Обобщение основной теоремы арифметики

Буланкина Вера, Зайцев Тимофей, Фролов Иван,
Петухов Алексей, Салимов Руслан*

Введение

Цель этого проекта — обобщить основную теорему арифметики с целых чисел на какие-то более "продвинутые" объекты. Для решения задач проекта можно (пожалуй, даже рекомендовано) объединяться в команды с другими участниками.

Основная теорема арифметики (Теорема 1 ниже, см. также её обобщения — Теоремы 4, 5, 7) полезна при решении различных уравнений в целых числах. Как мы увидим уже в первой части — примерами могут служить Рождественская теорема Ферма (Теорема 2) и Великая теорема Ферма (Теорема 3) для $n = 3$. Вы можете попробовать доказать их, не читая дальнейшего текста, но не тратьте на это много времени. Возвращайтесь к ним по мере чтения проекта. Также мы увидим, что однозначность разложения на простые множители не обязательно сохраняется для рассматриваемых нами аналогов целых чисел.

Во второй части проекта будет обсуждена версия основной теоремы арифметики, работающая для чисел вида $a + b\sqrt{d}$, где d — фиксированное целое число, a, b — любые целые (для этого нам потребуется понятие идеала). Эти знания мы применим к решению уравнений в целых числах.

В третьей части мы сформулируем более общее утверждение для произвольных алгебраических чисел.

Завершающая часть проекта будет посвящена связи общей теории с Великой теоремой Ферма. Вам предлагается доказать так называемый первый случай Великой теоремы Ферма для регулярных простых чисел. Используя похожие идеи можно доказать, что теорему Ферма и во втором случае для всех n, делящихся на регулярные простые числа p; все простые числа, меньшие 37 — регулярны, см. книги Дж. Милна и М. Постникова. Общее доказательство, придуманное Эндрю Вайлсом, использует существенно другие методы и идеи.

При подготовке проекта мы использовали книги К. Айэрланда и М. Роузена, Дж. Милна, М. Постникова, заметки К. Конрада и википедию. Мы также добавили несколько ссылок [SS, Go, ZSS], которые могут оказаться интересны читателю, желающему лучше познакомиться с этой темой.

Теорема 1. Основная теорема арифметики.
Каждое натуральное число $n > 1$ можно представить в виде $n = p_1 \cdot \ldots \cdot p_k$, где $p_1, \ldots, p_k$ — простые числа, причём такое представление единственно с точностью до порядка следования сомножителей.

Теорема 2. Рождественская теорема Ферма.
Натуральное число n представляется в виде суммы двух квадратов тогда и только тогда, когда все его простые делители вида $4k + 3$ входят в n в четной степени.

Теорема 3. Великая теорема Ферма.
Уравнение $x^n + y^n = z^n$ не имеет решений в натуральных числах при $n > 2$.

*Мы также хотим поблагодарить Михаила Скопенкова, Илью Богданова, Кейта Конрада за существенную помощь в подготовке проекта.

1 Гауссовы числа

Мы хотели обсудить в этой части проекта гауссовы числа — обобщение целых чисел, использующее $\sqrt{-1}$. Если у Вас не получится решить какие-то из задач про гауссовы числа, то попробуйте порешать задачи из других частей проекта и вернуться сюда позднее.

Определение. *Гауссовыми числами* называется множество комплексных чисел вида $a + bi$, где $a, b \in \mathbb{Z}$, $i = \sqrt{-1}$. Будем обозначать множество гауссовых чисел $\mathbb{Z}[i]$.

Задача 1. Докажите, что сумма и произведение любых двух гауссовых чисел — гауссово число.

Для решения следующей задачи потребуется дать более точную формулировку основной теоремы арифметики. Ведь, строго говоря, в старой формулировке она неверна уже для целых чисел: $2 \cdot 3 = 6 = (-2) \cdot (-3)$. Чтобы получить новую формулировку, нам потребуется новое понятие.

Определение. *Делители единицы в* $\mathbb{Z}[i]$ — такие гауссовы числа a, что существует гауссово число b такое, что $ab = 1$. Аналогично определяются делители единицы в $\mathbb{Z}$.

Упражнение 1. Докажите, что в целых числах делители единицы это 1 и -1, а в гауссовых добавляются еще i и $-i$.

Определение. Гауссово число называется *простым*, если в любом его разбиении на 2 множителя ровно один является делителем единицы.

Определение. Два разложения на простые множители называются *одинаковыми*, если в них одинаковое число множителей, и их можно так переставить, чтобы отношение соответствующих простых множителей было делителем единицы. Например, $7 \cdot 3, (-3) \cdot (-7)$ и $(-7i) \cdot (3i)$ — это одинаковые разложения числа 21 в гауссовых числах.

Наша ближайшая цель доказать и научиться применять идущую ниже теорему.

Теорема 4. Основная теорема арифметики для гауссовых чисел.
Любые два разложения гауссова числа на простые множители одинаковы.

Задача 2*. Определите деление с остатком для $\mathbb{Z}[i]$. Используя это, докажите Теорему 4. Подсказка: используйте модуль комплексного числа и графическую (гауссову) интерпретацию комплесных чисел.

Задача 3. Решите в целых числах уравнение $x^2 + 1 = y^n$.

Задача 4. а) Пусть $p \in \mathbb{Z}$ – простое число. Докажите, что число p является простым гауссовым числом тогда и только тогда, когда $p + 1$ делится на 4.

б) Если $n, m \in \mathbb{Z}$ представляются в виде $a^2 + b^2$, где a и $b \in \mathbb{Z}$, то mn представляется в виде суммы двух квадратов.

в) Докажите Рождественскую теорему Ферма (Теорему 2).

Задача 5. Как по разложению целого числа на (гауссовы) простые множители понять, сколькими способами оно раскладывается в сумму двух квадратов?

Числа Эйзенштейна

В этой главе мы постараемся помочь участникам решить следующую задачу.

Задача 6*. Докажите Теорему 3 для $n = 3$, используя формулу

$$x^3 + y^3 = (x + y)\left(x + \frac{-1 + \sqrt{-3}}{2}y\right)\left(x + \frac{-1 - \sqrt{-3}}{2}y\right).$$

Для этого мы введём несколько новых определений и рассмотрим несколько вспомогательных задач. Обозначим через ξ какой-то комплексный корень третьей степени из 1, не равный 1.

Упражнение 2. Докажите, что $\xi = \frac{-1\pm\sqrt{-3}}{2}$.

Положим $\mathbb{Z}[\xi] := \{a + b\xi : \ a, b \in \mathbb{Z}\}$.

