 \cup \dots \cup A_n)| &= \sum_{k=0}^n (-1)^k \binom{n}{k} \alpha_k. \end{aligned}$$

(b) Обозначим $M_k := \sum_{S \in \binom{n}{k}} \left| \bigcap_{j \in S} A_j \right|$, где суммирование производится по всем k -элементным подмножествам множества $\{1, \dots, n\}$. В частности, $M_0 := |U|$. Тогда

$$\begin{aligned} |A_1 \cup \dots \cup A_n| &= M_1 - M_2 + M_3 - \dots + (-1)^{n+1} M_n, \\ |U - (A_1 \cup \dots \cup A_n)| &= M_0 - M_1 + M_2 - \dots + (-1)^n M_n. \end{aligned}$$

(с) **Неравенства Бонферрони.** Для любого $0 \leq s < n/2$ справедливы неравенства

$$\begin{aligned} M_1 - M_2 + M_3 - \dots - M_{2s} &\leq |A_1 \cup \dots \cup A_n| \leq M_1 - M_2 + M_3 - \dots + M_{2s+1}, \\ M_0 - M_1 + M_2 - \dots + M_{2s} &\geq |U - (A_1 \cup \dots \cup A_n)| \geq \\ &\geq M_0 - M_1 + M_2 - \dots - M_{2s+1}. \end{aligned}$$

(d) Число элементов, принадлежащих ровно r из подмножеств $A_1, \dots, A_n$, равно $\sum_{k=r}^n (-1)^{k-r} \binom{k}{r} M_k$.

20.3.6. На полке стоят 10 различных книг.

(a) Сколькими способами их можно переставить так, чтобы ни одна книга не осталась на своем месте?

(b) Количество таких перестановок книг, при которых на месте остаётся ровно 4 книги, больше 50 000.

В следующей задаче в ответе можно использовать суммы (аналогично формуле включений и исключений).

20.3.7. (a) Сколькими способами можно расселить 20 туристов по 5 различным домикам, чтобы ни один домик не оказался пустым?

(b) Сколько существует различных сюръекций $f: \mathbb{Z}_k \rightarrow \mathbb{Z}_n$?

20.3.8. По кругу стоят числа $1, 2, \dots, n$. Найдите число способов выбрать k из них, чтобы никакие два выбранных числа не стояли рядом.

(b) Найдите число способов рассадить n пар враждующих рыцарей за круглый стол с нумерованными местами, чтобы никакие два враждующих рыцаря не сидели рядом.

20.3.9. Куб с ребром длины 20 разбит на 8000 единичных кубиков, и в каждом кубике записано число. Известно, что в каждом столбике из 20 кубиков, параллельном ребру куба, сумма чисел равна 1 (рассматриваются столбики всех трех направлений). В некотором кубике записано число 10. Через этот кубик проходят три слоя $1 \times 20 \times 20$, параллельные граням куба. Найдите сумму всех чисел вне этих слоев.

20.3.10.* Сколько существует шестизначных трамвайных билетов, в которых нет двух семерок рядом и всего

(a) не более трех семерок;

(b) не более четырех семерок;

(c) сколько угодно семерок?

20.3.11.* Докажите следующую формулу:

$$\begin{aligned}
 n! \cdot x_1 x_2 \dots x_n &= (x_1 + x_2 + \dots + x_n)^n - \\
 &\quad - \sum_{1 \leq i_1 < i_2 < \dots < i_{n-1} \leq n} (x_{i_1} + x_{i_2} + \dots + x_{i_{n-1}})^n + \\
 &\quad + \sum_{1 \leq i_1 < i_2 < \dots < i_{n-2} \leq n} (x_{i_1} + x_{i_2} + \dots + x_{i_{n-2}})^n - \dots + (-1)^{n-1} \sum_{i=1}^n x_i^n.
 \end{aligned}$$

Указания, ответы и решения

20.3.1. (а) *Ответ:* $n! - 2(n-1)! + (n-2)!$.

Указание. Всего имеется $n!$ способов переставить наши числа. Вычтем из них $(n-1)!$ способов перестановки, при которых число 1 остается на месте. Вычтем также $(n-1)!$ способов перестановки, при которых число 2 остается на месте. При этом $(n-2)!$ способов перестановки, при которых оба числа 1 и 2 остаются на месте, мы «вычли дважды». Значит, число $(n-2)!$ нужно добавить, чтобы в итоге мы эти способы «посчитали один раз». Получаем ответ: $n! - 2(n-1)! + (n-2)!$.

Комментарий. Это решение формализуется формулой включения и исключений 20.3.5, которую предлагается доказать и использовать в последующих задачах.

20.3.2. (а) *Ответ:* 720.

Первое указание. Для каждого j , делящего 1001, обозначим через A_j множество чисел от 1 до 1001, делящихся на j . Тогда

$$|A_j| = \frac{1001}{j} \quad \text{и} \quad A_{p_1} \cap \dots \cap A_{p_k} = A_{p_1 \dots p_k}$$

для различных простых чисел $p_1, \dots, p_k$. Следовательно, искомое

23.1 Конструкции³ (1). А. В. Шаповалов

Если на вопрос «Может ли?» вы подозреваете ответ «Может», то стоит спросить себя: «Как такое может быть?». Уточните вопрос: «Какими свойствами эта конструкция должна обладать?». Дополнительное знание поможет сильно сузить круг поисков. Задавайте себе вопросы на протяжении всего построения. Вы с удивлением увидите, как много конструкций окажутся логичными и единственно возможными.

Часто примеров много, а нужен только один. Избыток свободы может сбивать с толку: неясно, с чего начинать. Примените *здравый смысл, естественные соображения*. Они ограничивают поле для поиска примера, но зато поиск убыстряется и облегчается. Вообще, ваш опыт гораздо больше, чем вы думаете. Ответом может оказаться *хорошо знакомый объект*, просто надо посмотреть на него под нужным углом.

23.1.1. У двух треугольников равны по две стороны, а также равны высоты, проведённые к третьей стороне. Обязательно ли эти треугольники равны?

23.1.2. Верно ли, что в вершинах любого треугольника можно поставить по положительному числу так, чтобы длина каждой стороны была равна сумме чисел в её концах?

23.1.3. В кружке у каждого участника ровно по 6 друзей. Может ли у каждой пары участников быть ровно по два общих друга?

Конструкцию с большим числом деталей проще строить из одинаковых «кирпичей». Даже если все они одинаковыми быть не могут, попробуйте взять одинаковых побольше. Можно ещё выбрать два вида деталей и посчитать, сколько нужно тех и других.

Ну, а если детали «для сборки» заданы и они разные? Тогда стоит попытаться объединить эти части в *одинаковые блоки*, и строить из блоков.

23.1.4. Назовём неотрицательное целое число *зеброй*, если в его записи строго чередуются чётные и нечётные цифры и среди цифр

³Эта подборка задач составлена по книгам [Shap14] и [Shap15].

есть не менее трёх различных. Может ли разность двух 100-значных зебр быть 100-значной зеброй?

23.1.5. Грани параллелепипеда со сторонами 3, 4 и 5 разбиты на единичные клетки. В каждую клетку вписали по натуральному числу. Рассмотрим всевозможные кольца шириной в одну клетку, параллельные какой-нибудь грани. Может ли сумма чисел в каждом таком кольце быть одной и той же?

В задачах, где требуются равные части, приходится выбирать форму частей. Тут может помочь такое соображение: части заведомо равны, если они получаются друг из друга симметрией, сдвигом или поворотами. Так, для квадрата популярны разрезания, переходящие в себя при повороте на 90° , а для правильного треугольника — при повороте на 120° . Для симметричных объектов поиск примера начинают с симметричных или «почти симметричных» конструкций. Симметрия и идея «расположить объекты по кругу» применима и в негеометрических задачах.

23.1.6. Можно ли рёбра куба занумеровать числами $-6, -5, -4, -3, -2, -1, 1, 2, 3, 4, 5, 6$ так, чтобы для каждой тройки рёбер, выходящих из одной вершины, сумма была одинакова?

23.1.7. Круг разрезали на несколько равных частей. Обязательно ли граница каждой части проходит через центр круга?

Если к конструкции предъявляются противоречивые требования, присмотритесь внимательнее. Часто эти противоречия мнимые. Так, *большой* периметр не противоречит *малой* площади. Вообще, словам «много», «мало», «сильно» нужно уметь придать в решении точный математический смысл с помощью уравнений и неравенств.

23.1.8.* В море плавает айсберг в форме выпуклого многогранника. Может ли случиться, что 90 % его объёма находится ниже уровня воды и при этом больше половины его поверхности находится выше уровня воды?

23.1.9. Есть три игральные кубика с нестандартными наборами чисел на гранях. Скажем, что кубик А *выигрывает* у кубика В, если

при их одновременном бросании число на А будет больше числа на В с вероятностью *больше* 0,5. Может ли первый кубик выигрывать у второго, второй — у третьего, а третий — у первого?

(Приведём равносильную формулировку этой же задачи, не использующую понятие вероятности: для пары кубиков А и В составим 36 упорядоченных пар вида (грань А, грань В). Заменим в каждой паре грань на число, стоящее на грани. Кубик А *выигрывает* у В, если более чем в половине пар первое число больше второго.)

Помешать решить задачу могут невидимые барьеры в голове решателя. Если очевидного решения не видно, надо расширять список вариантов, по возможности до полного. *Инерция мышления* проявляется в том, что ключевой вариант пропускают либо не подозревают, что вариантов более одного. Примените «метод Шерлока Холмса»: отбросьте все невозможные случаи, тогда *последний вариант* окажется возможным, каким бы невероятным он ни казался.

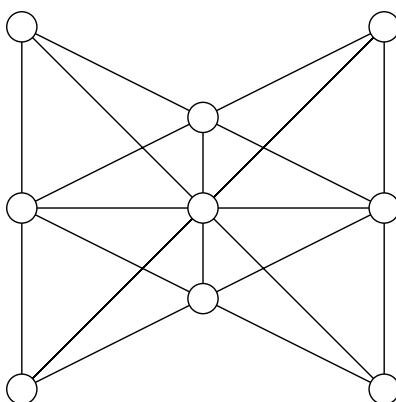


Рис. 2.3:

23.1.10. На столе лежат 9 яблок, образуя 10 рядов по 3 яблока в каждом (см. рис. 2.3). Известно, что у девяти рядов веса одинаковы, а вес десятого ряда отличается. Есть электронные весы, на которых за рубль можно узнать вес любой группы яблок. Какое наименьшее число рублей надо заплатить, чтобы узнать, вес какого именно ряда отличается?

23.1.11. Может ли прямая разбить какой-нибудь шестиугольник на 4 равных треугольника?

Редукция — это сведение сложной задачи к более простой. Так, если сложную конструкцию не удаётся сразу построить целиком, постройте её *необходимую часть*. Даже если эту часть не удастся потом достроить до целого, решение упрощённой задачи может послужить разминкой, после чего вы вернётесь к сложной задаче уже с накопленным опытом.

23.1.12. Барон Мюнхгаузен говорит, что у него есть многозначное число-*палиндром* (т. е. оно читается одинаково слева направо и справа налево). Написав его на бумажной ленте, барон сделал несколько разрезов между цифрами. Лента распалась на N кусков. Переложив куски в другом порядке, барон увидел, что на кусках по разу записаны числа $1, 2, \dots, N$. Могут ли слова барона быть правдой?

При построении конструкции может мешать неоднозначность выбора. В *узком месте* всё однозначно или неопределённость минимальна, что сокращает перебор. Начав с узкого места, мы либо быстро придём к противоречию, либо построим большой кусок конструкции. Как искать узкие места? Присмотритесь: они служат препятствиями к построению конструкции или кажутся таковыми.

23.1.13. Записав числа $1, \frac{1}{2}, \frac{1}{3}, \dots, \frac{1}{10}$ в некотором порядке, соедините их знаками четырёх арифметических действий так, чтобы полученное выражение равнялось 0. (Скобки использовать нельзя.)

23.1.14. Существуют ли три равных семиугольника, все вершины которых совпадают, но никакие стороны не совпадают?

23.1.15. Можно ли разрезать какой-нибудь треугольник на четыре выпуклые фигуры: треугольник, четырёхугольник, пятиугольник и шестиугольник?

При *постепенном конструировании* к примеру идут через цепочку вспомогательных конструкций-*заготовок*. На каждом шаге очередная конструкция *улучшается* до следующей. В заготовке требования к окончательной конструкции выполнены лишь частично. Оставляем *принципиальные условия*, временно забываем или ослабляем *технические*.

23.1.16. Могут ли в остроугольном треугольнике все стороны и высоты измеряться целым числом сантиметров?

23.1.17. Докажите, что существует палиндром, делящийся на 6^{100} . (Напомним, что *палиндром* — это число, которое не меняется при записи его цифр в обратном порядке.)

Наконец, при *конструкции по индукции* результат получается постепенно, но уже за бесконечное число шагов. Таким конструкциям посвящён п. 21.5 «Конечное и счётное».

Продолжить знакомство с конструкциями можно по статье [GK] и книгам [Shap14, Shap15, Shap08].

Указания, ответы и решения

Решения задач и *пути к решению* тщательно разделены. Решение — это то, что решающий задачу в идеале должен написать. Путь к решению должен остаться в голове, здесь он поясняет, как это решение можно было придумать. В задачах на конструкцию решение и путь к решению обычно имеют мало общего.

Решение в задаче на конструкцию состоит из двух частей: *примера*, то есть описания конструкции, и *доказательства* того, что она удовлетворяет условию задачи. Для наших задач вторая часть не представляет труда и обычно опускается. Но иногда из многих возможных примеров нужно ещё выбрать тот, для которого доказательство проще.

23.1.1. *Ответ:* не обязательно.

Решение. Рассмотрим равнобедренный треугольник ACD и точку B на продолжении основания DC . У треугольников ABC и ABD сторона AB и высота $АН$ общие, стороны AC и AD равны. Однако эти треугольники не равны: один — часть другого.

Путь к решению. Попробуем *построить* треугольник по двум сторонам b, c и высоте h , проведённой к третьей стороне. Для этого проведём прямую l (на ней будет лежать третья сторона) и построим вершину A на расстоянии h от l . Две другие вершины треугольника должны лежать на этой прямой на расстояниях b и c от точки A . Проведя окружности указанных радиусов с центром

23.4.12. Какое наименьшее число уголков из трёх клеток нужно разместить в квадрате 8×8 клеток, чтобы в него нельзя было поместить без наложения ни одной такой фигуры?

23.4.13. В квадрате 7×7 клеток нужно отметить центры n клеток так, чтобы никакие 4 отмеченные точки не являлись вершинами прямоугольника со сторонами, параллельными сторонам квадрата. При каком наибольшем n это возможно?

Указания, ответы и решения

23.4.1. Каждая фигура «домино» содержит одну белую и одну чёрную клетку. Но в нашей фигуре 32 чёрных и 30 белых клеток (или наоборот). Подробный разбор см. в статье [Soi].

23.5 Полуинварианты⁷(1). А. В. Шаповалов

Если слово «инвариант» означает «неизменный», то «полуинвариант» — неизменный наполовину.

Бывает так, что мы меняем конструкцию, а какая-то связанная с этой конструкцией величина может меняться только в одну сторону, то есть либо только увеличиваться, либо только уменьшаться. Ещё возможно, что мы делаем ходы и в одну сторону меняется величина, связанная с позицией. Например, при игре в крестики-нолики число заполненных клеток с каждым ходом увеличивается. На ограниченной доске из этого следует, что рано или поздно игра закончится. При игре на бесконечной доске игра может не закончиться никогда, но зато мы можем гарантировать, что позиция не повторится, — ведь число заполненных клеток каждый раз новое!

Чуть более формально: пусть мы меняем конструкции (или позиции) с помощью *разрешённых операций* (или *ходов*) и нам удалось связать с каждой конструкцией/позицией *величину*, значение которой при любом разрешённом преобразовании либо не меняется, либо меняется всегда в одну и ту же сторону. Тогда эта величина

⁷Идейными предшественниками подборок «Инварианты» и «Полуинварианты» были, среди прочего, соответствующие параграфы книги [KK08].

называется *полуинвариантом*⁸. Если полуинвариант меняется при каждой операции/ходе, он называется *строгим*, иначе — *нестрогим*.

В типовых задачах «на полуинвариант» доказывают невозможность а) повторения позиций; б) бесконечного числа ходов; в) построения конструкций. Для последнего находят полуинвариант и проверяют, что для получения искомой конструкции из исходной полуинвариант должен был бы *меняться не в ту сторону*.

Но как найти полуинвариант? Начните с проверки типовых величин: сумм, произведений, площадей, периметров и их комбинаций. Если конструкция зависит от целых чисел, то полуинвариантом может быть НОД или НОК.

В следующих двух задачах важно, что полуинвариант целочисленный и не может быть больше определённого числа.

23.5.1. На шахматной доске 100×100 королю разрешено ходить вправо, вверх или вправо-вверх по диагонали. Какое наибольшее число ходов он может сделать?

23.5.2. В клетках таблицы 99×99 расставлены целые числа. Если в каком-то ряду (строке или столбце) сумма отрицательна, разрешается в этом ряду поменять знаки всех чисел на противоположные. Докажите, что в итоге можно сделать лишь конечное число таких операций.