Определение. Число $a \in \mathbb{Z}[\xi]$ *делится* на $b \in \mathbb{Z}[\xi]$ тогда и только тогда, когда существует такое $c \in \mathbb{Z}[\xi]$, что $a = bc$.

Делители единицы в $\mathbb{Z}[\xi]$ определяются аналогично делителям единицы в $\mathbb{Z}$ и $\mathbb{Z}[i]$.

Определение. Число $\alpha \in \mathbb{Z}[\xi]$ *составное*, если $\alpha = \beta\gamma$, где β и $\gamma \in \mathbb{Z}[\xi]$ не являются делителями единицы. Число $\alpha \in \mathbb{Z}[\xi]$ называется *простым*, если α не составное и не делитель единицы.

Задача 7. Определите деление с остатком для $\mathbb{Z}[\xi]$. Используя его, сформулируйте и докажите, основную теорему арифметики для $\mathbb{Z}[\xi]$.

Задача 8. Найдите все делители единицы в $\mathbb{Z}[\xi]$.

Квадратичные расширения

В этой секции мы введём общие квадратичные расширения, как обобщения гауссовых чисел и чисел Эйзенштейна.

Определение. Для произвольного набора комплексных чисел $a_1, ..., a_n$ обозначим через $\mathbb{Z}[a_1, ..., a_n]$ множество всех комплексных чисел, получаемых из целых чисел ($\mathbb{Z}$), а также $a_1, ..., a_n$ сложением, вычитанием и умножением.

Аналогично определяется $\mathbb{Q}[a_1, ..., a_n]$. Мы рассматриваем такие множества $\mathbb{Z}[a_1, ..., a_n]$ как аналоги целых чисел (их элементы можно складывать, умножать и вычитать).

Фиксируем целое число $d \neq 1$, не делящееся на квадраты простых чисел.

Комментарий. Два важных примера: $d = -3$ и $d = 2$. Может оказаться полезным продумать и проанализировать все определения этой секции сначала для этих двух примеров, а потом для общего случая.

Упражнение 3. а) Докажите, что

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\} \text{ и } \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

б) Докажите, что если $a, b \in \mathbb{Q}[\sqrt{d}]$ и $b \neq 0$, то $\frac{a}{b} \in \mathbb{Q}[\sqrt{d}]$.

Определение. *Целыми числами в* $\mathbb{Q}[\sqrt{d}]$ называются $\alpha \in \mathbb{Q}[\sqrt{d}]$, которые являются корнями уравнений вида $x^2 + px + q$, где $p, q \in \mathbb{Z}$.

Упражнение 4. Является ли ξ целым в $\mathbb{Q}[\sqrt{-3}]$? Является ли $\frac{1+i}{2}$ целым в $\mathbb{Q}[i]$?

Положим $\omega = \sqrt{d}$ если $d \equiv 2, 3 \bmod 4$, и $\omega = \frac{\sqrt{d}+1}{2}$ если $d \equiv 1 \bmod 4$.

Для $\mathbb{Z}[\sqrt{d}]$ единственность разложения на простые множители не всегда имеет место, но, как мы надеемся, вы сможете доказать некоторую её модификацию. Для каждого числа $\alpha = a + b\sqrt{d}$, где $a, b \in \mathbb{Q}$, определим сопряженное число $\bar{\alpha} = a - b\sqrt{d}$, норму $N(\alpha) = \alpha\bar{\alpha}$ и след $\mathrm{Tr}(\alpha) = \alpha + \bar{\alpha}$.

Упражнение 5. Докажите, что $\overline{a+b} = \bar{a} + \bar{b}$ и $\overline{ab} = \bar{a}\bar{b}$.

Упражнение 6. а) Докажите, что $\alpha \in \mathbb{Q}[\sqrt{d}]$ — корень многочлена $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha)$.

б) Докажите что $\alpha \in \mathbb{Q}[\sqrt{d}]$ цело тогда и только тогда когда $N(\alpha) \in \mathbb{Z}$ и $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.

Задача 9. Докажите, что целые числа в $\mathbb{Q}[\sqrt{d}]$ совпадают с $\mathbb{Z}[\omega]$.

Делители единицы в $\mathbb{Z}[\xi]$ определяются аналогично делителям единицы в $\mathbb{Z}$ и $\mathbb{Z}[i]$.

Упражнение 7. Докажите, что для $\gamma \in \mathbb{Z}[\omega]$ выполнено $N(\gamma) = \pm 1$ тогда и только тогда, когда γ — делитель единицы.

Определение. Число $a \in \mathbb{Z}[\omega]$ *делится* на $b \in \mathbb{Z}[\omega]$ тогда и только тогда, когда существует такое $c \in \mathbb{Z}[\omega]$, что $a = bc$.

Определение. Число $\alpha \in \mathbb{Z}[\omega]$ *составное*, если $\alpha = \beta\gamma$, где β и $\gamma \in \mathbb{Z}[\omega]$ не являются делителями единицы. Число $\alpha \in \mathbb{Z}[\omega]$ называется *простым*, если α не составное и не делитель единицы.

Упражнение 8. Докажите, что если для числа $\gamma \in \mathbb{Z}[\omega]$ число $|N(\gamma)| \in \mathbb{Z}$ просто, то γ просто. Докажите что обратное утверждение неверно в $\mathbb{Z}[\sqrt{3}]$.

Упражнение 9. Докажите, что если $\gamma \in \mathbb{Z}[\omega]\backslash 0$ не делитель единицы, то γ равно произведению каких-то простых элементов $\mathbb{Z}[\omega]$.

Задача 10. Проверьте, что все множители в разложении

$$15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$$

простые.

Задача 11. Определите деление с остатком для а) $\mathbb{Z}[\sqrt{-2}]$; б) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Используя его, сформулируйте и докажите основную теорему арифметики для а) и б).

Задача 12. Найдите все делители единицы в

а) $\mathbb{Z}[\sqrt{-1}]$, б) $\mathbb{Z}[\sqrt{-d}]$, где $d \geq 1$, в) $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, г*) $\mathbb{Z}[\sqrt{2}]$.

Задача 13. Выполнена ли основная теорема арифметики для

а) $\mathbb{Z}[\sqrt{2}]$, б) $\mathbb{Z}[\sqrt{-3}]$, в) $\mathbb{Z}[\sqrt{3}]$, г) $\mathbb{Z}[\sqrt{-5}]$, д) $\mathbb{Z}[\sqrt{5}]$, е) $\mathbb{Z}[\sqrt{10}]$, ж) $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$,
з) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, и) $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, к*) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$?

Задача 14. При каких комплексных ξ сумма и произведение любых двух чисел вида $a + b\xi$, где a и $b \in \mathbb{Z}$, снова имеет такой же вид?