Если полуинвариант не целочисленный, то его ограниченность ещё не гарантирует окончания процесса (например, убывающий положительный полуинвариант мог бы бесконечно долго принимать значения $1, 1/2, 1/3, 1/4, \dots, 1/n, \dots$). В этих случаях прекращение ходов гарантируется конечным числом позиций.

23.5.3. Дано 10 чисел. За одну операцию можно два неравных числа заменить на два равных с той же суммой. Может ли этот процесс для какого-то исходного набора чисел

- (а) продолжаться бесконечно долго;
- (б) заикнуться (то есть может ли один и тот же набор чисел возникнуть дважды)?

⁸Эта фраза не является формальным определением полуинварианта. Но для решения задач формальное определение этого понятия не нужно.

23.5.4. По кругу выписано несколько чисел. Если для некоторых четырёх идущих подряд чисел a, b, c, d оказывается, что $(a - d)(b - c) < 0$, то числа b и c можно поменять местами. Докажите, что такую операцию можно проделать лишь конечное число раз.

Очень часто положение, в котором нет разрешённых операций, и является искомым.

23.5.5. В клетки прямоугольной таблицы вписаны числа. Разрешается одновременно менять знак у всех чисел некоторого столбца или некоторой строки. Докажите, что многократным повторением этой операции можно превратить данную таблицу в такую, у которой суммы чисел в любой строке или любом столбце неотрицательны.

В комбинаторных задачах полуинвариантом часто служит число комбинаций, например пар, троек, подмножеств или перестановок какого-то вида.

23.5.6. В тридевятом царстве все города подняли над ратушами флаги — голубые либо оранжевые. Каждый день жители узнают цвета флагов у соседей в радиусе 100 км. Один из городов, где у большинства соседей флаги другого цвета, меняет свой флаг на этот другой цвет. Докажите, что со временем смены цвета флагов прекратятся.

Некоторые конструкции создаются «методом последовательного улучшения». Мы берём несовершенную конструкцию и начинаем её преобразовывать. Полуинвариант гарантирует завершение процесса и достижение нужного эффекта в конце.

23.5.7. В парламенте каждый депутат имеет не более трёх врагов. Докажите, что парламент можно так разбить на две палаты, что у каждого депутата в его палате будет не более одного врага.

23.5.8. На плоскости дано 100 красных и 100 синих точек, никакие три из которых не лежат на одной прямой. Докажите, что можно провести 100 непересекающихся отрезков с концами разных цветов.

Полуинвариант может быть и *нестрогим*, т. е. не меняться при некоторых ходах. Тогда полезно найти ещё один полуинвариант, который строго меняется как раз тогда, когда первый остаётся неизменным.

23.5.9. На шахматной доске 100×100 королю разрешено ходить вправо, вверх, вправо-вверх или вправо-вниз по диагонали. Докажите, что он может сделать лишь конечное число ходов.

Если и второй полуинвариант оказывается нестрогим, то приходится рассматривать и третий, и четвёртый и т. д. В этом случае естественно рассматривать наборы значений полуинвариантов как строки, упорядоченные *лексикографически* (как слова в словаре: сравниваются первые элементы, при равенстве — вторые и т. д. и так до первого несовпадения).

23.5.10. В колоде часть карт лежит рубашкой вниз. Время от времени Петя вынимает из колоды пачку из нескольких подряд идущих карт, в которой верхняя и нижняя карты лежат рубашкой вниз (в частности, может вынуть просто одну карту рубашкой вниз), переворачивает эту пачку как одно целое и вставляет в то же место колоды. Докажите, что независимо от того, как Петя выбирает пачки, в конце концов все карты лягут рубашкой вверх.

В заключение — ещё несколько задач на полуинварианты и их комбинации.

23.5.11. В строке записано несколько чисел. Каждую секунду робот выбирает какую-либо пару рядом стоящих чисел, в которой левое число больше правого, меняет их местами и при этом умножает оба числа на 2. Докажите, что через некоторое время сделать очередную такую операцию будет невозможно.

23.5.12. У Карлсона есть 1000 банок с вареньем. Банки не обязательно одинаковые, но в каждой — не больше чем сотая часть всего варенья. На завтрак Карлсон может съесть поровну варенья из любых 100 банок. Докажите, что Карлсон может действовать так, чтобы за некоторое количество завтраков съесть всё варенье.

23.5.13. На окружности расставлено несколько положительных чисел, каждое из которых не больше 1. Докажите, что можно разделить окружность на три дуги так, что суммы чисел на соседних дугах будут отличаться не больше чем на 1. (Если на дуге нет чисел, то сумма на ней считается равной нулю.)

24 Алгоритмы

24.1 Игры (1)⁹. Д. А. Пермяков, М. Б. Скопенков, А. В. Шаповалов

На конкретных примерах мы познакомимся с некоторыми красивыми идеями теории игр. Общие методические указания по теме «Игры» можно найти в соответствующем разделе книги [GIF].

Симметричная стратегия

Самая распространённая стратегия в играх — *симметричная* (а также её обобщение — *дополняющая*). Для решения последующих задач полезно знакомство с п. 23.2 «Инварианты I», поскольку многие стратегии в играх основаны на инвариантах (пример инварианта — симметричность позиции).

24.1.1. (a) Двое по очереди выкладывают доминошки на шахматную доску. Каждая доминошка покрывает ровно две клетки доски, каждая клетка может быть покрыта не более чем одной доминошкой. Проигрывает тот игрок, который не может положить очередную доминошку. Кто выигрывает при правильной игре? Как он должен для этого играть?

(b) То же для доски 8×9 .

Вот что означают вопросы этой задачи. В ответе на первый вопрос нужно назвать игрока, который выигрывает при *любой* игре своего противника. В ответе на второй вопрос нужно привести *алгоритм* действий этого игрока, который гарантирует выигрыш (*выигрышную стратегию*). Важно чётко отделять *сам* алгоритм от *доказательства* того, что алгоритм приводит к желаемому результату.

Второй пункт этой задачи показывает, что не всегда симметричность позиции гарантирует, что симметричная стратегия работает.

⁹Подпункты «Симметричная стратегия», «Выращивание дерева позиций», «Передача хода» написаны Д. А. Пермяковым и М. Б. Скопенковым, «Игры-шутки», «Игра на опережение», «Накопление преимущества» — А. В. Шаповаловым, «Смесь» — всеми тремя авторами.

24.1.2.° (Загадка.) К какому результату приведёт попытка чёрных зеркально-симметрично копировать ходы противника в обычных шахматах при правильной игре белых? Выберите верный вариант ответа:

- 1) к ничьей; 2) к выигрышу белых; 3) к выигрышу чёрных.

Ключевой идеей является не столько симметрия, сколько разбиение всех возможных позиций на пары. *Дополняющая стратегия* состоит в том, чтобы на ход противника отвечать ходом во вторую позицию соответствующей пары.

24.1.3. На шахматной доске стоит король. Двое по очереди ходят им. Проигрывает игрок, после хода которого король оказывается в клетке, в которой побывал ранее. Кто выигрывает при правильной игре и как он должен для этого играть?

Игра на опережение

Игра на опережение — распространённый приём в нематематических играх. Но и в математических играх бывает, что выигрыш достаётся тому, кто первый сумеет занять ключевое положение. После этого, как правило, работает дополняющая стратегия.

24.1.4. Есть 9 запечатанных прозрачных коробок соответственно с 1, 2, 3, ..., 9 фишками. Двое играющих по очереди берут по одной фишке из любой коробки, распечатывая, если необходимо, коробку. Проигрывает тот, кто последним распечатает коробку. Кто из них может всегда выиграть независимо от игры противника?

24.1.5. В одном из углов шахматной доски лежит плоский картонный квадрат 2×2 , а в противоположном — квадрат 1×1 . Двое играющих по очереди перекатывают каждый свой квадрат через сторону: Боря — большой квадрат, а Миша — маленький. Боря выигрывает, если не позднее 100-го хода Мишин квадрат окажется на клетке, накрытой Бориным квадратом. Может ли Боря выиграть независимо от игры Миши, если

- (а) первым ходит Боря;
(б) первым ходит Миша?

Накопление преимущества

Накопление преимущества — тоже весьма распространённый приём в нематематических играх. В математических играх накопление обычно связано с каким-нибудь полуинвариантом. Поэтому для изучения таких игр полезно знакомство с п. 23.5 «Полуинварианты». При этом надо придумать алгоритм, ведущий к накоплению независимо от сопротивления соперника.

24.1.6. Миша стоит в центре круглой лужайки радиуса 100 метров. Каждую минуту он делает шаг длиной 1 метр. Перед каждым шагом он объявляет направление, в котором хочет шагнуть. Катя имеет право заставить его сменить направление на противоположное. Может ли Миша действовать так, чтобы в какой-то момент обязательно выйти с лужайки, или Катя всегда сможет ему помешать?

24.1.7. На клетчатой доске $1 \times 100\,000$ (вначале пустой) двое ходят по очереди. Первый может за ход выставить два крестика в любые два свободных поля доски. Второй может стереть любое количество крестиков, идущих подряд — без пустых клеток между ними. Если после хода первого образуется 13 или более крестиков подряд, он выиграл. Может ли первый игрок выиграть при правильной игре обеих сторон?

24.1.8. Двое играющих по очереди ломают палку: первый на две части, затем второй ломает любой из кусков на две части, затем первый — любой из кусков на две части и т. д. Один из игроков выигрывает, если сможет после какого-то из своих ходов сложить из 6 кусков два равных треугольника. Может ли другой ему помешать?

Игры-шутки

В *играх-шутках* побеждает всегда одна из сторон независимо от её желания.

24.1.9. (а) На столе лежат 2015 кучек по одному ореху. За один ход разрешается объединить две кучки в одну. Двое играющих делают

ходы по очереди, кто не сможет сделать ход, тот проигрывает. Кто выиграет?

(b) То же, но разрешается объединять кучки только с одинаковым числом орехов.

24.1.10. Дана клетчатая полоса $1 \times N$. Двое играют в следующую игру. На очередном ходу первый игрок ставит в одну из свободных клеток крестик, а второй — нолик. Не разрешается ставить в соседние клетки два крестика или два нолика. Проигрывает тот, кто не может сделать ход. Кто из игроков выигрывает при правильной игре? Как он должен для этого играть?

Кроме игр-шуток бывают и *почти шутки*, где выигрышная стратегия такова: если есть выигрыш в один ход, его надо сделать, иначе можно делать любой ход. Или, наоборот: делать любой ход, кроме тех, которые проигрывают в один ход. В таких играх важно догадаться, кому обязательно представится возможность сделать выигрышный ход или кто будет вынужден сделать проигрывающий ход, — и доказать это. Кроме того, выигрышная стратегия может состоять в достижении позиции, после которой игра превращается в игру-шутку с нужным исходом.

24.1.11. В десяти корзинах лежат яблоки: 1, 3, 5, ..., 19 яблок. Сначала берёт одно яблоко из любой корзины Вася, потом — Гена, потом Лёва, потом опять Вася и т. д. по кругу. Проигрывает тот, после чьего хода в каких-то корзинах станет яблок поровну. Кто из них не может избежать проигрыша?

24.1.12. Из спичек сложен клетчатый квадрат 9×9 , сторона каждой клетки — одна спичка. Петя и Вася по очереди убирают по спичке, начинает Петя. Выиграет тот, после чьего хода не останется целых квадратиков 1×1 . Кто может действовать так, чтобы обеспечить себе победу, как бы ни играл его соперник?

Выращивание дерева позиций

Один из универсальных способов анализа игры — *выращивание дерева позиций*.

24.1.13. *Ферзя — в угол, или «цзяньшицзы».* Ферзь стоит на d1. Двое по очереди ходят им по направлению вверх, вправо или вправо-вверх. Выигрывает тот, кто поставит его на h8. Кто выигрывает при правильной игре и как он должен для этого играть?

Если не получается, подумайте сначала над следующим вопросом.

24.1.14.° Кто выигрывает в игре из предыдущей задачи, если в начальный момент ферзь стоит на клетке f4? Выберите верный вариант ответа:

- 1) первый игрок; 2) второй игрок.

Выращивание дерева позиций означает полный анализ игры. Перейдём теперь к более сложной идее *передачи хода*, которая помогает даже тогда, когда для полного анализа нет никакой возможности.

Передача хода

24.1.15. В *двухходовых* шахматах фигуры ходят по обычным правилам, только за каждый ход разрешается сделать ровно два хода одной фигурой. Цель игры — съесть короля соперника. Правила троекратного повторения позиции и 50 ходов не действуют¹⁰. Докажите, что белые в двухходовых шахматах могут играть так, что заведомо не проиграют (т. е. либо выиграют, либо сыграют вничью).

24.1.16.° Правила *шахмат без цугцванга*¹¹ отличаются от правил обычных шахмат только добавлением возможности пропустить свой ход для каждого из игроков. Могут ли чёрные выиграть при правильной игре белых? Выберите верный вариант ответа:

- 1) могут; 2) не могут.

¹⁰Если не знаете, что это за правила, игнорируйте это предложение.

¹¹*Цугцвангом* в шахматах называется такая позиция для игрока, в которой любой его ход эту позицию ухудшает.

Данный параграф посвящён простейшим понятиям и применениям теории вероятности. Для его изучения необходимо знакомство с основами комбинаторики, например с п. 20.1 «Подсчёт числа способов» и 20.3 «Формула включений и исключений» данной книги. Кроме того, знакомство с теорией вероятностей полезно начинать на «физическом» уровне строгости, как в книге [Shen],[Kolm]. Здесь же мы сразу даём «математические» определения. Однако мы приводим многие задачи на «практическом» языке и показываем на примерах, как их формализовать. Формализацию остальных задач оставляем читателю. Такая формализация является первым шагом решения, от которого может зависеть ответ. См., например, задачи 25.2.7 (c),(d), 25.4.14, 25.3.5, [GDI, задачи 6.3.1.b и 6.3.3.c].

25.1 Классическое определение вероятности (1). А. А. Заславский, А. Б. Скопенков

Рассмотрим эксперимент, имеющий m равновозможных исходов, например бросание игральной кости, вытаскивание карты из колоды и т. д. Если интересующее нас событие (например, выпадение шестёрки, вытаскивание туза и т. д.) происходит в a из этих исходов, то *вероятность* события считают равной $p = a/m$.

Это пояснение полезно для начинающего, но не является математическим определением. Вот математическое определение.

Вероятностью подмножества A конечного множества M называется число

$$P(A) = P_M(A) := |A|/|M|.$$

Далее, если не оговорено противное, множество M фиксировано и пропускается из обозначений. Тогда вероятность определена для всех его подмножеств. Их часто называют *событиями*.

25.1.1. Из колоды в 52 карты вытаскивается одна карта. Найдите вероятность того, что она окажется

- (a) чёрной масти; (b) тузом; (c) картинкой;
- (d) дамой пик; (e) королём или бубной.

Например, в задаче 25.1.1 (c) множество M («всех возможных исходов») совпадает с множеством карт в колоде, а множество A

(«исходов, в которых происходит рассматриваемое событие») — с множеством картинок. Так эта и многие другие вероятностные задачи могут быть строго сформулированы на комбинаторном языке.

25.1.2. Монета бросается 3 раза. Найдите вероятность выпадения
(а) трёх орлов; (б) двух орлов и решки.

25.1.3. Пассажиру купейного вагона удобно, если все его попутчики одного с ним пола. Какая часть пассажиров испытывает удобства?

25.1.4. Найдите вероятность того, что при бросании двух игральных костей

- (а) на первой выпадет больше очков, чем на второй;
- (б) сумма выпавших очков составит $2, 3, \dots, 12$.

25.1.5. Найдите вероятность того, что случайное целое число от 1 до 105

- (а) делится на 5; (б) делится на 7; (с) делится на 35.
- (а', б', с') То же для случайного целого числа от 1 до 100.

Для решения некоторых из вышеприведённых задач полезны следующие.

25.1.6. (а) Правило сложения. Пусть $A \cap B = \emptyset$. Выразите $P(A \cup B)$ через $P(A)$ и $P(B)$.

(б) Выразите вероятность $P(A \cup B)$ через $P(A)$, $P(B)$ и $P(A \cap B)$.

(с) **Правило умножения.** Выразите вероятность $P_{M \times N}(A \times B)$ через $P_M(A)$ и $P_N(B)$.

Комментарий: $P_M(A) = P_{M \times N}(A \times N)$ и $P_N(B) = P_{M \times N}(M \times B)$.

Следующее определение обобщает ситуацию правила умножения 25.1.6 (с). Подмножества (т. е. события) A и $B \neq \emptyset$ конечного множества M *независимы*, если доля (т. е. вероятность) множества $A \cap B$ в B равна доле (т. е. вероятности) множества A в M . Приведём симметричную переформулировку, которая работает и для $B = \emptyset$. Подмножества A и B конечного множества M называются *независимыми*, если

$$|A \cap B| \cdot |M| = |A| \cdot |B|.$$

Основной пример независимых подмножеств — в множестве всех клеток шахматной доски подмножество клеток в первых трёх её строках и подмножество клеток в последних четырёх её столбцах, или, более строго, $A \times N$ и $M \times B$ в $M \times N$.