Задача 15*. Решите в целых числах уравнения
а) $3^n = k^2 + 2$ б) $2^n = k^2 + 7$.

Идеалы

В этой и последующих главах намечен подход к решению следующих трудных задач.

Задача 16. Решите в целых числах уравнения
а) $x^2+5=y^3$, б) $x^2+2x+7=y^3$ в) $5x^2+1=y^3$, г) $6x^2-12x+7=y^3$, д) $x^2-6=y^3$.

Определение. Непустое подмножество I множества целых чисел называется *идеалом*, если оно замкнуто относительно сложения, вычитания и умножения на целые числа:

$$a,b\in I \implies a\pm b\in I, \quad a\in I, b\in\mathbb{Z} \implies ab\in I.$$

Познавательная минутка. Идеалы были придуманы Юлиусом Дедекиндом как формализация "идеальных чисел", придуманных Э. Куммером, как считается, при размышлениях о Великой теоремы Ферма: можно говорить о том, делится или не делится данное число на "идеальное число" вне зависимости от того каков статус этого числа. Аналогичная идея стоит за определением дедекиндова сечения рациональных чисел.

Упражнение 10. а) Докажите, что всякий идеал содержит 0. б) Докажите, что если $a\in I$, то $-a\in I$. в) Докажите, что множество чётных чисел — идеал. г) Докажите, что множество чисел вида $2018m, m\in\mathbb{Z}$, — идеал.

Упражнение 11. Докажите, что пересечение идеалов — идеал.

Здесь и далее мы обозначаем через $(a_1,...,a_n)$ наименьший идеал, содержащий числа $a_1,...,a_n\in\mathbb{Z}$ (т.е. пересечение всех идеалов, содержащих числа $a_1,...,a_n\in\mathbb{Z}$).

Задача 17. а) Пусть a,b — это два взаимнопростых числа. Докажите, что $(a,b)=(1)=\mathbb{Z}$.
б) Докажите, что $(a,b)=(d)$, где $a,b\in\mathbb{Z}$, d есть наибольший общий делитель a,b.
в) Докажите, что любой идеал I в $\mathbb{Z}$ совпадает с (d) для какого-то числа $d\in\mathbb{Z}$.

Как в предудыщем разделе, считаем, что $\omega=\sqrt{d}$ если $d\equiv 2,3 \bmod 4$, и $\omega=\frac{\sqrt{d}+1}{2}$ если $d\equiv 1 \bmod 4$. Идеал в $\mathbb{Z}[\omega]$ определяется абсолютно точно так же, как и идеал в $\mathbb{Z}$ ($\mathbb{Z}$ заменяется на $\mathbb{Z}[\omega]$). Точно так же всякий набор $a_1,...,a_n\in\mathbb{Z}[\omega]$ определяет идеал $(a_1,...,a_n)$ в $\mathbb{Z}[\omega]$. В частности, любой элемент $a\in\mathbb{Z}[\omega]$ определяет идеал (a).

Упражнение 12. Докажите, что $(\alpha)=(\beta)$ тогда и только когда $\alpha/\beta\in\mathbb{Z}[\omega]$ и $\beta/\alpha\in\mathbb{Z}[\omega]$ (т.е. α/β — делитель единицы в $\mathbb{Z}[\omega]$).

Упражнение 13. Пусть $a,x,y\in\mathbb{Z}$. Докажите, что $x+y\omega\in(a)$ тогда и только тогда когда x и y делятся на a.

Определение. Идеал, имеющий вид (a) для какого-то $a\in\mathbb{Z}[\omega]$, называется *главным*. Как мы видели в Задаче 17, все идеалы в $\mathbb{Z}$ главные.

Задача 18. Докажите, что идеал $(2,\sqrt{-14})$ не является главным в $\mathbb{Z}[\sqrt{-14}]$.

Задача 19. Докажите, что для всякого идеала I в $\mathbb{Z}[\omega]$ существуют $\alpha,\beta\in\mathbb{Z}[\omega]$ такие, что

$$I=\{x\alpha+y\beta: \quad x,y\in\mathbb{Z}\}.$$

Определение. Для двух идеалов $I,J\in\mathbb{Z}[\omega]$ положим

$$I+J:=\{i_1+i_2: i_1\in I_1, i_2\in J\}, \quad \bar{I}:=\{\bar{i}: i\in I\},$$

$$IJ:=\{i_1j_1+...+i_kj_k: i_1,...,i_k\in I, j_1,...,j_k\in J\}.$$

Упражнение 14. Посчитайте в $\mathbb{Z}[\sqrt{-14}]$ произведение идеалов $I=(5+\sqrt{-14},2+\sqrt{-14})$ и $J=(4+\sqrt{-14},2-\sqrt{-14})$.

Упражнение 15. Проверьте равенства

$$(3) = p_1 p_2, \quad (5) = p_3 p_4, \quad (1 + \sqrt{-14}) = p_1 p_3, \quad (1 - \sqrt{-14}) = p_2 p_4,$$

где

$$p_1 = (3, 1 + \sqrt{-14}), p_2 = (3, 1 - \sqrt{-14}), p_3 = (5, 1 + \sqrt{-14}), p_4 = (5, 1 - \sqrt{-14}).$$

Упражнение 16. Опишите $(20)(18)$, $(20) + (18)$, $(20) \cap (18)$ в $\mathbb{Z}[\omega]$ для всех допустимых значений d ($d \neq 1$, d не делится на квадраты простых чисел).

Упражнение 17. Докажите, что $I+J, \bar{I}, IJ$ являются идеалами в $\mathbb{Z}[\omega]$ для любых идеалов $I, J \subset \mathbb{Z}[\omega]$.

2 Основная теорема арифметики: квадратичный случай

Все рассматриваемые в этой главе идеалы, являются идеалами в $\mathbb{Z}[\omega]$ для подходящего d. В Задаче 10 мы убедились, что однозначность разложения на множители в самом очевидном смысле теряется для $\mathbb{Z}[\sqrt{-14}]$

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}).$$

С другой стороны, по Упражнению 15:

$$(3) = p_1 p_2, \quad (5) = p_3 p_4, \quad (1 + \sqrt{-14}) = p_1 p_3, \quad (1 - \sqrt{-14}) = p_2 p_4,$$

где

$$p_1 = (3, 1 + \sqrt{-14}), p_2 = (3, 1 - \sqrt{-14}), p_3 = (5, 1 + \sqrt{-14}), p_4 = (5, 1 - \sqrt{-14})$$

Т.е. $(15) = p_1 p_2 p_3 p_4$. Идеалы p_1, p_2, p_3, p_4 играют роль простых сомножителей, см. Задачу 23, а разложение $(15) = p_1 p_2 p_3 p_4$ единственно с точностью до перестановки множителей в соответствии со следующей теоремой.