25.1.7. Зависимы ли следующие подмножества? (Мы называем *зависимыми* подмножества, не являющиеся независимыми.)

- (а) Подмножества $\{1, 2\} \subset \{1, 2, 3, 4\}$ и $\{1, 3\} \subset \{1, 2, 3, 4\}$.
- (б) Подмножества $\{1, 2\} \subset \{1, 2, 3, 4, 5, 6\}$ и $\{1, 3\} \subset \{1, 2, 3, 4, 5, 6\}$.

25.1.8. Зависимы ли следующие подмножества множества целых чисел от 1 до 105?

- (а) Подмножество чисел, делящихся на 5, и подмножество чисел, делящихся на 7.
- (б) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 21.
- (с) Подмножество чисел, делящихся на 15, и подмножество чисел, делящихся на 5.
- (д) Подмножество чисел, делящихся на 10, и подмножество чисел, делящихся на 7.

См. комбинаторные применения, например, в [GDI, п. 6.2].

Указания, ответы и решения

25.1.3. Ответ: $1/8$.

25.1.5. Ответы: (а) 0,2; (б) $\frac{1}{7}$; (с) $\frac{1}{35}$; (а') 0,2; (б') 0,14; (с') 0,02.

(а) *Решение* (написано Е. Павловым). Пусть $M = \{1, 2, \dots, 105\}$ — множество всех возможных исходов, $A = \{5, 10, \dots, 105\} = \{x \in M : 5 \mid x\}$ — множество благоприятных исходов. Тогда по определению вероятность множества A равна $P(A) = \frac{|A|}{|M|} = \frac{\lfloor \frac{105}{5} \rfloor}{105} = 0,2$.

25.1.6. Ответы: (а) $P(A \cup B) = P(A) + P(B)$;

(б) $P(A \cup B) = P(A) + P(B) - P(A \cap B)$;

(с) $P_{M \times N}(A \times B) = P_M(A)P_N(B)$.

25.2 Более общее определение вероятности (1). А. А. Заславский, А. Б. Скопенков

Вероятность того, что целое число от 1 до 100 делится на 7, равна 0.14 (задача 25.1.5.b'). Вероятности того, что при одновременном бросании двух монет будет 0, 1 или 2 орла, равны 0.25, 0.5 и 0.25, соответственно. Часто удобно считать «элементарными» исходами именно «делимость на 7» или «выпадение 0, 1 или 2 орлов». Иногда такие исходы возникают и без «разложения в более элементарные».

Для формализации следующее более общее определение. Пусть задано конечное множество M и каждому $m \in M$ поставлено в соответствие неотрицательное число $P(m)$, причём сумма всех этих чисел равна 1. Тогда *вероятностью* события A называется сумма чисел $P(m)$ по всем $m \in A$. Такая пара (M, P) называется (*конечным*) *вероятностным пространством*, ср. [CLRS].

25.2.1. (Загадки) Сформулируйте и докажите аналог правила

- (a) сложения; (b) умножения

для вышеприведённого обобщения.

Подмножества A и B множества M с указанным отображением $P : M \rightarrow [0, 1]$ называются *независимыми*, если $P(A \cap B) = P(A) \cdot P(B)$.

25.2.2. (a) Один стрелок попадает в цель с вероятностью 0,8, другой — 0,7. Найдите вероятность поражения цели, если оба стреляют одновременно.

(b) Рабочий обслуживает три станка. Вероятности их остановки равны соответственно 0,1; 0,2; 0,15. Найдите вероятность безотказной работы всех станков.

(c)* Отец, мать и сын увлекаются шахматами. Отец обещает сыну приз, если он выиграет две партии подряд из трёх, сыгранных поочерёдно с отцом и матерью. Сын знает, что отец играет лучше матери. С кем ему выгоднее играть первую партию?

25.2.3. (a) Вероятность рождения мальчика равна 0,515. Найдите вероятность того, что среди 6 детей не более 2 девочек.

(b)* (Загадка) Старик ловил неводом рыбу ровно тридцать лет и три года. Каждый день он ловил ровно 7 рыб, которых как раз

хватало на ужин. Живущий у старухи кот-долгожитель ест только макрель, которая ловится вдвое реже остальных рыб. В результате он 700 раз оставался голодным. Плавает ли макрель в море косяками или поодиночке?

Комментарий. Конечно, точно ответить на поставленный вопрос невозможно. Однако можно оценить, какая из двух гипотез лучше согласуется с данными. Ср. с законом больших чисел 25.5.3.b.

Схемой Бернулли из n испытаний с вероятностью успеха p (каждого испытания) называется множество $\mathbb{Z}_2^n$ упорядоченных наборов длины n из 0 и 1, вместе с функцией $P : \mathbb{Z}_2^n \rightarrow [0, 1]$, определенной формулой $P(x) = p^{|x|}(1-p)^{n-|x|}$, где $|x|$ — количество единиц в наборе x , т.е. *число успехов* для набора x . Схема Бернулли являются одной из фундаментальных теоретико-вероятностных моделей, возникающей во многих задачах.

25.2.4. В схеме Бернулли из n испытаний с вероятностью успеха p найдите

- (a) вероятность ровно k успехов;
- (b) наиболее вероятное значение числа успехов.

Приведённое определение вероятности можно обобщить на случай бесконечного множества M . (В этом случае для всех $t \in M$, кроме счётного числа, $P(t) = 0$.) Ещё более интересно следующее обобщение.

25.2.5. Найдите вероятность того, что случайная точка правильного треугольника лежит

- (a) в треугольнике, образованном средними линиями;
 - (b) во вписанном круге.
- (Формализация приводится после условий.)

Пусть $A \subset M$ — подмножества прямой (или плоскости, или пространства), имеющие длину (или площадь, или объем). Не все подмножества имеют длину (или площадь или объём), см. замечание в п. 26.5 «принцип Дирихле и его применения в геометрии». Тогда *вероятностью* подмножества A в M называется число

$$P(A) = P_M(A) := L(A)/L(M),$$

где $L(A), L(M)$ — длины (или площади, или объемы) подмножеств.

Как и в дискретном случае, когда множество M фиксировано, его подмножества, имеющие длину (или площади, или объемы), часто называются *событиями*.

25.2.6.* Сформулируйте и докажите аналоги правил суммы и произведения для вышеопределенных «геометрических» вероятностей.

25.2.7.* (а) Дуэли в городе Осторожности редко кончаются печальным исходом. Дело в том, что каждый дуэлянт прибывает на место встречи в случайный момент времени между 5 и 6 часами утра и, прождав соперника 5 минут, удаляется. В случае же прибытия последнего в эти 5 минут дуэль состоится. Какая часть дуэлей действительно заканчивается поединком?

(б) Стержень случайным образом ломают на три части. С какой вероятностью из этих частей можно составить треугольник?

(с) Найдите вероятность того, что случайный треугольник является остроугольным.

(d) С какой вероятностью случайная хорда в круге длиннее стороны вписанного в этот круг правильного треугольника?

Парадоксально, что у каждого из пунктов (с) и (d) имеются разные естественные формализации, дающие разный ответ!

Указания, ответы и решения

25.2.2. (а) *Ответ:* $1 - (1 - 0,7)(1 - 0,8) = 0,94$.

(с) *Ответ:* с отцом.

Решение. Обозначим через p_1 и p_2 вероятность выигрыша одной партии у отца и у матери соответственно: $0 < p_1 < p_2$. Обозначим через M множество строк длины 3 из символов 0 и 1 (для каждого $k = 1, 2, 3$ символ на k -м месте «кодирует» результат k -й партии). Обозначим через $P_1(m)$ и $P_2(m)$ вероятности элемента $m \in M$ в случае, когда первая партия играет с отцом и с матерью соответственно. Эти вероятности определяются правилом произведения 25.2.1. В частности, $P_1(111) = p_1 p_2 p_1$, $P_1(110) = P_1(011) = (1 - p_1) p_2 p_1$, $P_2(111) = p_2 p_1 p_2$, $P_2(110) = P_2(011) = (1 - p_2) p_1 p_2$.

Чтобы каждая из этих частей была меньше суммы двух других, изображающая разлом точка в правильном треугольнике должна лежать в правильном треугольнике, образованном средними линиями. Поэтому искомая вероятность равна $1/4$.

(с) *Первая интерпретация условия. Ответ:* $12 \ln 2 - 8$. Каждому разлому стержня из п. (b) можно сопоставить треугольник, составленный из получившихся кусков. При этом полученный треугольник остроугольный, если и только если сумма квадратов длин любых двух кусков больше квадрата длины третьего.

Вторая интерпретация условия. Ответ: $1/4$. Каждому разлому стержня из п. (b) можно сопоставить вспомогательный треугольник, величины углов которого относятся как длины получившихся кусков. При этом составить из кусков треугольник можно тогда и только тогда, когда вспомогательный треугольник остроугольный. Поэтому естественно считать, что искомая вероятность равна полученной в п. (b) величине.

(d) Если считать равномерно распределенными на окружности концы хорды, получаем $1/3$. Если середина хорды равномерно распределена в круге, то $1/4$. А, если зафиксировать перпендикулярный хорде диаметр и равномерно выбирать точку на нем, то $1/2$.

25.3 Условная вероятность (1). А. А. Заславский, А. Б. Скопенков

25.3.1. Федя знает ответы на 10 вопросов из 30. Билет состоит из двух вопросов. С какой вероятностью Федя ответит на оба вопроса?

25.3.2. (a) В ящике лежат красные и чёрные носки. Какое минимальное количество носков может быть в ящике, если вероятность того, что два случайно вытянутых носка красные, равна $1/2$?

(b) То же, если дополнительно известно, что число чёрных носков чётно.

25.3.3.* (a) С какой вероятностью треугольник, образованный тремя случайными вершинами правильного $2n$ -угольника, будет прямоугольным; остроугольным; тупоугольным?

(b) Найдите пределы полученных вероятностей при $n \rightarrow \infty$. (Подумайте о смысле полученных результатов. Ср. с задачей 25.2.7 (с).)

25.3.4. Два дворянина из свиты короля в ожидании выхода его Величества решили сыграть в кости. Они сделали одинаковые ставки и договорились, что тот, кто первым выиграет 10 партий, получает все деньги. При счёте 9:8 появился король и игру пришлось закончить. Как следует поделить деньги?

Это одна из задач, положивших начало теории вероятностей. (Решить её вам будет проще после задачи 25.3.11.) В XVII в. её предложил великому французскому математику Блезу Паскалю его знакомый — один из тех дворян, о которых говорится в задаче. Паскаль понял, что следует поделить деньги пропорционально шансам, которые имели игроки на окончательную победу в момент остановки игры. Он нашёл способ вычисления этих шансов (для любого счёта). Другой метод решения задачи, приводящий к тому же результату, нашёл другой великий математик XVII в. Пьер Ферма. Их методы основаны на следующем понятии.

Условной вероятностью подмножества A при условии подмножества B , для которого $P(B) \neq 0$, называется отношение

$$P(A|B) = P(A \cap B)/P(B).$$

Ясно, что независимость подмножеств A и B равносильна тому, что $P(A|B) = P(A)$.

25.3.5. (а) Известно, что при броске игральной кости выпало чётное число. Найдите вероятность того, что оно меньше 5.

(б) **Парадокс мальчика и девочки.** В семье два ребёнка. Известно, что один из них мальчик. Найдите вероятность того, что второй ребёнок тоже мальчик. (Мы предполагаем, что вероятности рождения мальчика и девочки равны половине и что пол второго ребёнка не зависит от пола первого.)

Для определения вероятности из предыдущего пункта независимость и условная вероятность определяются аналогично.

25.3.6. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Найдите вероятность того, что купленная лампочка горит.

Решение этой задачи обобщает следующий факт.

25.3.7. Формула полной вероятности. Если $P : M \rightarrow [0, 1]$ — вероятностная функция, $M = B_1 \sqcup \dots \sqcup B_n$ и $P(B_j) \neq 0$ (говорят, что $B_1, \dots, B_n$ — полная система событий), то

$$P(A) = P(A|B_1)P(B_1) + \dots + P(A|B_n)P(B_n).$$

25.3.8. Победитель в поединке двух боксёров определяется большинством голосов трёх судей. Двое судей выносят верное решение с вероятностью p , а третий голосует, бросая монету. Найдите вероятность принятия судьями верного решения.

25.3.9.* Правила распространённой в ряде стран игры следующие: игрок бросает две кости. Он выигрывает, если сумма выпавших очков равна 7 или 11, и проигрывает, если она равна 2, 3 или 12. Во всех остальных случаях он бросает кости до тех пор, пока не выиграет, выбросив первоначальную сумму, или не проиграет, выбросив 7. Найти вероятность выигрыша.

25.3.10. Лампочки выпускаются двумя заводами, причём первый из них производит 70 % всей продукции. Лампочки, произведённые первым заводом, горят с вероятностью 0,98, вторым — 0,95. Купленная лампочка оказалась бракованной. Найдите вероятность того, что она выпущена первым заводом.

Решение этой задачи обобщает следующий факт.

25.3.11. Формула Байеса. Для любых вероятностной функции $P : M \rightarrow [0, 1]$ и подмножеств $A, B \subset M$ выполнено $P(B|A) = P(A|B)P(B)/P(A)$.

Часто применяется следствие формул 25.3.7 и 25.3.11:

$$P(X|A) = \frac{P(A|X)P(X)}{P(A|B_1)P(B_1) + \dots + P(A|B_n)P(B_n)}.$$

25.3.12. Вероятность того, что изделие бракованное, равна 0,04. Если изделие бракованное, то оно пройдёт тест с вероятностью 0,05, а иначе — с вероятностью 0,98. Найдите (с точностью до 0,0001) вероятность того, что изделие, дважды выдержавшее тест, бракованное.

25.3.13. Король Артур проводит рыцарский турнир по системе с выбыванием. Среди 2^n одинаково искусных рыцарей два близнеца. Найдите вероятность их встречи.

25.3.14.* Разборчивая невеста. (Загадка.) Девушка выбирает себе жениха из n претендентов, поочерёдно делающих ей предложение. Каждое предложение она может принять (тогда всё заканчивается) или отвергнуть (отвергнутый претендент с повторным предложением не обращается). Она хочет действовать так, чтобы вероятность выбрать наиболее достойного жениха была наибольшей.

(а) Докажите, что оптимальная стратегия имеет следующий вид: отвергнуть первые $s(n)$ предложений, а затем принять первое предложение от претендента, превосходящего всех предыдущих.

(b) Определите оптимальное значение $s(n)$.

Указания, ответы и решения

25.3.1. Ответ: $\frac{3}{29}$.

Решение (написано П. Белопашенцевой). Обозначим через M множество всех неупорядоченных пар различных чисел от 1 до 30. Это множество соответствует множеству всех возможных билетов. Количество элементов в M равно $|M| = \binom{30}{2}$.

Обозначим через A множество всех неупорядоченных пар различных чисел от 1 до 10. Множество A соответствует множеству выученных Федей билетов. Количество элементов в A есть $|A| = \binom{10}{2}$. Вероятность подмножества A в множестве M есть по определению отношение $P_M(A) = |A|/|M| = \binom{10}{2}/\binom{30}{2} = \frac{10 \cdot 9/2}{30 \cdot 29/2} = \frac{3}{29}$.

25.3.2. Ответы: (а) 4; (b) 21.

Указание. Обозначим через r и b количество красных и чёрных носков соответственно. Тогда вероятность вытащить два красных носка равна $\frac{r(r-1)}{(r+b)(r+b-1)}$. Это выражение равно $1/2$ для бесконечного множества пар (r, b) , наименьшими из которых будут $(3, 1)$ и $(15, 6)$. Подробнее см. задачу 1 из книги [Мо].

25.3.3.* (а) Ответ: $\frac{3}{2n-1}$, $\frac{n-2}{2(2n-1)}$, $\frac{3(n-2)}{2(2n-1)}$.

Указание. Первую вершину можно считать фиксированной. Если вторая попадает в противоположную точку, то треугольник точ-

что вероятность выбрать наилучшего жениха, отвергнув k -го, является убывающей функцией от k . Поэтому пока первая вероятность меньше второй, женихов надо отвергать, а когда первая вероятность станет больше, надо принять предложение первого жениха, превосходящего всех предыдущих.

(b) Если невеста действует по описанной стратегии, то она получает лучшего жениха при выполнении следующих двух условий: номер k этого жениха больше $s = s(n)$ и лучший из первых $k - 1$ женихов попадает в число первых s . Вероятность этого равна $\frac{1}{n} \left(1 + \frac{s}{s+1} + \dots + \frac{s}{n-1} \right)$, что примерно равно $\frac{s}{n} \ln(n/s)$. Потому оптимальное значение s примерно равно $\frac{n}{e}$. При этом вероятность выбрать лучшего жениха при больших n примерно равна $\frac{1}{e}$ (см. [Мо, задача 47], [GZ]).

25.4 Математическое ожидание (3). А. А. Заславский, А. Б. Скопенков

25.4.1. (a) Монета подбрасывается 5 раз. Для каждого $k = 0, 1, 2, 3, 4, 5$ найдите вероятность того, что выпало k орлов.

(b) Федя знает ответы на 20 из 30 вопросов. В билет входят 3 вопроса. Для каждого $k = 0, 1, 2, 3$ найдите вероятность того, что Федя сможет ответить на k вопросов.

Пусть дано конечное или счётное множество M и для каждого элемента $m \in M$ задано число (вероятность) $P(m) \geq 0$, причем $\sum_{m \in M} P(m) = 1$. *Случайной величиной* называется функция $\xi : M \rightarrow Y$ (обычно $Y = \mathbb{Z}_2, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \dots$ — числовое множество). *Распределением* случайной величины ξ называется функция $p_\xi : Y \rightarrow [0, 1]$, заданная формулой

$$p_\xi(y) := \sum_{\xi(m)=y} P(m).$$

Комментарии. Как правило, при изучении случайной величины не требуется знать, на каком множестве она определена. Достаточно знать только её распределение.

Если $Y = \mathbb{R}$, то *функцией распределения* называется функция $F_\xi : Y \rightarrow [0, 1]$, заданная формулой $F_\xi(y) := \sum_{\xi(m) < y} P(m)$.

25.4.2. (a) Вам предлагается такая игра. Вы платите 2 конфеты, затем бросается игральная кость, и вы получаете столько конфет, сколько очков выпадает. Выгодна ли вам эта игра?

(b) Правила те же, только в случае выпадения 1 очка вы платите 100 конфет. (У вас достаточно конфет, чтобы заплатить.) Выгодна ли вам эта игра?

(c) Вы кладете в банк 8 конфет, после чего бросается игральная кость. Если выпадает 2, 3 или 4 очка, то вы получаете назад свой вклад плюс еще 1 конфету вдобавок. Если выпадает 5 или 6 очков («рост рынка»), то вы получите даже плюс 2 конфеты вдобавок. А если выпадет 1 очко, то это «кризис», и вы теряете весь свой вклад. Выгодна ли вам эта игра?

(d) В распространённой азартной игре игрок может делать ставку на один из номеров от 1 до 6. Бросаются 3 кости, и если выбранный номер выпал хотя бы на одной, то игрок получает свою ставку плюс столько же за каждое появление выбранного номера. Выгодна ли игра для игрока?

25.4.3. (a) *Cherchez la femme*. На русско-французской встрече не было представителей других стран. Суммарное количество денег у французов оказалось больше суммарного количества денег у русских, и суммарное количество денег у женщин оказалось больше суммарного количества денег у мужчин. Обязательно ли на встрече была француженка?

(b) Денежные купюры разного достоинства и разных стран упакованы в два чемодана. Средняя стоимость купюры равна 100 рублям. Общее число купюр в левом чемодане больше, чем в правом. Обязательно ли в левом чемодане найдется купюра стоимостью не более 200 рублей? (Ср. с неравенством Маркова 25.4.4.с.)

(c)* Для любых целых $l, q > 0$ существует граф, не содержащий несамопересекающихся циклов длины менее l и который невозможно правильно раскрасить в q цветов.

Утверждение 25.4.3.с доказывается при помощи излагаемой ниже теории, см. [GDI, §6.3].

Математическим ожиданием или *средним значением* случайной величины $\xi : M \rightarrow Y$ называется сумма

$$\mathbb{E}\xi := \sum_{m \in M} \xi(m)P(m).$$

Комментарий. Если множество M бесконечно, то это определение нуждается в уточнении. Сумма ряда в правой части называется *математическим ожиданием*, только когда этот ряд сходится абсолютно. В противном случае говорят, что у случайной величины *не существует математического ожидания*. В дальнейшем мы предполагаем, что для всех рассматриваемых случайных величин математические ожидания существуют.

25.4.4. Пусть $\xi : M \rightarrow \mathbb{R}$ — случайная величина и $a \in \mathbb{R}$.

- (а) Пусть $\xi(m) = a$ для любого $m \in M$. Найдите $\mathbb{E}\xi$.
- (б) Если $\mathbb{E}\xi \leq a$, то существует $m \in M$, для которого $\xi(m) \leq a$.
- (в) *Неравенство Маркова.* $P(|\xi| > a) \leq \mathbb{E}|\xi|/a$ для любого $a > 0$.
(Здесь через $|\xi| > a$ сокращённо обозначено событие $\xi^{-1}(a, +\infty)$. Ср. с задачей 25.4.3.б.)

25.4.5. (а,б) В задачах 25.4.1.аb найдите средние значения количества орлов и правильных ответов, соответственно.

(в) В схеме Бернулли из n испытаний с вероятностью успеха p найдите среднее значение числа успехов.

25.4.6. Пусть $\xi, \eta : M \rightarrow \mathbb{R}$ — случайные величины.

- (а) $\mathbb{E}(a\xi) = a\mathbb{E}\xi$ для любого $a \in \mathbb{R}$.
- (б) $\mathbb{E}(\xi + \eta) = \mathbb{E}\xi + \mathbb{E}\eta$.
- (в) $\mathbb{E}\xi = \sum_{y \in Y} yp_{\xi}(y)$.

25.4.7. Найдите

- (а) наиболее вероятное; (б) среднее
число бросков кубика до появления первой шестерки.

25.4.8. Кубик бросается до первого появления числа, меньшего 6, но не более четырёх раз. Найдите среднее число бросков.

25.4.9. Каждая из двух одинаковых колод карт перетасовывается, и карты последовательно парами выкладываются на стол. Найдите среднее значение числа пар, карты в которых совпадают.

25.4.10. Предприниматели предоставляют всем рабочим выходной, если хотя бы у одного из них день рождения. Остальные дни являются рабочими. Сколько человек нужно принять на работу, чтобы среднее значение числа рабочих человекодней было максимальным?

25.4.11. В ряд в случайном порядке выписаны m единиц и n нулей. Найдите среднее число серий из k одинаковых цифр подряд.

25.4.12. Из колоды в 52 карты вынимаются карты до первого туза. Сколько карт в среднем будет вынуто?

25.4.13. По узкой дороге в одном направлении едут n машин. Вначале скорости всех машин различны. Каждая машина едет с постоянной скоростью, пока не догонит едущую впереди, после чего едет со скоростью передней машины. В результате через достаточно большое время машины разбиваются на несколько групп. Найдите среднее значение числа групп.

25.4.14. (Загадка.) Площадка имеет форму квадрата со стороной 350 м. При измерении стороны вероятность ошибки ± 10 м равна 0,16, ± 20 м — 0,08, ± 30 м — 0,05. Найдите среднее значение измеренной площади.

Комментарий. На самом деле ответ на этот вопрос зависит от того, как формализовано понятие измерения площади. Если независимо измерить каждую из сторон квадрата и перемножить полученные значения, то по задаче 25.4.15.с среднее значение будет равно 350^2 м². Если же измерить только одну сторону и возвести результат в квадрат, то ответ будет другим.

25.4.15. (а) (Загадка) Можно ли выразить $\mathbb{E}\xi\eta$ через $\mathbb{E}\xi$ и $\mathbb{E}\eta$?

(b) *Неравенство Коши-Буняковского.* Если $\xi(t), \eta(t) \geq 0$ для любого $t \in M$, то $(\mathbb{E}\xi\eta)^2 \leq \mathbb{E}\xi^2 \mathbb{E}\eta^2$.

(с) Событие $\xi^{-1}(y) = \{t \in M: \xi(t) = y\}$ в дальнейшем сокращённо обозначается $\xi = y$. Случайные величины ξ и η называются

независимыми, если события $\xi = x$ и $\eta = y$ независимы при любых $x, y \in Y$, т. е.

$$P(m \in M: \xi(m) = x \text{ и } \eta(m) = y) = p_\xi(x)p_\eta(y).$$

Неформально независимость означает, что значения одной из случайных величин не влияют на распределение другой. Например, для схемы Бернулли любые две из определённых на множестве $\mathbb{Z}_2^n$ случайных величин $\xi_i(x_1, \dots, x_n) := x_i$, $i = 1, \dots, n$, независимы.

Докажите, что если случайные величины ξ и η независимы, то математическое ожидание их произведения равно произведению их математических ожиданий: $\mathbb{E}\xi\eta = \mathbb{E}\xi\mathbb{E}\eta$.

Указания, ответы и решения

Большинство решений получены редактированием текстов, написанных Т. Чергановым.

25.4.1. (а) *Ответ:* $p(0) = p(5) = \frac{1}{32}$, $p(1) = p(4) = \frac{5}{32}$, $p(2) = p(3) = \frac{10}{32}$.

(b) *Ответ:* $p(0) = \frac{6}{203}$, $p(1) = \frac{45}{203}$, $p(2) = \frac{95}{203}$, $p(3) = \frac{57}{203}$.

Решение. Множество билетов M — это множество неупорядоченных троек различных чисел от 1 до 30. Тогда $|M| = \binom{30}{3}$.

Обозначим через A_0 множество неупорядоченных троек различных чисел от 21 до 30. Тогда $P(A_0) = \binom{10}{3} / \binom{30}{3} = \frac{6}{203}$.

Обозначим через A_1 множество неупорядоченных троек различных чисел, в которых два числа принадлежат $\{21, \dots, 30\}$ и одно число принадлежит $\{1, \dots, 20\}$. Тогда $P(A_1) = 20 \binom{10}{2} / \binom{30}{3} = \frac{45}{203}$.

Аналогично $P(A_2) = 10 \binom{20}{2} / \binom{30}{3} = \frac{95}{203}$ и $P(A_3) = \binom{20}{3} / \binom{30}{3} = \frac{57}{203}$.

25.4.2. (d) *Ответ:* нет.

Решение. Обозначим через ξ число выпадений выбранного номера. Тогда

$$p_\xi(0) = \frac{5^3}{6^3}, \quad p_\xi(1) = \frac{3 \cdot 5^2}{6^3}, \quad p_\xi(2) = \frac{3 \cdot 5}{6^3}, \quad p_\xi(3) = \frac{1}{6^3}.$$

Значит, математическое ожидание выигрыша при единичной ставке равно

$$\frac{2 \cdot 3 \cdot 5^2 + 3 \cdot 3 \cdot 5 + 4}{6^3} \approx 0.92 < 1.$$

25.4.15. (с) *Решение.*

$$\begin{aligned}
\mathbb{E}\xi\eta &= \sum_{m \in M} \xi(m)\eta(m)P(m) = \sum_{x \in X, y \in Y} xyP(\xi(m) = x, \eta(m) = y) = \\
&= \sum_{x \in X, y \in Y} xyp_{\xi}(x)p_{\eta}(y) = \sum_{x \in X} xp_{\xi}(x) \sum_{y \in Y} yp_{\eta}(y) = \mathbb{E}\xi\mathbb{E}\eta.
\end{aligned}$$

25.5 Дисперсия и ее применения (3). *А. А. Заславский, А. Б. Скопенков*

Дисперсией случайной величины ξ называется число

$$\mathbb{D}\xi = \mathbb{E}((\xi - \mathbb{E}\xi)^2).$$

Комментарий. Если множество значений случайной величины бесконечно, то дисперсия может не существовать. В дальнейшем предполагается, что для всех рассматриваемых случайных величин дисперсия существует.

25.5.1. (а) Найдите дисперсию числа успехов для схемы Бернулли из n испытаний с вероятностью успеха p .

(b) Для любой случайной величины ξ выполнено $\mathbb{D}\xi = \mathbb{E}\xi^2 - (\mathbb{E}\xi)^2$.

(с) Для любых ли случайных величины ξ, η выполнено $\mathbb{D}(\xi + \eta) = \mathbb{D}\xi + \mathbb{D}\eta$?

(d) Для любых независимых случайных величины ξ, η выполнено $\mathbb{D}(\xi + \eta) = \mathbb{D}\xi + \mathbb{D}\eta$.

25.5.2. Кооператив отгружает железные балки. Средняя длина балки 3 м, дисперсия 0,09 м². Сколько балок надо заказать, чтобы с вероятностью, не меньшей чем 0,999, хотя бы 1000 из них имели длину не менее 2 м?

25.5.3. (а) **Неравенство Чебышёва.** Для любой случайной величины ξ и любого $t > 0$ выполнено

$$P(|\xi - \mathbb{E}\xi| \geq t) \leq \mathbb{D}\xi/t^2.$$

(b) **Закон больших чисел.** Обозначим через ξ число успехов в схеме Бернулли из n испытаний с вероятностью успеха p . Для любого $t > 0$ выполнено

$$P(|\xi - np| \geq t) \leq np(1-p)/t^2$$

Закон больших чисел означает, что при большом числе испытаний вероятность того, что число успехов сильно отличается от его среднего значения, мала. Аналогичный закон справедлив не только для схемы Бернулли: если наблюдать много независимых реализаций произвольной случайной величины, то их среднее арифметическое с большой вероятностью будет мало отличаться от её среднего значения. Этот закон позволяет, например, проводить социологические исследования, в которых на основе опроса некоторого количества случайно выбранных людей (достаточно большого, но составляющего малую часть всего населения) делаются выводы о распространённости в обществе тех или иных мнений и предпочтений.

25.5.4. В условиях задачи 25.2.3.b предположим, что макрель плавают

(a) поодиночке; (b) косяками.

Тогда вероятность того, что число голодных дней кота меньше 1000,

(a) больше 0.99; (b) меньше 0.0001.

Указания, ответы и решения

Большинство решений получены редактированием текстов, написанных Т. Чергановым.

25.5.1. (a) *Ответ:* $np(1-p)$.

(b) *Решение*

$$\begin{aligned} \mathbb{D}\xi &= \mathbb{E}(\xi - \mathbb{E}\xi)^2 = E(\xi^2 - 2\xi\mathbb{E}\xi + (\mathbb{E}\xi)^2) = \\ &= \mathbb{E}\xi^2 - 2(\mathbb{E}\xi)(\mathbb{E}\xi) + (\mathbb{E}\xi)^2 = \mathbb{E}\xi^2 - (\mathbb{E}\xi)^2. \end{aligned}$$

26.8 Собери квадрат (3*). *М. Б. Скопенков, О. А. Малиновская, С. А. Дориченко, Ф. А. Шаров*

Этот пункт посвящён решению такой задачи (для некоторых частных случаев).

Задача. Когда из прямоугольников, подобных данному, можно составить квадрат?

В процессе решения мы познакомимся с красивыми применениями алгебры в комбинаторной геометрии, а именно — систем линейных уравнений и многочленов с целыми коэффициентами. Для решения задач необходимо первоначальное знакомство с этими темами, см., например, [Gu]. Желательно также первоначальное знакомство с задачами на разрезание, см., например, [Sa97].

Наш подход к решению развивает идеи книги [Ya68].

Другой подход к решению — это физическая интерпретация, использующая электрические цепи (хотя без неё решать проще). Познакомиться с этой физической интерпретацией и её применением к решению поставленной задачи можно в статьях [SPD, SMD]. Увлекательный рассказ об истории её возникновения можно прочитать в книге [Ga99].

Наводящие вопросы

- У меня есть мысль! — сказал удав, открывая глаза. — Мысль. И я её думаю.
- Какая мысль? — спросила мартышка.
- Так сразу не скажешь...
- Ух ты! — подпрыгнула мартышка. — Ох, какая хорошая мысль. А можно я её тоже немножко подумаю?

Г. Остёр. Бабушка удава

26.8.1.° Верно ли, что при любых натуральных m и n из нескольких прямоугольников $m \times n$ можно сложить квадрат? Выберите верный вариант ответа:

- 1) верно; 2) неверно.

26.8.2. Дизайнеру заказали рамы для квадратного окна. На проектах (рис. 2.37 А, В) показано, как должны примыкать стёкла друг к другу и как они должны быть ориентированы (короткой или длинной стороной вверх). Можно ли сделать все стёкла в каждой раме подобными прямоугольниками?



А



В

Рис. 2.37: Проекты оконных рам; см. задачу 26.8.2

26.8.3. Можно ли разрезать квадрат на три подобных, но неравных прямоугольника?

26.8.4. Можно ли разрезать квадрат на 5 квадратов?

26.8.5. Все полки у шкафа на рис. 2.38 С, как и все лоскутки, из которых сшито одеяло на рис. 2.38 D — квадратные. Являются ли квадратными сами шкаф и одеяло?

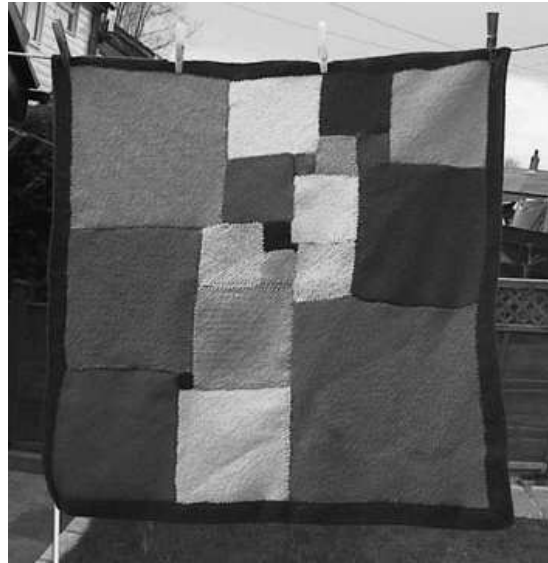
26.8.6. Можно ли замостить всю плоскость попарно различными квадратами, длины сторон которых — целые числа?