Теорема 5. Основная теорема арифметики для квадратичных расширений.
Для каждого идеала $I \subset \mathbb{Z}[\omega]$ существует единственное с точностью до перестановки множителей разложение в произведение простых идеалов

$$I = p_1, ..., p_s \subset \mathbb{Z}[\omega].$$

(Определение простого идеала идёт ниже, Определение 2.)

В Теореме 5 есть две существенные части: существование такого разложения и его единственность. Первая доказывается в Задаче 24, вторая — в Задаче 27. В качестве примера задачи, которые можно решить, используя эту теорему, мы предлагаем Задачу 16, см. также завершающий листок про теорему Ферма.

Следствие. Для каждого $m \in \mathbb{Z}[\omega]$ существует единственное с точностью до перестановки множителей разложение идеала (m) в произведение простых идеалов $p_1, ..., p_s \subset \mathbb{Z}[\omega]$.

Доказательство можно разбить на цепочку утверждений, каждое из которых условно просто. В общем и целом схема доказательства похожа на схему доказательства основной теоремы арифметики для целых чисел.

Задача 20. Для всякого набора $a_1, ..., a_n \in \mathbb{Z}[\omega]$ докажите, что

$$\text{а) } (a_1, ..., a_n)(\bar{a}_1, ..., \bar{a}_n) = (N(a_i), \mathrm{Tr}(a_i \bar{a_j}))_{1 \le i,j \le n}.$$

Подсказка: разберите сначала случай идеала, порождённого 2 элементами.

Определение. Будем говорить что идеал I делится на идеал J, если $I = JH$, где H — какой-то идеал в $\mathbb{Z}[\omega]$.

Задача 21. Для любых двух идеалов I, J в $\mathbb{Z}[\omega]$, докажите, что I делится на J тогда и только тогда, когда I содержится в J.
Подсказка: воспользуйтесь предыдущей задачей.

Упражнение 18. Используя Задачу 20 докажите, что, для всякого идеала I в $\mathbb{Z}[\omega]$, существует неотрицательное целое число $N(I)$, такое что $I\bar{I} = (N(I))$.

Задача 22. Докажите, что идеал H делит I и J тогда и только тогда, когда он делит $I + J$.

Упражнение 19. Докажите что $N((a)) = |N(a)|$ для всех $a \in \mathbb{Z}[\omega]$.

Упражнение 20. Докажите что $N(I)N(J) = N(IJ)$ для любых двух идеалов I, J.

Упражнение 21. Докажите, что если идеал I делит идеал J, то $N(I)$ делит $N(J)$. Верно ли обратное?

Упражнение 22. Докажите, что $N(I) = 1$ тогда и только тогда, когда $I = (1)$.

Определение. Идеал I в $\mathbb{Z}[\omega]$ называется *простым*, если он делится ровно на два идеала: себя и (1).

Упражнение 23. Докажите, что идеал I прост тогда и только тогда, когда он максимален, т.е. когда единственный идеал больший его равен (1).

Два идеала называются *взаимнопростыми*, если $I + J = (1)$.

Упражнение 24. Докажите, что любые два различных простых идеала взаимнопросты.

Задача 23. Проверьте, что данные идеалы просты в $\mathbb{Z}[\sqrt{-14}]$:

$$p_1 = (3, 1 + \sqrt{-14}), p_2 = (3, 1 - \sqrt{-14}), p_3 = (5, 1 + \sqrt{-14}), p_4 = (5, 1 - \sqrt{-14})$$

Задача 24. Докажите, что любой ненулевой идеал I в $\mathbb{Z}[\omega]$ разлагается в произведение простых идеалов.

Задача 25. Докажите, что если два идеала I, J в $\mathbb{Z}[\omega]$ взаимнопросты и существует третий идеал H такой, что I делит HJ, то I делит H.

Задача 26. а) Пусть $a \in \mathbb{Z}[\omega]\backslash 0$ и $(a)I = (a)J$ для двух идеалов $I, J \subset \mathbb{Z}[\omega]$. Докажите, что тогда $I = J$.
б) Пусть для некоторых идеалов I, H, J верно что $H \neq (0)$ и $HI = HJ$. Докажите, что тогда $I = J$.

Задача 27. Докажите, что разложение на простые множители из Задачи 24 единственно с точностью до перестановки множителей.

Простые идеалы и простые числа

Задача 28. а) Докажите, что любой идеал в $\mathbb{Z}[\sqrt{-5}]$ либо главный, либо имеет вид $((1 + \sqrt{-5})a, 2a)$ для некоторого $a \in \mathbb{Q}[\sqrt{-5}]$.
б) Докажите, что любой идеал в $\mathbb{Z}[\sqrt{-6}]$ либо главный, либо имеет вид $(\sqrt{-6}a, 2a)$ для некоторого $a \in \mathbb{Q}[\sqrt{-6}]$.

Задача 29. Докажите, что любой ненулевой идеал в $\mathbb{Z}[\omega]$ содержит ненулевое целое число.

Задача 30. Докажите, что любой простой идеал I в $\mathbb{Z}[\omega]$ содержит единственное простое число $p \in \mathbb{Z}, p > 0$.

Задача 31. Докажите, что для всякого простого идеала I либо число $p = N(I)$ простое, либо оно квадрат простого числа $p > 0$.

Задача 32. Докажите, что простые числа p, определённые в двух предыдущих задачах, совпадают.

Задача 33. Докажите, что для всякого простого числа $p \in \mathbb{Z}$ или идеал $(p) \subset \mathbb{Z}[\omega]$ прост, или он равен произведению двух (не всегда различных) сопряжённых простых идеалов.

Задача 34. Пусть $P_\omega(x)$ — это приведённый квадратный трёхчлен с целыми коэффициентами, для которого $P_\omega(\omega) = 0$. Докажите, что в условиях предыдущей задачи первый случай имеет место тогда и только тогда, когда уравнение $P_\omega(x) = 0$ не имеет решений по модулю p.

Алгебраические числа

В этой части мы бы хотим обсудить понятие алгебраического числа, а также те задачи, которые при этом возникают. В общем и целом этот материал часто присутствует в университетских курсах по теории чисел, но может быть усвоен и в старших классах школы.