26.8.7. Можно ли разрезать квадрат на прямоугольники с отношением сторон $2 + \sqrt{2}$? То же для $2 - \sqrt{2}$, для $3 + 2\sqrt{2}$ и для $3 - 2\sqrt{2}$.

26.8.8. Является ли $1 + \sqrt{2}$ суммой квадратов чисел вида $a + b\sqrt{2}$, где a и b рациональны?



C



D

Рис. 2.38: Шкаф и одеяло; см. задачу 26.8.5

Определение. Пусть на прямоугольном листе бумаги нарисовано разбиение на прямоугольники. Разрешается разрезать лист вдоль любого отрезка на два прямоугольника, потом произвести такие операции по отдельности с каждой из получившихся частей и так далее. Если таким образом можно реализовать исходное разбиение, то назовём его *тривиальным*. Например, разбиения на рис. 2.37 тривиальные, а на рис. 2.38 нетривиальные.

Следующие 4 задачи предлагается сначала решить для тривиальных разбиений, а уже потом подумать над произвольными разбиениями. В последующих подпунктах будут даны подсказки к решению этих трудных задач.

26.8.9. Какие прямоугольники можно (тривиально) разрезать на прямоугольники со стороной 1?

26.8.10. Какие прямоугольники можно (тривиально) разрезать на квадраты?

26.8.11. Можно ли квадрат (тривиально) разрезать на прямоугольники с отношением сторон $\sqrt{2}$? То же для $1 + \sqrt{2}$.

Все числа, которые можно представить в виде $x = a + b\sqrt{2}$ с рациональными a и b , назовём *хорошими*.

26.8.12. (Основная задача.) При каких хороших x квадрат можно (тривиально) разрезать на прямоугольники с отношением сторон x ?

Прямоугольник из квадратов.

Ты, дорога, иду по тебе и гляжу, но мне думается,
Мне думается, в тебе много такого, чего не увидишь глазами.

Уолт Уитмен. Песня большой дороги

В этом подпункте мы наметим новый вариант элементарного решения задач 26.8.10 и 26.8.12. В этом подпункте латинские буквы a , b , c , d и эти же буквы с индексами обозначают *рациональные* числа.

26.8.13. Можно ли прямоугольник $1 \times \sqrt{2}$ разрезать на квадраты с рациональными сторонами? А со сторонами, которые либо рациональны, либо имеют вид $b\sqrt{2}$? А со сторонами, которые являются произвольными хорошими числами? Те же вопросы для прямоугольников $1 \times (1 + \sqrt{2})$ и $1 \times (2 + \sqrt{2})$.

Для доказательства невозможности разрезаний естественно использовать площадь и её *аддитивность*: площадь целого равна сумме площадей частей. Вряд ли получится ответить на вопросы задачи 26.8.13 для прямоугольника $1 \times (2 + \sqrt{2})$ без следующего обобщения понятия площади (мы обобщаем понятие площади так, чтобы площадь этого прямоугольника стала отрицательной, а площади квадратов оставались неотрицательными).

Определение. Пусть x — действительное число. Назовём *x -площадью* (или *площадью Гамеля*) прямоугольника $(a + b\sqrt{2}) \times (c + d\sqrt{2})$ число $(a + bx)(c + dx)$. Число $\bar{s} := a - b\sqrt{2}$ назовём *сопряжённым* к числу $s = a + b\sqrt{2}$.

26.8.14. Обычная площадь прямоугольника $(a + b\sqrt{2}) \times (c + d\sqrt{2})$ и сопряжённое к ней число — это одни из его x -площадей. Чему равно x в каждом из случаев?

26.8.15. Найдите все прямоугольники вида $(a + b\sqrt{2}) \times (c + d\sqrt{2})$, x -площади которых неотрицательны при всех x .

26.8.16. Аддитивность x -площади. Если прямоугольник разрезан на конечное число прямоугольников, стороны которых — хорошие числа, то для любого $x \in \mathbb{R}$ x -площадь разрезаемого прямоугольника равна сумме x -площадей прямоугольников, на которые он разрезан.

Указание. Начните со случая разрезания на 2 прямоугольника.

26.8.17. Решите задачи 26.8.10 и 26.8.12 для частного случая, когда стороны всех квадратов и всех прямоугольников, участвующих в разрезании, — хорошие числа (разрезание не обязательно тривиально).

Для доказательства теоремы Дена в общем случае определение x -площади нам уже не годится: ведь она определена только для хороших чисел, а теперь у нас в разрезании могут присутствовать квадраты с какими угодно сторонами.

В следующих трёх задачах мы считаем, что прямоугольник $s_0 \times t_0$ разрезан на прямоугольники $s_1 \times t_1, s_2 \times t_2, \dots, s_N \times t_N$, причем s_0 и t_0 несоизмеримы.

26.8.18. Обозначим

$$P = \{s_0, t_0, s_1, t_1, \dots, s_N, t_N\}.$$

Тогда можно выбрать такие числа $e_1, e_2, \dots, e_n \in P$, чтобы любое число $p \in P$ единственным образом представлялось в виде

$$p = as_0 + bt_0 + a_1e_1 + a_2e_2 + \dots + a_ne_n.$$

Указание. Начните с примера, изображённого на рис. 2.39.

Зафиксируем набор чисел $s_0, t_0, e_1, e_2, \dots, e_n$ из задачи 26.8.18. Он называется *базисом*.

Определение. Пусть y — действительное число. Назовём y -*площадью* прямоугольника со сторонами

$as_0 + bt_0 + a_1e_1 + a_2e_2 + \dots + a_ne_n$ и $cs_0 + dt_0 + c_1e_1 + c_2e_2 + \dots + c_ne_n$ число $(a + by)(c + dy)$.

$2 + \sqrt{2}$	
$1/3 \times \sqrt{3}$	$1 \times (2 + \sqrt{2} - \sqrt{3})$
$2/3 \times \sqrt{3}$	

Рис. 2.39: К построению базиса

Обратите внимание на то, что при $y = x$ и хороших несоизмеримых s_0, t_0 это определение не всегда эквивалентно определению x -площади выше!

26.8.19. Вычислите y -площадь разрезаемого прямоугольника $s_0 \times t_0$. Является ли она неотрицательной при всех y ?

26.8.20. Докажите, что для любого y y -площадь разрезаемого прямоугольника $s_0 \times t_0$ равна сумме y -площадей прямоугольников, на которые он разрезан.

26.8.21. Теорема Дена. Если прямоугольник разрезан на квадраты (не обязательно равные), то отношение его сторон рационально.

26.8.22. Если квадрат 1×1 разрезан на прямоугольники, отношение сторон каждого из которых — хорошее число, то и сами стороны всех прямоугольников — хорошие числа.

От разрезаний к корням многочленов

Вот испытанье для мудрых,
Для мудрости, не пройденной в школе...
Уолт Уитмен. Песня большой дороги

26.8.23. Из нескольких прямоугольников с отношением сторон r составили прямоугольник. Докажите, что стороны полученного прямоугольника относятся как $P(r) : Q(r)$, где $P(x)$ и $Q(x)$ — некоторые многочлены с целыми коэффициентами.

26.8.24. Эти многочлены можно выбрать так, что $P(-x)/Q(-x) = -P(x)/Q(x)$ при всех x и $P(x)/Q(x) > 0$ при всех $x > 0$.

WHEN ANY GROUP OF N ELEMENTS IS CYCLIC? ¹

V. Bragin, Ant. Klyachko and A. Skopenkov ²

We give a simple proof of the well-known fact: any group of n elements is cyclic if and only if n and $\phi(n)$ are coprime. This note is accessible for students familiar with permutations and basic number theory. No knowledge of group theory is required; a few necessary notions are introduced in the course of the proof.

Introduction

We call a *group* a nonempty family G of transformations (i.e. permutations or rearrangements) of some set, which family is closed with respect to composition and taking inverse transformation (i.e. if $f, g \in G$, then $f \circ g \in G$ and $f^{-1} \in G$). Common term: transformation group. Cf. [A, comment to problem 5].

If a finite group G contains an element g such that G consists of all powers of g (i.e. $G = \{g, g^2, \dots, g^n, \dots\}$), then group G is called *cyclic*.

We give a simple proof of the following well-known fact.

Theorem. *Any group consisting of n elements is cyclic if and only if n and $\phi(n)$ are coprime.*

Here $\phi(n)$ is the number of positive integers not exceeding n and coprime to n (the Euler function). Note that n and $\phi(n)$ are coprime if and only if in the prime decomposition $n = p_1 \dots p_k$

(*) all p_i are different and

(**) p_i does not divide $p_j - 1$ for any i and j .

Although we did not find such a proof in the literature, we do not claim any novelty. ³ One can see from [BKKSS] (or from the complete Russian version of this text) how to invent this proof.

Proof of the “only if” part.

If g and h are transformations of disjoint sets M and N , then we can regard them as transformations of $M \sqcup N$ and hence take their composition.

A cycle $(a_1, a_2, \dots, a_n)$ is the transformation of a set containing $a_1, a_2, \dots, a_n$ that carries a_n to a_1 and a_i to a_{i+1} for each $i < n$, whereas it carries every other element to itself.

If condition (*) above is violated, e.g., $p_1 = p_2 = p$, then the following group consists of n elements and is not cyclic:

$$\left\{ (1, 2, \dots, p)^i \circ (p+1, p+2, \dots, p+\frac{n}{p})^j \mid i = 1, \dots, p, j = 1, \dots, \frac{n}{p} \right\}.$$

Assume that condition (**) above is violated, e.g., p_1 divides $p_2 - 1$. Denote by $\mathbb{Z}_k$ the set of residues modulo k with the summation and the multiplication operations. Then from the primitive root theorem it follows that there is $a \in \mathbb{Z}_{p_2}$ for which the powers $a, a^2, \dots, a^{p_1} = 1$ are different. Denote by G_{p_1, p_2} the group of transformations $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$ defined by the formula $f_{k, l}(x, y) := (a^k x, lx + y)$ for $k \in \mathbb{Z}_{p_1}$ and $l \in \mathbb{Z}_{p_2}$. ⁴ Then the following group is not cyclic (it is even nonabelian):

$$\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}. \quad QED$$

Proof of the “if” part.

Denote by $|X|$ the number of elements in a set X . Denote given group by G .

We use the induction on the number of prime factors of $|G|$. If $|G|$ is a prime, then the “if” part is implied by the following Lagrange Theorem.

¹We would like to acknowledge M. Vyalyi, P. Kozhevnikov and K. Kohas for useful discussions.

²Homepage: www.mccme.ru/~skopenko. Supported by Simons-IUM Fellowship

³Although we do not use the Sylow theorems, our argument in the second case below is similar to their proof. We do not use the notion of a quotient group, as opposed to more traditional proofs (see, e.g., [B]).

⁴In more advanced notation $G_{p_1, p_2} := \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, l \in \mathbb{Z}_{p_2} \right\}$.

The **order** $\text{ord } a$ of an element a of a group with the identity element e is the minimal positive integer n such that $a^n = e$. If the group is finite, it is clear that such n exists.

Lagrange Theorem (particular case). *The number of elements of any finite group is divisible by the order of any its element.*

Proof. Denote the group by G . For each $x \in G$ consider the set $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$. By the definition of order these elements are different. Therefore this set contains $\text{ord } f$ elements. If $xf^k = yf^l$, then $y = xf^{k-l}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by $\text{ord } f$. QED

Now suppose that the number of prime factors in $|G|$ is greater than one. We need the following general version of the Lagrange Theorem.

A **subgroup** of a group G is a subset of G that is itself a group.

Lagrange Theorem. *The number of elements of any finite group is divisible by the number of elements of any subgroup.*

Proof. Denote the group by G and the subgroup by $\{h_1, h_2, \dots, h_m\}$. For each $x \in G$ consider the set $\{xh_1, xh_2, \dots, xh_m\}$. This set contains m elements. If $xh_k = yh_l$, then $y = xh_k h_l^{-1}$. Therefore for different x these sets either coincide or are disjoint. Thus $|G|$ is divisible by m . QED

A **maximal subgroup** of a group is a maximal by inclusion subgroup not coinciding with G and containing more than one element. By the induction hypothesis and the Lagrange Theorem, *each maximal subgroup is cyclic.*

For an element f of a group G let $\langle f \rangle$ be the set of all powers of f (including zero and negative ones). The element f is called **generating** for the (cyclic) subgroup $\langle f \rangle$.

Suppose to the contrary that the group G is noncyclic. Then each element is contained in a maximal subgroup.

Elements f, g of a group G are **conjugate** in G if $g = b^{-1}fb$ for some $b \in G$.

First case: *generator f of some maximal subgroup is conjugate only to (some of) its powers.* Take $h \in G \setminus \langle f \rangle$. Let q be the minimal positive integer n such that $h^n \in \langle f \rangle$. Such a q exists because $h^{\text{ord } h} \in \langle f \rangle$.

Proof that $|G|$ is divisible by q . Let $\text{ord } h = qt + r$ be division of $\text{ord } h$ on q with remainder r . Then $h^r = h^{\text{ord } h - qt} \in \langle f \rangle$ and $0 \leq r < q$. Hence $r = 0$ by the minimality of q . So $\text{ord } h$ is divisible by q . Therefore by Lagrange Theorem $|G|$ is divisible by q . QED

Proof that $fh = hf$. Since $h^{\text{ord } h} \in \langle f \rangle$, using division with a remainder we obtain that By the condition of the first case $h^{-1}fh = f^k$ for some $k \in \mathbb{Z}$. The inclusion $h^q \in \langle f \rangle$ implies $f = h^{-q}fh^q = f^{k^q}$ (here the last equality holds for each q and is proved by induction on q). Therefore $k^q \equiv 1 \pmod{\text{ord } f}$. Hence k and $\text{ord } f$ are coprime. By conditions (*), (**) and the Lagrange Theorem $|G|$ and $\varphi(\text{ord } f)$ are coprime. Since $|G|$ is divisible by q , numbers q and $\varphi(\text{ord } f)$ are coprime. So there are integers x and y such that $qx + \varphi(\text{ord } f)y = 1$. Thus $k \equiv k^{qx + \varphi(\text{ord } f)y} \equiv 1 \pmod{\text{ord } f}$. Hence $fh = hf$. QED

Completion of the argument for the first case. Since $fh = hf$, the group G contains a subgroup

$$\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$$

of $q \text{ord } f$ elements. Hence by condition (*) and the Lagrange Theorem $\text{ord } f$ is coprime to q . Since $(fh)^j = f^j h^j$ for each j , we obtain that $\text{ord}(fh)$ is divisible both by q and by $\text{ord } f$. Hence $\text{ord}(fh) = q \text{ord } f$. Thus $\text{ord}(fh) = q \text{ord } f$. Since the subgroup $\langle f \rangle$ is maximal, we have $\langle fh \rangle = G$. Thus G is cyclic. Contradiction. QED

Second case: *generator of any maximal subgroup is conjugate not only to its powers.*

The **product of subsets** X and Y of a group G is the set of all products xy , where $x \in X$ and $y \in Y$. If one of these subsets consists of only one element, e.g., $Y = \{y\}$, then we write Xy instead of $X\{y\}$.

Assertion 1. Any maximal subgroup F contains the **center**

$$Z = Z(G) := \{a \in G : ga = ag \text{ for any } g \in G\},$$

i.e., the set of elements commuting with each element of the group.

Proof. Otherwise FZ is a larger commutative subgroup. By the maximality of F we have $FZ = G$. Hence G is commutative. This contradicts to the assumption of the second case. QED

Assertion 2. The intersection of two maximal subgroups equals the center.

Proof. A nontrivial element of the intersection commutes with all elements of both subgroups. Hence it commutes with any product of several multiples, each multiple being an element of one of our subgroups. The set of such products is a subgroup. By the maximality of our subgroups this subgroup coincides with the entire group. Therefore the intersection is contained in the center.

Assertion 1 implies the converse inclusion. QED

Conclusion of the proof of the second case: calculations. Recall that any element of G is contained in certain maximal subgroup. By Assertion 2 for any *non-central* element such a subgroup is unique. So the group is split into the center and disjoint union of complements of maximal subgroups to the center. The number of elements in such complements are the same for conjugate subgroups. Denote by $\widehat{F}$ the number of non-central elements of G in the union of subgroups conjugate to given maximal subgroup F . Let $F_1, \dots, F_s$ be a maximal family of pairwise non-conjugate maximal subgroups. Then

$$|G| = |Z| + \sum_{i=1}^s \widehat{F}_i.$$

By the left inequality in the following Assertion 3 the number of summands is at most one; by the right inequality one summand is also impossible. QED

Assertion 3. $|G|/2 \leq \widehat{F} < |G| - |Z|$.

Proof. A subgroup conjugate to a maximal subgroup is also maximal. (Indeed, if $g^{-1}Fg \subset F' \subset G$, then $F \subset gF'g^{-1} \subset G$.)

Consider the set

$$N(F) := \{a \in G : Fa = aF\}.$$

Then the number of different subgroups conjugate to F (including F) is $|G|/|N(F)|$.

(Indeed, the conjugation by each element of G takes F to a conjugate subgroup. If the conjugation by two different elements u and v takes the F to the same subgroup, i.e., $u^{-1}Fu = v^{-1}Fv$, then $Fuv^{-1} = uv^{-1}F$. This means that $uv^{-1} \in N(F)$ or, equivalently, $u \in N(F)v$. Conversely, the condition $u \in N(F)v$ implies $u^{-1}Fu = v^{-1}Fv$. Clearly, $|N(F)v| = |N(F)|$. Therefore the number of elements of G conjugation by which takes F to a given subgroup equals $|N(F)|$. Therefore the number of different subgroups conjugate to F is precisely $|N(F)|$ times less than $|G|$.)

We have $N(F) = F$.

(Indeed, it is easy to verify that $N(F)$ is a subgroup. By the assumption of the second case $N(F) \neq G$. Since $N(F) \supset F$, the maximality implies that $N(F) = F$.)

The three statements just proved imply that $\widehat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right)$.

Since $|G| > |F|$, we have $\widehat{F} < |G| - |Z|$.

By the assumption of the second case, $Z \neq F$. By Assertion 1 the center is a subgroup of F . Hence by the Lagrange theorem $|Z|$ divides $|F|$. Therefore $\widehat{F} \geq |G|/2$. QED

References

- [A] V. I. Arnold, Ordinary Differential Equations, The MIT Press (1978), ISBN 0-262-51018-9.
- [B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf
- [BKKSS] D. Baranov, A. Klyachko, K. Kohas, A. Skopenkov and M. Skopenkov, When are all groups of order n cyclic? <http://olympiads.mccme.ru/lktg/2011/6/index.htm>

КОГДА ЛЮБАЯ ГРУППА ИЗ N ЭЛЕМЕНТОВ ЦИКЛИЧЕСКАЯ? ⁵

В. Брагин, Ант. Клячко и А. Скопенков ⁶

Аннотация. Группой называется непустое семейство G перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки. Приводится простое доказательство ответа на следующий вопрос: *для каких n в любой группе из n элементов найдется перестановка $g \in G$, для которой $G = \{g, g^2, \dots, g^n\}$?* Для понимания доказательства необходимо знание основ теории чисел (включая теорему Ферма-Эйлера). Знаний по теории групп не требуется: небольшое количество понятий, необходимых для доказательства, приведены.

It startled the well informed by being a new and fantastic idea they had never encountered. It startled the ignorant by being an old and familiar idea they never thought to have seen revived.

G. K. Chesterton. The Man Who Knew Too Much.

СОДЕРЖАНИЕ

1. Введение: зачем, для кого и как устроена эта заметка	4
2. Как придумать	6
2.1. Постановка задачи	6
2.2. План §2	6
2.3. Почему вопрос интересен	6
2.4. Примеры групп	7
2.5. Докажем и применим теорему Лагранжа	8
2.6. Сопряжение	9
2.7. Максимальные подгруппы и центр	10
2.8. Указания, решения и ответы к некоторым задачам	10
3. Доказательство из Книги	13
3.1. Формулировка основного результата	13
3.2. Доказательство части «только тогда»	13
3.3. Доказательство части «тогда»	14

1. ВВЕДЕНИЕ: ЗАЧЕМ, ДЛЯ КОГО И КАК УСТРОЕНА ЭТА ЗАМЕТКА

Мы хотели бы привлечь внимание к теории групп широкого круга людей, включая учителей, руководителей кружков и школьников, серьезно интересующихся математикой и программированием. В этой теории есть доступные и интересные им результаты-жемчужины. Формулировки таких результатов кратки и используют лишь простейшие определения; доказательства красивы и похожи на решения сложных олимпиадных задач. К сожалению, в большей части существующей литературы эти жемчужины погребены под огромным количеством немотивированного материала. На примере исследования просто формулируемого вопроса мы покажем, как *появляются* некоторые основные понятия теории групп. Основные идеи представлены на «олимпиадных» примерах: на простейших частных случаях, свободных от технических деталей. ⁷

⁵ Благодарим М. Вялого, О. Иванова, П. Кожевникова, К. Кохася, А. Сгибнева, Б. Френкина и А. Шеня и за полезные замечания.

⁶Поддержан грантом фонда Саймонса. Инфо: www.mcsme.ru/~skopenko

⁷Это не только делает материал более доступным, но помогает тем, кто привык к абстрактному изложению, развить математический вкус. Благодаря этому они смогут разумно выбирать проблемы для исследования и ясно излагать собственные открытия, не скрывая ошибок (или известности полученного результата) за чрезмерным формализмом. К сожалению, такое (непреднамеренное) сокрытие иногда происходит с математиками, воспитанными на чрезмерно формальных курсах.

Эта заметка предназначена для того, кому понятна и интересна формулировка вопроса, сформулированного в аннотации. Мы приведем простое доказательство теоремы, отвечающей на этот вопрос. Оно не претендует на новизну, хотя мы не нашли такого доказательства в литературе.

Заметка может быть интересна читателю, не знакомому с основами абстрактной теории групп, но изучавшему перестановки и основы теории чисел. Например, по книгам [Al, KS, V] и [GDI, п. 1.7, 1.8 и 1.9]. Она может быть интересна и читателю, знакомому с этими основами, ибо ответ на сформулированный вопрос нетривиален. Такому читателю может оказаться достаточным прочесть §3.

Эта заметка не должна быть единственным и даже первым шагом в теорию групп. В миникурс «Рождение понятия группы» можно включить [GDI, п. 1.7, 1.8 и 1.9], [Z, глава 6], [Z, глава 3, разделы «Малая теорема Ферма», «Квадратичные вычеты» и «Первообразные корни»], [S08], [S15], данную заметку и другой материал.

Для понимания доказательства необходим опыт работы с перестановками и числами (включая теорему Ферма-Эйлера).⁸ Знаний по теории групп и опыта работы с определением абстрактной группы не требуется. Небольшое количество необходимых понятий вводятся (и могут быть освоены читателем) в процессе доказательства.

Конечно, читателю, не знакомому с основами теории групп, нужно будет потрудиться, чтобы самостоятельно доказывать тривиальные факты про эти понятия. Такие упражнения — важная часть изучения этих понятий. Выполнять их интереснее ради красивых результатов, формулировки которых ясны и доступны неспециалисту (в частности, не используют этих понятий), но в доказательствах которых эти понятия возникают. А не в процессе долгого немотивированного изучения теории. Эта заметка будет особенно интересна читателю, предпочитающему изучить доказательство красивого результата на несколько страниц, самостоятельно разбираясь в деталях, чем прочесть сотню страниц более легкого материала, не мотивированных таким результатом.

Опыт работы с абстрактными группами как раз появится при изучении данной заметки, хотя в ней формально не используется этого понятия. Читатель увидит, что помимо всех рассматриваемых объектов есть еще одно множество (на котором действуют перестановки). Станным образом оно так никогда и не выходит из тени. В результате естественно возникает общее понятие группы. Итак, *данная заметка посвящена мотивировке важного общего понятия группы* (здесь оно не используется, но его и основы соответствующей теории можно найти в [Al, K, KS]).⁹ Поэтому усилия по изучению заметки будут сполна вознаграждены тем, что вслед за великими математиками в процессе изучения конкретной задачи читатель увидит, как естественно возникает важное понятие. Надеюсь, это поможет ему совершить собственные настолько же полезные открытия (не обязательно в математике)!

Параграфы 2 и 3 формально независимы друг от друга.

⁸В частности, наше доказательство не привлекает явно понятия факторгруппы, в отличие от более традиционных доказательств, см., например, [B]. Также, мы не используем теорем Силова, хотя наш разбор второго случая похож на их доказательство.

⁹*Добавление от А. Скопенкова.* О необходимости мотивировок говорили классики математики [K], [P1, Глава 2 ‘Математические определения и преподавание’], [P2, стр. 455–475], [A, стр. 49, комментарий к задаче 5]; см. также [Z, Философски-методическое отступление]. Пр процитируем В.И. Арнольда: ‘...Обычно определяют группу как множество с двумя операциями, удовлетворяющими набору аксиом вроде $f(gh) = (fg)h$. Эти аксиомы автоматически выполняются для групп преобразований. В действительности эти аксиомы означают просто, что группа образована из некоторой группы преобразований забыванием преобразуемого множества. Такие аксиомы, наряду с другими немотивированными определениями, служат математикам главным образом для того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет.’

2. КАК ПРИДУМАТЬ

2.1. Постановка задачи. *Общие замечания к формулировкам задач.* Если условие задачи является утверждением, то в задаче требуется это утверждение доказать. Если некоторая задача не получается, то читайте дальше — соседние задачи могут оказаться подсказками.

1. Дано семейство G из 11 перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$). Тогда найдется перестановка $g \in G$, для которой $G = \{g, g^2, \dots, g^{11}\}$.

2. Верен ли аналог предыдущего утверждения для аналогичного семейства G из n перестановок при $n =$

(7) 2,3,4,5,6,7 (ответ может быть разным для разных значений n);

(8) 8; (9) 9; (10) 10; (12) 12; (15) 15; (21) 21; (1001) 1001?

Основной Вопрос. Дано семейство G из n перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки. Для каких n обязательно найдется перестановка $g \in G$, для которой $G = \{g, g^2, \dots, g^n\}$?

Группой называется непустое семейство G преобразований (т.е. перестановок) некоторого множества, замкнутое относительно композиции и взятия обратного преобразования (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$).¹⁰

Если в конечной группе G найдется перестановка g , из всех возможных степеней которой состоит G (т.е. $G = \{g, g^2, \dots, g^n, \dots\}$), то эта группа называется *циклической*. Примеры циклических и нециклических групп Вы привели при решении задачи 2.

3. Для любого n имеется циклическая группа из n элементов.

2.2. План §2. Пункт 2.3 нужен только для мотивировки, задачи 6.с и п. 3.2. Пункт 2.4 подводит читателя к построению примеров, необходимых для ответа на основной вопрос, т.е., к доказательству достаточности критерия, который мы нащупаем. (Немногие задачи в пунктах 2.5-2.7, использующие пункт 2.4, можно пропустить, ибо эти задачи не касаются основного вопроса.) А вот пункты 2.5-2.7 подводят читателя к необходимым условиям из этого критерия. Пункты 2.4-2.7 интересны и сам по себе, независимо от основного вопроса.

Пункты 2.3, 2.4 и 2.5-2.7 формально независимы друг от друга. В пунктах 2.4-2.7 используется следующее определение и обозначение.

Циклом $(a_1, a_2, \dots, a_n)$ называется перестановка множества, содержащего элементы $a_1, a_2, \dots, a_n$, которая переводит a_n в a_1 и a_i в a_{i+1} для любого $i < n$, а каждый из остальных элементов переводит в себя.

2.3. Почему вопрос интересен. Теорема о первообразном корне.¹¹ Число g , для которого $g^1, g^2, g^3, \dots, g^{\varphi(n)}$ есть все вычеты по модулю n , взаимно простые с n , существует тогда и только тогда, когда n есть либо 2, либо 4, либо степень нечетного простого, либо удвоенная степень нечетного простого.

Поставленный вопрос касается аналога теоремы о первообразном корне для перестановок. Впрочем, ситуация для перестановок не совсем аналогична: существуют циклическая и нециклическая группы с одинаковым числом элементов.

В процессе изучения этого вопроса мы в основном будем работать преобразованиями, забыв про множество, на котором они действуют. Такая ситуация часто встречается в математике и мотивирует следующее определение. Группы преобразований G и H множеств M и N называются *изоморфными*, если существует биекция $\varphi : G \rightarrow H$, для которой $\varphi(g_1) \circ \varphi(g_2) = \varphi(g_1 \circ g_2)$ при любых $g_1, g_2 \in G$. Важная тема в математике — классификация групп с точностью до изоморфизма. Ясно, что для любого n имеется циклическая

¹⁰Это определение равносильно обычному ввиду теоремы Кэли. Группы, определенные как здесь, обычно называют *группами преобразований*.

¹¹Операция умножения на множестве ненулевых вычетов по простому модулю имеет общее обобщение с операцией композиции перестановок. Но для доказательства результата заметки не нужно понимать этого.

группа из n элементов, ровно одна с точностью до изоморфизма. Поэтому вопрос о *циклическости любой группы из n элементов* равносильен вопросу о *единственности группы из n элементов с точностью до изоморфизма*.

2.4. Примеры групп. (1) Группа S_n *всех* перестановок n -элементного множества.

(2) Группа перестановок $\{\text{id} = (1)(2)(3)(4), (13)(24), (1234), (1432)\}$ множества из четырех элементов.

(3) Группа перестановок $\{(1, 2, 3, 4, 5, 6, 7, 8)^k\}$, $k = 1, 2, \dots, 8$, 8-элементного множества.

(4) Группа перестановок $\{(1, 2, 3)^k(4, 5, 6, 7, 8)^l\}$, $k = 1, 2, 3$, $l = 1, 2, 3, 4, 5$, 8-элементного множества.

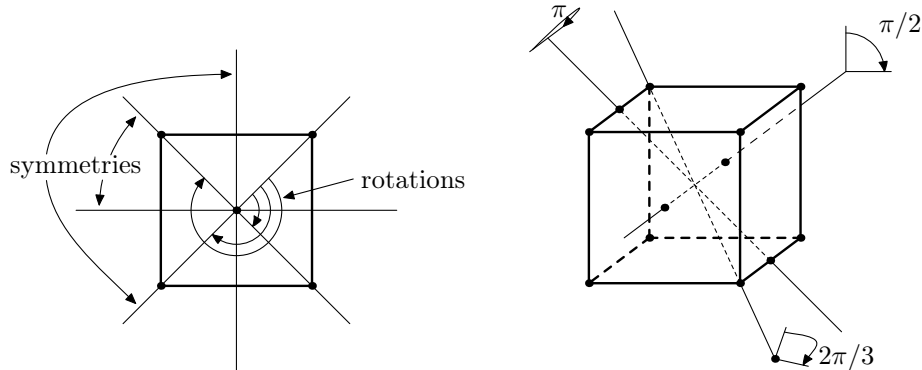


Рисунок: движения квадрата и куба

(5) Рассмотрим квадрат на плоскости и все движения плоскости, переводящие его в себя. Это тождественное преобразование, 3 поворота и 4 симметрии. Всего 8 преобразований. Возьмем группу из 8 перестановок множества вершин квадрата, происходящих при применении перечисленных восьми преобразований плоскости.

(6) Рассмотрим куб в пространстве и все вращения пространства (включая тождественное), переводящие его в себя.

(a) Возьмем группу из всех перестановок множества *вершин* куба, происходящих при применении таких вращений.

(b) Возьмем группу из всех перестановок множества *середин ребер* куба, происходящих при применении таких вращений.

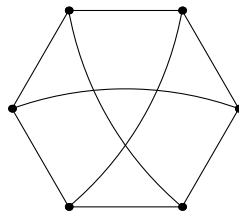


Рисунок: граф $K_{3,3}$

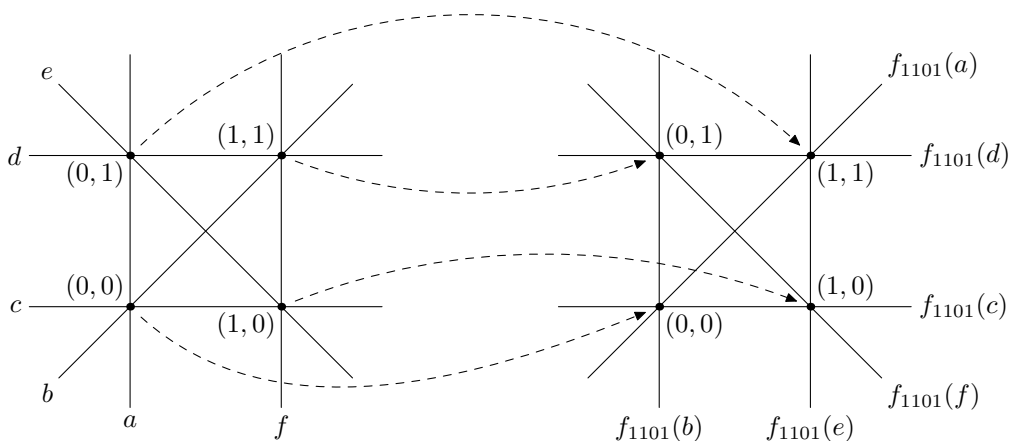


Рисунок: линейное преобразование $f_{1101} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$

(7) Группа всех перестановок 6-элементного множества, являющихся изоморфизмами графа $K_{3,3}$. (*Изоморфизм* графа G — такая перестановка множества его вершин, что для любых двух вершин эти вершины соединены ребром тогда и только тогда, когда их образы при перестановке соединены ребром.)

(8) Рассмотрим множество $\mathbb{Z}_2^2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$ упорядоченных пар вычетов по модулю 2. Для любых четырех вычетов a, b, c, d по модулю 2 рассмотрим отображение $f_{abcd} : \mathbb{Z}_2^2 \rightarrow \mathbb{Z}_2^2$, заданное формулой $f_{abcd}(x, y) = (ax + by, cx + dy)$. Среди всех таких отображений выберем взаимно-однозначные. Они образуют группу.

4. (a) Любая группа содержит тождественное преобразование.

(b) Множество из примера 8 действительно является группой.

5. Какие из приведенных примеров групп являются циклическими?