Определение. Комплексное число $\alpha \in \mathbb{C}$ называется *алгебраическим*, если оно является корнем ненулевого многочлена с рациональными коэффициентами. Алгебраическое число $\alpha \in \mathbb{C}$ называется *целым*, если оно является корнем приведённого многочлена с целыми коэффициентами. Множество алгебраических чисел обозначается $\bar{\mathbb{Q}}$. Множество целых алгебраических чисел обозначается $\bar{\mathbb{Z}}$.

Задача 35. Если для рационального числа a верно, что $a \in \bar{\mathbb{Z}}$, то $a \in \mathbb{Z}$.

Задача 36.* Докажите, что если $a, b \in \bar{\mathbb{Q}}$, то и $a \pm b \in \bar{\mathbb{Q}}$, $ab \in \bar{\mathbb{Q}}$, $a/b \in \bar{\mathbb{Q}}$ (в последнем случае считаем, что $b \neq 0$). Подсказка: попробуйте воспользоваться теоремой Виета.

Задача 37.* Пусть b — это корень уравнения $a_n x^n + ... + a_0$, где $a_0, ..., a_n \in \bar{\mathbb{Q}}$. Докажите, что $b \in \bar{\mathbb{Q}}$.

Задача 38. а) Определите деление с остатком в множестве многочленов от одной переменной с комплексными, вещественными и рациональными коэффициентами.

б) Докажите единственность разложения на простые множители в множестве многочленов с рациональными коэффициентами.

Задача 39. (Лемма Гаусса) Пусть c_g — наибольший общий делитель коэффициентов многочлена $g \in \mathbb{Z}[x]$. Тогда для любых $g_1(x), g_2(x) \in \mathbb{Z}[x]$ выполнено $c_{g_1 g_2} = c_{g_1} c_{g_2}$.

Задача 40. Какие из конструкций и утверждений Задачи 38 применимы к многочленам с целыми коэффициентами от одной переменной? К многочленам с рациональными коэффициентами от двух переменных?

Задача 41. Пусть a — алгебраическое число. Пусть $P_a(x)$ — приведённый ненулевой многочлен наименьшей степени с рациональными коэффициентами, для которого $P_a(a) = 0$. Докажите, что если $Q(a) = 0$ для какого-то многочлена $Q(x)$, то Q делится на P_a.

Задача 42.* Докажите, что если $a, b \in \bar{\mathbb{Z}}$, то и $a \pm b \in \bar{\mathbb{Z}}$, $ab \in \bar{\mathbb{Z}}$.
Подсказка: попробуйте воспользоваться теоремой Виета.

Задача 43.* Пусть $a_1, ...a_n$ — алгебраические числа. Докажите, что если $a, b \in \mathbb{Q}[a_1, ..., a_n]$ и $b \neq 0$, то $\frac{a}{b} \in \mathbb{Q}[a_1, ..., a_n]$.

Задача 44.* Пусть a — это целое алгебраическое число. Пусть $Q(x)$ — это приведённый многочлен наименьшей степени с рациональными коэффициентами, для которого $Q(a) = 0$. Докажите, что $Q(x)$ имеет целые коэффициенты.

Задача 45.* Пусть есть приведенный многочлен с целыми коэффициентами, такой что все его корни по модулю равны 1. Докажите, что тогда все его корни есть корни из 1.

3 Классы идеалов

Определение. Для алгебраических $\alpha_1, \ldots, \alpha_k$ положим $\widetilde{\mathbb{Q}} := \mathbb{Q}[a_1, ..., a_k]$ и $\widetilde{\mathbb{Z}} := \bar{\mathbb{Z}} \cap \widetilde{\mathbb{Q}}$. Отметим, что любое подмножество в $\mathbb{C}$, замкнутое относительно сложения, вычитания и умножения называется *кольцом*.

Определение. Непустое подмножество в $\widetilde{\mathbb{Z}}$ называется *идеалом*, если оно замкнуто относительно сложения, вычитания и умножения на элементы $\widetilde{\mathbb{Z}}$.

Определение. Назовем идеалы $I, J \subseteq \widetilde{\mathbb{Z}}$ *эквивалентными*, если существуют ненулевые $\alpha, \beta \in \widetilde{\mathbb{Z}}$, такие что $(\alpha)I = (\beta)J$. Эквивалентность идеалов будем обозначать $I \sim J$.

Задача 46. Проверьте, что $\sim$ является отношением эквивалентности.

Определение. Классы эквивалентности идеалов будем называть *классами идеалов*.

Задача 47. Докажите, что число классов идеалов равно 1 тогда и только тогда, когда все идеалы – главные.

Задача 48. Проверьте, что если $I_1 \sim I_2$ и $J_1 \sim J_2$, то $I_1 J_1 \sim I_2 J_2$.

Задача 49. Опишите классы идеалов в $\mathbb{Z}[\sqrt{-5}]$ и $\mathbb{Z}[\sqrt{-6}]$. Как в них устроено умножение идеалов?

Задача 50. Докажите, что если $I \subseteq (\alpha)$, то множество $(1/\alpha)I$ – идеал в $\widetilde{\mathbb{Z}}$.

В следующей серии задач обсуждается одно из фундаментальных утверждений алгебраической теории чисел. Это утверждение будет играть ключевую роль в доказательстве общего случая основной теоремы арифметики. Само доказательство обсуждается в следующей части проекта и может сдаваться в предположении что Теорема 6 уже доказана.

Теорема 6. Число классов идеалов конечно.

Определение. Назовем набор чисел $x_1, ..., x_n \in \widetilde{\mathbb{Q}}$ *базисом* над $\mathbb{Q}$, если любой элемент $a \in \widetilde{\mathbb{Q}}$ единственным образом представляется в виде $m_1 x_1 + ... + m_n x_n$, где $m_1, ..., m_n \in \mathbb{Q}$.

Задача 51. Если α — алгебраическое, то в $\mathbb{Q}[\alpha]$ существует конечный $\mathbb{Q}$-базис.

Задача 52. Докажите, что в $\widetilde{\mathbb{Q}}$ существует конечный базис над $\mathbb{Q}$.

Задача 53. Для любого алгебраического α существует такое ненулевое $n \in \mathbb{Z}$, что $n\alpha$ — целое алгебраическое число.

Задача 54. Пусть I – идеал в $\widetilde{\mathbb{Z}}$. Докажите, что существует конечный набор $\alpha_1, \ldots, \alpha_N \in I$, такой что любое $\alpha \in I$ представимо в виде $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_N\alpha_N$ с целыми $m_1, \ldots, m_N$ (не обязательно единственным образом).

Подсказка: докажите, что для фиксированного базиса в $\widetilde{\mathbb{Q}}$ коэффициенты $\alpha \in I$ не могут быть слишком маленькими.