6. (a) Существует нециклическая группа из 21 элемента.

(b) Существует нециклическая группа из 55 элементов.

(c) Если p и q простые числа и $q - 1$ делится на p , то существует нециклическая группа из pq элементов.

2.5. Докажем и применим теорему Лагранжа.

7. Если количество перестановок в группе является простым числом, то эта группа циклическая.

Порядком $\text{ord } a = \text{ord}_G a$ перестановки a в группе G называется наименьшее целое положительное n , для которого $a^n = \text{id}$ (если такое n существует).

8. Пусть G — группа и $f, h \in G$.

(a) $f^n = \text{id}$ тогда и только тогда, когда n делится на $\text{ord } f$.

(b) Число $\text{ord } h$ делится на наименьшее $\text{ord}_f h$ из целых положительных n , для которых $h^n \in \langle f \rangle := \{f, f^2, f^3, \dots\}$.

9. (a) Найдите порядок каждой перестановки в группе S_4 .

(b) Любая перестановка конечной группы имеет (конечный) порядок.

(c) Если в конечной группе есть перестановка порядка 2, то число перестановок в группе четно.

(d) Если в конечной группе есть перестановка порядка 3, то число перестановок в группе делится на 3.

(e) *Теорема Лагранжа.* Число перестановок конечной группы делится на порядок любой ее перестановки.

(Это ‘некоммутативная версия’ теоремы Ферма-Эйлера, а также подсказка к задаче 7.)

10. (a) Если число n четное составное, то существует группа из n перестановок, не являющаяся циклической.

(b) Если число n делится на квадрат простого, то существует группа из n перестановок, не являющаяся циклической.

Группа G называется *коммутативной*, если $xy = yx$ для любых $x, y \in G$.

11. (b) Любая циклическая группа является коммутативной.

(c) Верно ли обратное?

12. (a) Любая коммутативная группа из 10 перестановок является циклической.

(b) То же для 21 перестановки.

(c) То же для 1001 перестановки.

(d) Для каких n любая коммутативная группа из n перестановок является циклической?

13. Может ли в коммутативной группе из 10 перестановок быть две различных перестановки порядка 2?

(Это подсказка к задаче 12.а.)

14. * Для каких n любая группа из n элементов является коммутативной? (Решение этой непростой задачи лучше отложить до разрешения основного вопроса.)

Подгруппой группы G называется подмножество группы G , также являющееся группой.

15. Теорема Лагранжа. Число перестановок в конечной группе делится на число перестановок в любой ее подгруппе.

(Это подсказка к задаче 13.)

16. Пусть G — группа из 15 элементов и $f, g \in G$ — элементы порядка 5.

- (a) Множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ пересекаются.
- (b) Множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ совпадают.
- (c) Один из элементов f, g является степенью другого.
- (d) В G есть элемент порядка 3.

17. Пусть G — группа из 15 элементов и $f, g \in G$ — элементы порядка 3.

- (a) Множества $\{f, f^2\}$ и $\{g, g^2\}$ либо не пересекаются, либо совпадают.
- (b) Если $\{f, f^2\} \neq \{g, g^2\}$, то $fg \neq gf$.

2.6. Сопряжение. Цикличность любой группы из 15 перестановок вытекает либо из задач 16.с, 19.б, 20.с и 22.с, либо из задач 20.с и 21.д (второй способ сложнее, но его удобно переносить на общий случай).

Перестановки $f, g \in G$ называются *сопряженными* в группе G , если $g = b^{-1}fb$ для некоторой перестановки $b \in G$.

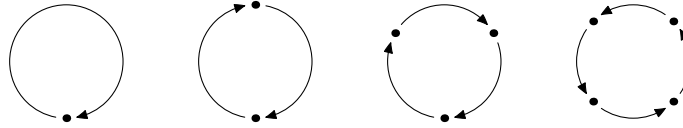


Рисунок: перестановка типа $\langle 1, 2, 3, 4 \rangle$

18. (a) Перестановка $(n_1 + \dots + n_k)$ -элементного множества, являющаяся композицией непересекающихся циклов порядков $n_1, \dots, n_k$, называется перестановкой типа $\langle n_1, \dots, n_k \rangle$.

Перестановки f и g сопряжены в S_n тогда и только тогда, когда они одного типа.

(b) Пусть a и x — произвольные перестановки n -элементного множества. Тогда

$$xax^{-1} = \begin{pmatrix} x(1) & x(2) & \dots & x(n) \\ x(a(1)) & x(a(2)) & \dots & x(a(n)) \end{pmatrix}.$$

Иными словами, циклическое разложение перестановки xax^{-1} получается из циклического разложения перестановки a заменой каждого элемента на его x -образ: если $a = \prod_{j=1}^q (i_{j1}, i_{j2}, \dots, i_{js_j})$, то $xax^{-1} = \prod_{j=1}^q (x(i_{j1}), x(i_{j2}), \dots, x(i_{js_j}))$.

(c) Вращения куба вокруг больших диагоналей сопряжены.

19. Пусть G — группа, $b, f \in G$ и k — целое положительное.

- (a) $(b^{-1}fb)^k = b^{-1}f^kb$.
- (b) Порядки сопряженных перестановок равны.
- (c) Если $b^{-1}fb = f^m$, то $b^{-1}f^kb = f^{km}$ и $b^{-k}fb^k = f^m$.

20. Пусть G — группа из 15 перестановок, $f \in G - \{e\}$ сопряжена только со своими степенями и $h \in G - \langle f \rangle$.

- (a) $h^{-1}fh = f$.
- (b) $\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$ подгруппа в G .
- (c) $G = \langle f \rangle h^{\text{ord } f}$.

Подгруппа группы G называется *собственной*, если она не совпадает ни с $\{\text{id}\}$, ни с G .

21. Пусть G — группа из 15 перестановок. Пусть любая перестановка сопряжена не только со своими степенями.

(a) Любые две различные собственные подгруппы пересекаются только по тождественной перестановке.

(b) С собственной подгруппой из s элементов сопряжено ровно $15/s$ различных подгрупп.

(c) Для числа $\widehat{F}$ нетождественных перестановок, сопряженных перестановкам данной собственной подгруппы, справедливы неравенства $7 < \widehat{F} < 14$.

(d) Получите противоречие.

Через $|X|$ обозначается число элементов в множестве X .

22. Для группы G и $f \in G$ обозначим через

- $c_G(f)$ число перестановок, сопряженных с f (вместе с самой f).
- $z_G(f)$ число перестановок, коммутирующих с f (вместе с самой f).

(a) Найдите $c_{S_3}(f)$ и $z_{S_3}(f)$ для каждого $f \in S_3$.

(b) $c_G(f)z_G(f) = |G|$.

(c) Если в группе из 15 перестановок нет перестановок порядка 5, то с каждой нетождественной перестановкой сопряжено ровно 4 других перестановки.

23. (Это подсказка к 21.b.) Для группы G и $f \in G$ обозначим через $n_G(f)$ число перестановок, сопряжение f с которыми переводит f в ее степень:

$$n_G(f) := |\{b \in G : fb = bf^k \text{ для некоторого } k\}|.$$

(a) Найдите $n_{S_3}(f)$ для каждого $f \in S_3$.

(b) $n_G(f) \geq \text{ord } f$.

(c) $n_G(f) = \text{ord } f$, если элемент f сопряжен не только со своими степенями и $|G| = 15$.

(d) Число различных подгрупп, сопряженных с $\langle f \rangle$, равно $|G|/n_G(f)$.

24. Если число перестановок в группе есть произведение pq простых чисел, $p < q$ и $q - 1$ не делится на p , то эта группа циклическая.

25. Если G — группа из 1001 перестановки и $f \in G - \{e\}$ сопряжен только со своими степенями, то G циклическая.

2.7. Максимальные подгруппы и центр.

26. Пусть G — группа из 1001 элемента, не являющаяся циклической.

(a) Каждый элемент содержится в максимальной по включению подгруппе, не совпадающей со всей G . Такие подгруппы будем сокращенно называть *максимальными подгруппами*.

(b) Каждая максимальная подгруппа является циклической.

Максимальные подгруппы аналогичны собственным подгруппам, на рассмотрении которых было основано доказательство для $n = 15$. Различные собственные подгруппы пересекались только по единичному элементу. Доказать аналогичное утверждение для максимальных подгрупп при $n = 1001$ не получается. Как же устроено пересечение максимальных подгрупп?

27. Назовем *коммутативизатором* группы G множество

$$Z = Z(G) := \{a \in G : ga = ag \text{ для любого } g \in G\}$$

тех элементов, которые коммутируют со всеми. (Мы надеемся, что использование слова *коммутативизатор* вместо общепринятого *центр* более удобно для начинающих.)

(a) Найдите $Z(S_n)$ для каждого $n = 2, 3, 4, \dots$

(b) Коммутативизатор группы является подгруппой.

28. Пусть G — группа из 1001 элемента, не являющаяся циклической. Пусть порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.

(a) Любая максимальная подгруппа содержит коммутативизатор.

(b) Пересечение двух максимальных подгрупп равно коммутативизатору.

(c) Число различных подгрупп, сопряженных с максимальной подгруппой из s элементов, равно $1001/s$.

(d) Для числа $\widehat{F}$ элементов, сопряженных элементам максимальной подгруппы F и не лежащих в коммутативизаторе, справедливы неравенства $500 < \widehat{F} \leq 1000 - |Z|$.

(e) Получите противоречие.

2.8. Указания, решения и ответы к некоторым задачам. 1. Аналогично решению нижеприведенной задачи 2.7 для $n = 3$.

2. (7) для $n = 3$. Пусть, напротив, имеется нециклическая группа G из трех перестановок. Обозначим через a нетождественную перестановку в ней. Если $a^2 \neq e$, то перестановки a, a^2, a^3 различны и группа циклическая. Если же $a^2 = e$, то рассмотрим перестановку $b \in G$, отличную от e и a . Тогда перестановка ab отлична от e, a, b . (Действительно, $ab \neq a$ и $ab \neq b$ очевидно. Если $ab = e$, то $b = a^2b = a$ — противоречие.) Противоречие.

(10) Рассмотрим правильный пятиугольник на плоскости. Рассмотрим все движения плоскости, переводящие его в себя. Это тождественное преобразование, 4 поворота и 5 симметрий. Всего 10 преобразований. Нужную группу образуют 10 перестановок множества вершин правильного пятиугольника, происходящих при применении перечисленных десяти преобразований плоскости. Эта группа нециклическая, поскольку для двух перестановок s и t , «пришедших из симметрий», $st \neq ts$. А если бы $s = g^k$ и $t = g^l$ для некоторой перестановки g , то $st = ts$.

Другое решение задачи 2.10. Оно более сложное, чем предыдущее, но зато может помочь Вам в решении задачи 6. Рассмотрим перестановки r и s 5-элементного множества вершин правильного 5-угольника, «соответствующие» повороту на $2\pi/5$ и симметрии. Тогда $r^5 = e = s^2$ и $sr = r^{-1}s$. Рассмотрим 10 перестановок $r^k s^l$, $k, l \in \mathbb{Z}$. Из соотношения $sr = r^{-1}s$ можно получить, что это множество является группой. (Именно в этом отличие приводимого решения от предыдущего — мы получили замкнутость относительно композиции и взятия обратного не из геометрических соображений, а из комбинаторных. Поэтому появилась возможность обобщать это доказательство на случаи, когда геометрической интерпретации не видно.) Из этого же соотношения вытекает, что эта группа не является циклической.

2. Ответы: верен для $n \in \{2, 3, 5, 7, 15, 1001\}$ и неверен иначе.

Доказательство верности для простых n аналогично приведенному для $n = 7$, а для $n = 15$ и $n = 1001$ намечено в задачах далее.

Доказательство верности для четных $n > 2$ аналогично приведенному для $n = 10$, а для $n = 21$ намечено в задачах далее.

3. Множество степеней цикла длины n .

4. $f \in G \Rightarrow f^{-1} \in G \Rightarrow ff^{-1} = e \in G$.

5. Ответ: группы из примеров (1) для $n = 2$, (3) и (4) — циклические, а из остальных примеров — нет.

6. (а) Искомая группа является группой некоторых перестановок 49-элементного множества $\mathbb{Z}_7^2$. Для описания группы представим его элементы как пары (x, y) вычетов по модулю 7. Для любых целых неотрицательных k, l определим преобразование

$$f_{k,l} : \mathbb{Z}_7^2 \rightarrow \mathbb{Z}_7^2 \quad \text{формулой} \quad f_{k,l}(x, y) := (2^k x, lx + y).$$

Проверьте, что

- таких преобразований ровно 21;
- они образуют группу;
- эта группа не является циклической (она даже не является абелевой).

Другое указание. См. другое решение задачи 2-10. Попробуйте сообразить, каким соотношениям должны удовлетворять перестановки r и s , чтобы множество $r^k s^l$, $k, l \in \mathbb{Z}$, образовывало бы нециклическую группу из 21 перестановки. А потом попробуйте придумать такие перестановки.

(b) Воспользуйтесь тем, что $2^5 = 33 - 1$. Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_{11}^2 \rightarrow \mathbb{Z}_{11}^2$ формулой $f_{k,l}(x, y) := (4^k x, lx + y)$.

(c) По теореме о первообразном корне существует элемент $a \in \mathbb{Z}_q$ порядка p . Для любых целых неотрицательных k, l определим преобразование $f_{k,l} : \mathbb{Z}_q^2 \rightarrow \mathbb{Z}_q^2$ формулой $f_{k,l}(x, y) := (a^k x, lx + y)$. Нетрудно проверить, что

- таких преобразований ровно pq ;
- они образуют группу;
- эта группа не является циклической (она даже не является абелевой).

8. (a) Поделите n на $\text{ord } f$ с остатком.

(b) Поделите $\text{ord } h$ на $\text{ord}_f h$ с остатком.

9. (d) Пусть a — элемент порядка 3. Выпишем все элементы группы. Теперь будем постепенно зачеркивать их следующим образом: на каждом шаге выбираем произвольным образом незачеркнутый элемент x и зачеркиваем три элемента x, xa, xa^2 .

При этом никакой элемент мы не зачеркнем больше одного раза.

(Действительно, предположим, что, например, зачеркиваемый элемент xa уже был зачеркнут. Тогда либо $xa = y$, либо $xa = ya$, либо $xa = ya^2$ для некоторого ранее выбранного элемента y . Но тогда либо $x = ya^2$, либо $x = y$, либо $x = ya$. Таким образом, элемент x уже был зачеркнут. Противоречие.)

Значит, на каждом шаге зачеркивается ровно три новых элемента.

В конце будут зачеркнуты все элементы. Значит, число элементов группы делится на 3.

(e) *Теорема Лагранжа.* Для $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, xf^{\text{ord } f - 1}\}$. По определению порядка указанные элементы различны. Значит, в этом множестве $\text{ord } f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\text{ord } f$.

12. (a) Обозначим через p порядок неединичного элемента f . Если $p = 10$, то группа циклическа. Пусть теперь $p < 10$. По теореме Лагранжа $p \in \{5, 2\}$. Если есть элемент g порядка $10/p$, то $G = \{fg, (fg)^2, \dots, (fg)^{10}\}$. Иначе есть элемент $g \notin \{f, f^2, \dots, f^p\}$ порядка p . Тогда $\{f^k g^l\}_{k,l \in \mathbb{Z}}$ есть подгруппа из p^2 перестановок. Противоречие с теоремой Лагранжа (задача 15.b).

13. (a) Если f, g — такие элементы, то $\{e, f, g, fg\}$ — подгруппа из 4 перестановок. Противоречие с теоремой Лагранжа (задача 15.b).

14. Все группы порядка n коммутативны тогда и только тогда, когда в разложении $n = p_1^{k_1} \dots p_l^{k_l}$ числа n на простые сомножители $k_i < 3$ и p_i не делит $p_j^{k_j} - 1$.

Доказывается это примерно так же, как и для циклических групп, но в случае 1 надо воспользоваться тем, что любая конечная коммутативная группа раскладывается в прямую сумму циклических подгрупп.

16. (a) Рассмотрим 25 элементов $f^k g^l$ для $1 \leq k, l \leq 5$. Так как в группе всего 15 элементов, то существуют $1 \leq k, l, m, n \leq 5$ такие, что $(k, l) \neq (m, n)$ и $f^k g^l = f^m g^n$. Домножая на f^{-m} слева и на g^{-l} справа, получаем $f^{k-m} = g^{n-l}$. Так как f и g — элементы порядка 5, то множества $\{f, f^2, f^3, f^4\}$ и $\{g, g^2, g^3, g^4\}$ пересекаются.

(b) По (a) эти множества пересекаются. Тогда существуют такие натуральные числа $1 \leq k, l \leq 4$, что $f^k = g^l$. Так как $\text{НОД}(k, 5) = 1$, то существует такое целое число m , что $5 \mid km - 1$. Тогда $f = f^{km} = (f^k)^m = (g^l)^m = g^{lm}$. Отсюда следует, что эти множества совпадают.

(c) Следует из (b).

(d) Следуют из (c). (Пункт (d) не нужен для решения основной задачи.)

17. (a) Аналогично 16.b.

(b) Иначе есть подгруппа из 9 элементов, что противоречит теореме Лагранжа.

20. (a) Используйте задачу 8.ab.