Задача 55. Докажите, что существует конечный набор $\alpha_1, \ldots, \alpha_n \in I$, для которого такое представление единственно.
Подсказка: индукция по размеру базиса.

Определение. Такие наборы будем называть *целым базисом* идеала I.

Задача 56. Докажите, что любой целый базис I является $\mathbb{Q}$-базисом $\widetilde{\mathbb{Q}}$.

Определение. Обозначим $\widetilde{\mathbb{Z}}/I$ – множество классов эквивалентности элементов $\widetilde{\mathbb{Z}}$ по отношению эквивалентности

$$z_1 \equiv z_2 \mod I \iff z_1 - z_2 \in I.$$

Элементы $\widetilde{\mathbb{Z}}/I$ будем называть *вычетами по модулю* I.

Задача 57. Проверьте, что это действительно отношение эквивалентности, и при $\widetilde{\mathbb{Z}} = \mathbb{Z}$ – определение вычета совпадает со стандартным.

Задача 58. Чему равно количество элементов в $\widetilde{\mathbb{Z}}/I$ для квадратичных расширений?

Задача 59. Докажите, что I содержит ненулевое целое число.

Задача 60. Докажите, что число элементов в $\widetilde{\mathbb{Z}}/I$ конечно.

Задача 61. Докажите, что существует только конечное число идеалов, содержащих данное $\alpha \in \widetilde{\mathbb{Z}}$.

Зафиксируем целый базис $\alpha_1, \ldots, \alpha_n$ для идеала $(1) = \widetilde{\mathbb{Z}}$ и сопоставим каждому $\alpha \in \widetilde{\mathbb{Z}}$ набор целых чисел $(x_1, \ldots, x_n)$, таких что $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$. Положим

$$||\alpha|| = |x_1| + |x_2| + \ldots + |x_n|.$$

Задача 62. Пусть $\{\beta_1, ..., \beta_m\}$ — какой-то целый базиса идеала I. Докажите, что набор $\{\beta_1, ..., \beta_m\}$ является $\mathbb{Q}$-базисом в $\widetilde{\mathbb{Q}}$.

Задача 63. Докажите, что существует такое натуральное M_1, что для любого ненулевого $\beta \in \widetilde{\mathbb{Z}}$ можно выбрать целый базис $\beta_1, \ldots \beta_n$ идеала (β), такой что $||\beta_i|| < M_1||\beta||$ для всех i.

Задача 64. Докажите, что для любых $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$ существует $c \in \widetilde{\mathbb{Z}}$, такое что

$$||\alpha - c\beta|| < nM_1||\beta||.$$

Задача 65. Докажите, что для любых $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$ существуют натуральное

$$m \leq (2n^2M_1 + 1)^n + 1 = M_2$$

и $c \in \widetilde{\mathbb{Z}}$, такие что $||m\alpha - c\beta|| < ||\beta||$.

Задача 66. Докажите, что для любого идеала I существует $\beta \in I$, такое что $M_2!I \subseteq (\beta)$. В частности, $M_2! \in (1/\beta)M_2!I$.

Задача 67. Докажите, что число классов идеалов — конечно.

Основная теорема арифметики. Общий случай

Теорема 7. Основная теорема арифметики для целых алгебраических чисел.
Пусть $a_1, ..., a_n$ — набор целых алгебраических чисел, такой что $\mathbb{Z}[a_1, ..., a_n]$ совпадает с подмножеством целых алгебраических чисел в $\mathbb{Q}[a_1, ..., a_n]$. Тогда для каждого идеала $I \subset \mathbb{Z}[a_1, ..., a_n]$ существует и единственное с точностью до перестановки множителей разложение в произведение простых идеалов

$$I = p_1, ..., p_s \subset \mathbb{Z}[a_1, ..., a_n].$$

В Теореме 7 есть две существенные части: существование такого разложения и его единственность. Первая рассматривается в Задаче 73, вторая — в Задаче 78.

Задача 68. Пусть для некоторого $\alpha \in \widetilde{\mathbb{Q}}$ выполнено $\alpha I \subseteq I$. Докажите, что $\alpha \in \widetilde{\mathbb{Z}}$.
Подсказка: в целом базисе I запишите условие того, что $\alpha I \subseteq I$, и, вспомнив метод Гаусса решения системы линейных уравнений, постройте приведенный многочлен с целыми коэффициентами, корнем которого является α.

Задача 69. Пусть для некоторых идеалов I, J выполнено $JI = I$. Докажите, что $J = (1)$. Подсказка: действуйте по аналогии с предыдущей задачей.

Задача 70. Докажите, что для любого идеала I существуют натуральные $m > k$, такие что $I^k \sim I^m$.

Задача 71. Докажите, что существует $\alpha \in \widetilde{\mathbb{Z}}$, такое что $I^{m-k} = (\alpha)$. В частности, для всякого идеала $I \subseteq \widetilde{\mathbb{Z}}$ существует идеал $J \subseteq \widetilde{\mathbb{Z}}$ и $\alpha \in \widetilde{\mathbb{Z}}$, такие что $IJ = (\alpha)$.

Задача 72. Докажите, что для любых двух идеалов I, J в $\widetilde{\mathbb{Z}}$ — идеал I делится на J тогда и только тогда, когда I содержится в J.

Задача 73. Докажите, что любой идеал $I \subseteq \widetilde{\mathbb{Z}}$ представим в виде произведения конечного набора простых идеалов.

Задача 74. Докажите, что если идеалы I, J взаимнопросты и $JH \subseteq I$, то $H \subseteq I$.

Задача 75. Докажите, что любые два различных простых идеала взаимно просты.

Задача 76. Докажите, что если I — простой идеал, и $I^m \subseteq J$, то $J = I^k$ для целого $k \leq m$.

Задача 77. Докажите, что степени двух различных простых идеалов взаимно просты.

Задача 78. Докажите однозначность разложения на множители в Задаче 73.

Основная теорема арифметики и Великая Теорема Ферма

Фиксируем простое число $p > 2$ и обозначим через ζ_p комплексный корень p-ой степени из 1. Цель данного раздела доказать следующую теорему.

Теорема 8. Пусть целые числа x, y, z таковы что $x^p + y^p = z^p$ и число классов $\mathbb{Z}[\zeta_p]$ не делится на p. Тогда xyz делится на p.

Мы надеемся, что участники проекта смогут доказать Теорему 8, после того, как прорешают идущие ниже задачи.

Упражнение 25. Докажите, что $1 + \zeta_p + \zeta_p^2 + .. + \zeta_p^{p-1} = 0$.

Задача 79. Найдите приведённый многочлен с целыми коэффициентами степени $p - 1$, корнем которого является $1 - \zeta_p$.

Задача 80. Докажите, что все коэффициенты этого многочлена (кроме первого) делятся на p и что этот многочлен неприводим.

Упражнение 26. Докажите, что $\Sigma_{i=0}^{p-1} a_i \zeta_p^i = \Sigma_{i=0}^{p-1} b_i \zeta_p^i$ для рациональных чисел

$$a_0, .., a_{p-1}, b_0, ..., b_{p-1}$$

если и только если

$$a_0 - b_0 = a_1 - b_1 = ... = a_{p-1} - b_{p-1}.$$

Напомним что число γ называется делителем единицы, если γ и $1/\gamma$ — целые алгебраические числа.

Задача 81. Докажите, что $\frac{1-\zeta_p^n}{1-\zeta_p}$ — делитель единицы, если n не делится на p.

Задача 82. Докажите, что $(1 - \zeta_p)^p = (p)$ (равенство идеалов).

Упражнение 27. Докажите, что если $a \in \mathbb{Z}[\zeta_p]$ делится на p, то оно делится на $1 - \zeta_p$.

Пусть числа $a_0, ..., a_{p-1}$ рациональны, $a = a_0 + .. + a_{p-1}\zeta_p^{p-1}$.

Задача 83. Докажите, что все коэффициенты многочлена

$$P(a_0, ..., a_{p-1}; x) := \Pi_{k=1}^{p-1}(x - \Sigma_{i=0}^{p-1} a_i \zeta_p^{ki}),$$

рассматриваемого как многочлен от x, также рациональны.

Напомним, что для всякого алгебраического числа a через $P_a(x)$ обозначается приведённый многочлен наименьшей степени, для которого $P_a(a) = 0$.

Задача 84.* Докажите, что $P(a_0, ..., a_{p-1}; x) = P_a(x)^d$, где d — целое положительное число.

Задача 85. Если многочлен $P_a(x)$ имеет целые коэффициенты, то для любых целых чисел $1 \leq k \leq p-1, l \in \mathbb{Z}$, число $\Sigma_{i=0}^{p-1} a_i \zeta_p^{ki+l}$ является целым алгебраическим.

Задача 86. Пусть многочлен $P_a(x)$ имеет целые коэффициенты. Докажите, что тогда $p(a_i - a_j) \in \mathbb{Z}$ для всех $0 \leq i, j \leq p-1$.

Задача 87. Докажите, что число $1/(1 - \zeta_p)$ не является целым алгебраическим.

Задача 88. Докажите что $\mathbb{Z}[\zeta_p]$ совпадает с множеством целых алгебраических чисел в $\mathbb{Q}[\zeta_p]$.
Подсказка: постарайтесь найти применение Упражнению 27.

Задача 89. Докажите, что для любого элемента $a \in \mathbb{Z}[\zeta_p]$ существует $b \in \mathbb{Z}$, такое что $a^p - b$ делится на p.

Задача 90. а) Докажите, что $\sqrt{-1} \notin \mathbb{Z}[\zeta_p]$.
б) Пусть $q \neq p, q \neq 2$ простое число, а ζ_q — комплексный корень q-ой степени из 1. Докажите, что $\zeta_q \notin \mathbb{Z}[\zeta_p]$.
в) Пусть ζ_{p^2} — корень p^2-ой степени из 1, не являющийся корнем p-ой степени из 1. Докажите, что $\zeta_{p^2} \notin \mathbb{Z}[\zeta_p]$.
г) Найдите все корни из 1 в $\mathbb{Z}[\zeta_p]$.

Задача 91.* Докажите, что любой делитель единицы в $u \in \mathbb{Z}[\zeta_p]$ представляется в виде $\zeta_p^i v$, где $i \in \mathbb{Z}$, $v \in \mathbb{R}$.

Пусть x, y, z, p как в теореме 8.

Задача 92. Докажите что идеалы $(x + \zeta_p^i y)$ попарно взаимно просты при $0 \leq i \leq p-1$.

Задача 93. Докажите Теорему 8.

Список литературы

[IR] К. Айерлэнд, М. Роузен, *Классическое введение в современную теорию чисел*, Мир, 1987.

[Po] М. Постников, *Теорема Ферма*, Наука, 1978.

[C1] K. Conrad, *Factoring in quadratic fields*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/quadraticgrad.pdf.

[C2] K. Conrad, *Ideal factorization*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/idealfactor.pdf.

[Mi] J. Milne, *Algebraic number theory*, http://jmilne.org/math/CourseNotes/ANT.pdf.

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer-Verlag, 1996.

[Go] А. Гончаров, *Арифметика гауссовых чисел*, Журнал "Квант"12 (1985), http://kvant.mccme.ru/1985/12/.

[SS] В. Сендеров, А. Спивак, *Суммы квадратов и целые гауссовы числа*, Журнал "Квант"3 (1993), см. также http://kvant.mccme.ru/pdf/1999/03/.

[ZSS] А. Заславский, А. Скопенков, М. Скопенков (редакторы), *Элементы математики в задачах - через олимпиады и кружки к профессии*, 2-ое изд., издательство МЦНМО, 2017.

Задача 1. $(a+bi)+(c+di)=(a+c)+(b+d)i$
$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$.

Упражнение 1. Делители единицы имеют норму 1 и находятся перебором.

Задача 2. Докажем деление с остатком по норме $N(a+bi)=(a+bi)(a-bi)=a^2+b^2$ в целых гауссовых числах: если $x,y\in\mathbb{Z}[i]$ и $y\neq 0$, то существуют $r,t\in\mathbb{Z}[i]$, такие что $x=yr+t$ и $N(t)<N(y)$.

Доказательство в алгебраической интерпретации: пусть $x=a+bi$ и $y=c+di$, тогда $x/y=(a+bi)/(c+di)=(a+bi)(c-di)/(c^2+d^2)=((ac+bd)+(bc-ad)i)/(c^2+d^2)=n+mi+(k+li)/(c^2+d^2)$, где n,m,k,l — целые, и $|k|,|l|\leq(c^2+d^2)/2$ (обычное деление с остатком $ac+bd$ и $bc-ad$ на c^2+d^2). Значит, $a+bi=(c+di)(n+mi)+(k+li)(c+di)/(c^2+d^2)$, причем $(k+li)(c+di)/(c^2+d^2)\in\mathbb{Z}[i]$ и $N(k+li)=k^2+l^2\leq(c^2+d^2)^2/2$, поэтому $N((k+li)(c+di)/(c^2+d^2))=N(k+li)N(c+di)/N(c^2+d^2)\leq N(c+di)/2$. Значит, $r=n+mi$ и $t=(k+li)(c+di)/(c^2+d^2)$ — подходят.