(b) Следует из (a).

(c) Докажите, что $\text{ord}(fh^{\text{ord } f})$ делится на q и на $\text{ord } f$.

18. Перенумеруем элементы множества так, чтобы f перешла в g . Эта перенумерация задает требуемую перестановку b .

19. (a,d) Утверждения доказываются индукцией по k .

21. (d) Ввиду (c) $\widehat{F} = (s-1)15/s = 15(1 - 1/s)$.

22. (b) Для каждого $b \in G$ проведите стрелку от f к $b^{-1}fb$. Докажите, что если от f к g есть хотя бы одна стрелка, то общее количество стрелок от f к g равно общему количеству стрелок от f к f .

(с) Из 17.b следует, что с f коммутируют только элементы e, f, f^2 . Теперь по (а) $c_G(f) = 15/3 = 5$.

23. (b) Ответ: $n(e) = n((ijk)) = 6$.

(с) Аналогично 22.

24. Аналогично разобранному случаю $p = 3, q = 5$.

25. Аналогично 20.

28. (d) Ввиду (с) $\widehat{F} = (|F| - |Z|)1001/|F| = 1001(1 - |Z|/|F|)$.

3. ДОКАЗАТЕЛЬСТВО ИЗ КНИГИ

3.1. Формулировка основного результата. Группой называется непустое семейство G перестановок некоторого множества, замкнутое относительно композиции и взятия обратной перестановки (т.е. если $f, g \in G$, то $f \circ g \in G$ и $f^{-1} \in G$).

Теорема (фольклор). Для любой группы из n перестановок найдется перестановка $g \in G$, для которой $G = \{g, g^2, \dots, g^n\}$, тогда и только тогда, когда в разложении числа n на простые сомножители $n = p_1 \dots p_t$

(*) все p_i различны и

(**) p_i не делит $p_j - 1$ ни для каких i и j .

Заметим, что условие ‘(*) и (**)’ равносильно взаимной простоте n с $\phi(n)$. Здесь $\phi(n)$ — количество целых чисел от 1 до n , взаимно простых с n (функция Эйлера).

Интересные частные случаи приведены в задачах 7, 24 и 6.с. Как его придумать, видно из §2.

Если в конечной группе G найдется перестановка g , из всех возможных степеней которой состоит G (т.е. $G = \{g, g^2, \dots, g^n, \dots\}$), то эта группа называется *циклической*.

3.2. Доказательство части «только тогда». Обозначим $\mathbb{Z}/k := \{(1, 2, \dots, k)^i \mid i = 1, 2, \dots, k\}$.

Несвязное объединение множеств M и N определяется как $M \sqcup N := M \times \{0\} \cup N \times \{1\}$. Если g и h — преобразования множеств M и N , то преобразование $g \sqcup h$ несвязного объединения $M \sqcup N$ определяется формулой $(g \sqcup h)(x) := \begin{cases} g(x) & x \in M \times \{0\} \subset M \sqcup N \\ h(x) & x \in N \times \{1\} \subset M \sqcup N \end{cases}$. Для групп G и H , состоящих из преобразований множеств M и N , определим

$$G \times H := \{g \sqcup h : M \sqcup N \rightarrow M \sqcup N \mid g \in G, h \in H\}.$$

Если нарушается вышеприведенное условие (*), например, $p_1 = p_2 = p$, то в качестве нециклической группы из n элементов можно взять группу $\mathbb{Z}/p \times \mathbb{Z}/\frac{n}{p}$.¹²

Обозначим через $\mathbb{Z}_k$ множество вычетов по модулю k с операциями суммы и произведения, известными из теории чисел. (Не путайте с группой $\mathbb{Z}/k$, определенной выше!) Если нарушается вышеприведенное условие (**), например, p_1 делит $p_2 - 1$, то *существует* вычет $a \in \mathbb{Z}_{p_2}$, для которого степени $a, a^2, \dots, a^{p_1} = 1$ различны. Это следует из теоремы о первообразном корне (сформулированной в §1).

Обозначим через G_{p_1, p_2} группу преобразований $f_{k, l} : \mathbb{Z}_{p_2}^2 \rightarrow \mathbb{Z}_{p_2}^2$, заданных формулой $f_{k, l}(x, y) := (a^k x, lx + y)$ для $k \in \mathbb{Z}_{p_1}$ и $l \in \mathbb{Z}_{p_2}$.¹³ Тогда в качестве нециклической (даже некоммутативной) группы из n элементов можно взять группу $G_{p_1, p_2} \times \mathbb{Z}/\frac{n}{p_1 p_2}$.¹⁴ QED

¹²Т.е. группу $\left\{ (1, 2, \dots, p)^i (p+1, p+2, \dots, p+\frac{n}{p})^k \mid i = 1, \dots, p, k = 1, \dots, \frac{n}{p} \right\}$.

¹³ Научно говоря, $G_{p_1, p_2} = \left\{ \begin{pmatrix} a^k & l \\ 0 & 1 \end{pmatrix} \in \mathbb{Z}_{p_2}^{2 \times 2} \mid k \in \mathbb{Z}_{p_1}, l \in \mathbb{Z}_{p_2} \right\}$.

¹⁴Т.е. группу $\left\{ f \circ (1, 2, \dots, \frac{n}{p_1 p_2})^j \mid f \in G_{p_1, p_2}, j = 1, 2, \dots, \frac{n}{p_1 p_2} \right\}$.

3.3. Доказательство части «тогда». Через $|X|$ обозначается число элементов в множестве X . Обозначим данную группу через G . Используем индукцию по числу простых сомножителей в $n = |G|$. Если сомножитель один, то часть «тогда» вытекает из следующего частного случая теоремы Лагранжа.

Порядком $\text{ord } a$ элемента a группы с единичным элементом e называется наименьшее целое положительное n , для которого $a^n = e$. Если группа конечна, то ясно, что такое n существует.

Теорема Лагранжа (частный случай). Число элементов конечной группы делится на порядок любого ее элемента.

*Доказательство.*¹⁵ Обозначим данную группу через G . Для любого $x \in G$ рассмотрим множество $\{x, xf, xf^2, \dots, xf^{\text{ord } f-1}\}$. Из определения порядка вытекает, что указанные элементы различны. Значит, в этом множестве $\text{ord } f$ элементов. Если $xf^k = yf^l$, то $y = xf^{k-l}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на $\text{ord } f$. QED

Пусть теперь простых сомножителей в $n = |G|$ больше одного. Нам понадобится следующая общая версия теоремы Лагранжа.

Подгруппой группы называется подмножество этой группы, которое само по себе является группой.

Теорема Лагранжа. Число элементов конечной группы делится на число элементов любой ее подгруппы.

Доказательство. Обозначим данную группу через G , а ее подгруппу через $\{h_1, \dots, h_m\}$. Для любого $x \in G$ рассмотрим множество $\{xh_1, xh_2, \dots, xh_m\}$. В этом множестве m элементов. Если $xh_k = yh_l$, то $y = xh_k h_l^{-1}$. Поэтому для разных x эти множества либо не пересекаются, либо совпадают. Значит, $|G|$ делится на m . QED

Максимальной подгруппой назовем максимальную по включению подгруппу, не совпадающую со всей группой и содержащую более одного элемента. По предположению индукции и теореме Лагранжа каждая максимальная подгруппа является циклической.

Для элемента f группы G обозначим через $\langle f \rangle \subset G$ множество всех его степеней (в т.ч. нулевой и отрицательных). Элемент f называется **порождающим** для (циклической) подгруппы $\langle f \rangle$.

Предположим противное, т.е. что группа G не является циклической. Тогда каждый элемент f содержится в некоторой максимальной подгруппе (в максимальной по включению подгруппе, содержащей $\langle f \rangle$).

Элементы f и g группы G называются **сопряженными** в G , если $g = b^{-1}fb$ для некоторого $b \in G$.

Первый случай: порождающий элемент f некоторой максимальной подгруппы сопряжен только с некоторыми своими степенями. Возьмем $h \in G - \langle f \rangle$. Обозначим через q наименьшее из целых положительных n , для которых $h^n \in \langle f \rangle$. Такое q существует, поскольку $h^{\text{ord } h} \in \langle f \rangle$.

Доказательство того, что $|G|$ делится на q . Поделим с остатком $\text{ord } h$ на q : $\text{ord } h = qt + r$. Тогда $h^r = h^{\text{ord } h - qt} \in \langle f \rangle$ и $0 \leq r < q$. Поэтому ввиду минимальности q имеем $r = 0$. Т.е. $\text{ord } h$ делится на q . Значит, по теореме Лагранжа $|G|$ делится на q . □

Доказательство того, что $hf = fh$. По условию первого случая $h^{-1}fh = f^k$ для некоторого $k \in \mathbb{Z}$. Значит, $f = h^{-q}fh^q = f^{k^q}$ (последнее равенство верно для произвольного q и доказывается индукцией по q). Поэтому $k^q \equiv 1 \pmod{\text{ord } f}$. Следовательно, k и $\text{ord } f$ взаимно просты. По теореме Лагранжа и условиям (*) и (**), $|G|$ и $\varphi(\text{ord } f)$ взаимно просты. Так как $|G|$ делится на q , то q и $\varphi(\text{ord } f)$ взаимно просты. Следовательно, найдутся целые x и y , для которых $qx + \varphi(\text{ord } f)y = 1$. Значит, $k \equiv k^{qx + \varphi(\text{ord } f)y} \equiv 1 \pmod{\text{ord } f}$. Поэтому $fh = hf$. QED

¹⁵Более подробно это доказательство (и его обобщение, см. ниже) изложено в [KS, стр. 64].

Завершение разбора первого случая. Так как $fh = hf$, то в G есть подгруппа

$$\{f^i h^j \mid 1 \leq i \leq \text{ord } f, 1 \leq j \leq q\}$$

из $q \text{ ord } f$ элементов. Значит, по условию (*) и теореме Лагранжа $\text{ord } f$ и q взаимно просты. Обозначим $g := fh^{\text{ord } f}$. Так как $g^j = f^j h^{j \text{ ord } f}$ для любого j , то $\text{ord } g$ делится на q и на $\text{ord } f$. Поэтому $\text{ord } g = q \text{ ord } f$. Так как подгруппа $\langle f \rangle$ максимальна, то $\langle g \rangle = G$. Значит, G циклическая. Противоречие. QED

Второй случай: порождающий элемент любой максимальной подгруппы сопряжен не только со своими степенями.¹⁶

Произведением двух подмножеств X и Y группы G называют множество всевозможных произведений xy , где $x \in X$ и $y \in Y$. Если одно из этих подмножеств состоит только из одного элемента, например, $Y = \{y\}$, то для краткости пишут Xy вместо $X\{y\}$.

Центром группы G называют

$$Z = Z(G) := \{a \in G : ga = ag \text{ для любого } g \in G\},$$

т.е. множество тех элементов, которые коммутируют со всеми.

(1) Любая максимальная подгруппа содержит центр.

Доказательство утверждения (1). Пусть, напротив, максимальная подгруппа F не содержит Z . Тогда FZ — большая подгруппа, чем F . Ввиду максимальной подгруппы F имеем $FZ = G$. Значит, G коммутативна, т.е. $G = Z(G)$. Поэтому порождающий элемент любой максимальной подгруппы сопряжен только с собой. Это противоречит условию второго случая. QED

(2) Пересечение двух максимальных подгрупп равно центру.

Доказательство утверждения (2). Неединичный элемент в пересечении коммутирует с элементами обеих подгрупп. Значит, он коммутирует с любым произведением нескольких сомножителей, каждый из которых лежит в одной из наших подгрупп. Множество таких произведений является подгруппой, содержащей обе максимальные подгруппы. В силу максимальной наших подгрупп эта подгруппа совпадает со всей группой. Значит, пересечение содержится в центре.

Из (1) вытекает обратное включение. QED

Завершение разбора второго случая: подсчет. Напомним, что любой элемент группы содержится в некоторой максимальной подгруппе. Ввиду (2) для любого нецентрального элемента такая подгруппа единственна. Поэтому вся группа разбивается на центр и несвязное объединение дополнений максимальных подгрупп до центра. Количества элементов в таких дополнениях одинаковы для сопряженных максимальных подгрупп. (Подмножества $F, F' \subset G$ называются *сопряженными*, если $g^{-1}Fg = F'$ для некоторого $g \in G$.) Обозначим через $\hat{F}$ общее количество нецентральных элементов во всех максимальных подгруппах, сопряженных с максимальной подгруппой F . Обозначим через $F_1, \dots, F_s$ наибольший набор попарно несопряженных максимальных подгрупп. Тогда

$$|G| = |Z| + \sum_{i=1}^s \hat{F}_i.$$

Ввиду левого неравенства в следующем утверждении число слагаемых не превосходит единицы, а ввиду правого — одного слагаемого тоже быть не может. QED

(3) $|G|/2 \leq \hat{F} < |G| - |Z|$.

Доказательство утверждения (3). Подгруппа, сопряженная к максимальной, также максимальна.

(Действительно, если $g^{-1}Fg \subset F' \subset G$, то $F \subset gF'g^{-1} \subset G$.)

¹⁶Вот план немного другого разбора второго случая, предложенный М.Н. Вялым. Сначала вводим множество $N(F)$ из доказательства утверждения (3) ниже. Доказываем, что $N(F) = F$, см. там же. Тогда (1) очевидно, так $Z(G) \subset N(F)$. Далее делаем то же, что и в приводимом разборе.

Рассмотрим множество

$$N(F) := \{a \in G : Fa = aF\}.$$

Тогда число различных подгрупп, сопряженных с F (включая F), равно $|G|/|N(F)|$.¹⁷

(Действительно, сопряжение каждым элементом группы G переводит подгруппу F в одну из сопряженных подгрупп. Если сопряжение двумя разными элементами u, v группы G переводит подгруппу F в одну и ту же подгруппу, т.е. $u^{-1}Fu = v^{-1}Fv$, то $(uv^{-1})^{-1}Fuv^{-1} = F$. Это означает, что $uv^{-1} \in N(F)$ или, что то же самое, $u \in N(F)v$. Обратно, условие $u \in N(F)v$ влечет $u^{-1}Fu = v^{-1}Fv$. Ясно, что $|N(F)v| = |N(F)|$. Поэтому число элементов в G , сопряжение с которыми переводит подгруппу F в данную фиксированную сопряженную подгруппу, равно $|N(F)|$. Значит, число подгрупп, сопряженных к F , равно в $|N(F)|$ раз меньше, чем элементов группы G .)

Имеем $N(F) = F$.

(Действительно, $N(F)$ является подгруппой. По условию второго случая $N(F) \neq G$. Так как $N(F) \supset F$, то в силу максимальности $N(F) = F$.)

$$\widehat{F} = (|F| - |Z|) \frac{|G|}{|F|} = |G| \left(1 - \frac{|Z|}{|F|}\right).$$

Так как $|G| > |F|$, то $\widehat{F} < |G| - |Z|$.

По (1) центр является подгруппой в F . Значит, по теореме Лагранжа $|Z|$ делит $|F|$. По условию второго случая $Z \neq F$. Следовательно, $|Z| \leq |F|/2$. Поэтому $\widehat{F} \geq |G|/2$. QED

Литература

- [A] В.И. Арнольд, Обыкновенные дифференциальные уравнения, М, Наука, 1984.
- [Al] В.Б. Алексеев, Теорема Абеля. М: Наука, 1976.
- [B] Ken Brown, Mathematics 4340, When are all groups of order n cyclic? Cornell University, March 2009, http://www.cornell.edu/~kbrown/4340/cyclic_only_orders.pdf
- [BKKSS] Д. Баранов, А. Клячко, К. Кохась, А. Скопенков и М. Скопенков, Когда любая группа из n элементов циклическая? <http://olympiads.mccme.ru/lktg/2011/6/index.htm>
- [GDI] А.А. Глибичук, А.Б. Дайняк, Д.Г. Ильинский, А.Б. Купавский, А.М. Райгородский, А.Б. Скопенков, А.А. Чернов, Элементы дискретной математики в задачах, Изд-во МЦНМО, 2015.
- [K] Ф. Клейн, Элементарная математика с точки зрения высшей.
- [KS] Л.А. Калужнин и В.И. Суцанский, Преобразования и перестановки, М.: Наука, 1985.
- [P1] А. Пуанкаре, О науке, М.: Наука, 1990.
- [P2] А. Пуанкаре 'Наука и метод',
- [S08] А. Скопенков, Еще несколько доказательств из Книги: разрешимость и неразрешимость уравнений в радикалах, <http://arxiv.org/abs/0804.4357>
- [S15] А. Skopenkov, A short elementary proof of the Ruffini-Abel Theorem <http://arxiv.org/abs/1508.03317>
- [V] Виноградов И.М., Основы теории чисел. М.; Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003.
- [Z] Математика в задачах. Сборник материалов московских выездных математических школ. Под редакцией А. Заславского, Д. Пермякова, А. Скопенкова, М. Скопенкова и А. Шаповалова. Москва, МЦНМО, 2009. <http://www.mccme.ru/circles/oim/mvz.pdf>

¹⁷Это вытекает из теоремы о длине орбиты для действия группы на себе сопряжениями. Те, кому это доказательство непонятно, могут прочитать следующий абзац.