В геометрической интерпретации это доказательство выглядит так: множество целых гауссовых чисел, кратных y, выглядит на плоскости комплексных чисел как квадратная решетка, натянутая на векторы y и yi, которые имеют равную длину и ортогональны друг другу. Это решетка естественным образом разбивает плоскость на квадраты со стороной, равной длине вектора y, то есть $\sqrt{c^2+d^2}=\sqrt{N(y)}$. В частности, вектор x лежит в каком-то из этих квадратов, и мы можем выбрать его вершину $z=rb$ такую, что расстояние от неё до x — минимальное. Тогда расстояния e и f от z до проекций x на стороны квадрата, прилежащие к z, не больше половины стороны квадрата, и квадрат расстояния $|x-z|^2=e^2+f^2\leq(c^2+d^2)/2=N(y)/2$, поэтому $r=z/b$ и $t=x-z$ — подходят.

Из деления с остатком теперь легко доказать основную теорему арифметики. Заметим, что если p — простое и x не делится на p, то применяя к x и p алгоритм Евклида, мы получим $ax+bp=1$ для каких-то a и b. Далее, если xy делится на p, то x или y делятся на p — действительно, иначе $ax+bp=1$ и $cy+dp=1$ для каких-то a,b,c,d, поэтому $acxy=(1-bp)(1-dp)=1+p(bd-b-d)$ делится на p, противоречие.

Для любого z существует можно построить какое-то разложение на простые, просто раскладывая его на сомножители, отличны от делителей единицы (норма уменьшается, поэтому процесс когда-нибудь закончится). Если есть два различных разложения на простые, то сначала сократим на одинаковые простые, а потом для произвольного оставшегося простого p получим, что он делит произведение отличных от него простых, что невозможно (достаточно несколько раз применить то, что если xy делится на p, то x или y делятся на p).

Задача 3. Заметим, что если n делится на 2, то $x = 0$, т.к. разность квадратов натуральных чисел делится на их сумму, которая больше 1. Значит, если n делится на 2, то $x = 0$ и $y = \pm 1$.

Если n не делится на 2, то разложим в целых гауссовых числах $x^2+1 = (x+i)(x-i) = y^n$. Заметим, что $2|x$, т.к. иначе $x^2+1 \equiv 2 \mod 4$, а $y^n \not\equiv 2 \mod 4$ при $n > 1$. Значит, $\gcd(x+i, x-i) = \gcd(2i, x-i) = \gcd(2i, -i) = 1$, то есть $x+i$ и $x-i$ взаимно просты. Значит, из единственности разложения на множители, $x+i = \varepsilon z^n$, где $z \in \mathbb{Z}[i]$, а ε — делитель единицы в $\mathbb{Z}$, то есть $\varepsilon \in \{1, -1, i, -i\}$. Но n не делится на 2, так что после умножения z на делитель единицы можно считать, что $x + i = z^n$. Пусть $z = a + bi$, тогда $i = \operatorname{Im} z^n = i(na^{n-1}b - \binom{n}{3}a^{n-3}b^3 + \ldots + (-1)^{\frac{n-1}{2}}b^n)$. Значит, 1 делится на b, то есть $b = \pm 1$. Заметим, что a делится на 2, т.к. иначе $z = a + bi \equiv 1 + i \mod 2$, поэтому $z^2 \equiv (1+i)^2 \equiv 0 \mod 2$ и $x^2 + 1 = z^n \equiv 0 \mod 2$, но x делится на 2, противоречие. Если $a = 0$, то $x + i = \pm i$, поэтому $x = 0$ и $y = 1$.

Если $a \neq 0$, то $1 \equiv (-1)^{\frac{n-1}{2}}b^n \mod 4$, поэтому $1 = (-1)^{\frac{n-1}{2}}b^n$ и $0 = \binom{n}{n-2} + \ldots + (-1)^{\frac{n-5}{2}}\binom{n}{3}a^{n-5} + (-1)^{\frac{n-3}{2}}na^{n-3} = \binom{n}{2} + \ldots + (-1)^{\frac{n-5}{2}}\binom{n}{n-3}a^{n-5} + (-1)^{\frac{n-3}{2}}\binom{n}{n-1}a^{n-3}$. Докажем, что все слагаемые в этой сумме, кроме $\binom{n}{2}$, делятся на степень 2, большую, чем $\binom{n}{2}$ — из этого очевидно следует, что равенство невозможно. Для этого заметим, что

$$\binom{n}{2k}a^{2k-2} = \binom{n}{2}\binom{n-2}{2k-2}\frac{2a^{2k-2}}{(2k-1)2k} = \binom{n}{2}\binom{n-2}{2k-2}\frac{(a/2)^{2k-2}}{2k-1}\frac{2^{2k-2}}{k}$$

и $2^{2k-2} > k$ при $k \geq 2$, из чего следует предыдущее утверждение. Значит, уравнение не имеет других решений, кроме $x = 0, y = 1$ при любом $n \geq 2$, и $x = 0, y = -1$ при четном n.

Задача 4. а) Если $p = 2$, то $p = (1+i)(1-i)$, поэтому p не простое в гауссовых целых числах.

Если $p = 4k+3$, то предположим противное, т.е. p не простое гауссово число. Тогда пусть $p = q_1 q_2 \ldots q_n$ — разложение на простые. Заметим, что $\bar{p} = p = \bar{q}_1 \ldots \bar{q}_n$, поэтому p делится на сопряженные к своим простым делителям. Заметим, что сопряженное к простому также простое (иначе его разложение можно снова сопрячь), и в нашем случае оно отличается от исходного (с точностью до домножения на делитель единицы). Действительно, иначе при $q = a + bi$ число $q/\bar{q} = (a+bi)/(a-bi) = ((a^2-b^2)+2abi)/(a^2+b^2)$ должно быть целым гауссовым, что возможно только в случаях $a = \pm b$ и $ab = 0$ (т.к. $|2ab| \leq a^2 + b^2$). В первом случае q делится на $1+i$, поэтому $p\bar{p} = p^2$ делится на $(1+i)(1-i) = 2$, противоречие. Во втором случае можно считать, что q — натуральное (с точностью до домножения на делитель единицы), но p простое в целых

числах, поэтому $q = p$ и p — простое в целых гауссовых, противоречие.

Значит, q и $\bar{q}$ — различные простые (q — простой делитель p в целых гауссовых), и p делится на оба. Значит, p делится на $q\bar{q} = a^2 + b^2$, и т.к. p — простое в целых числах, то $p = a^2 + b^2$. Но как известно, простое p вида $4k + 3$ нельзя представить в виде суммы двух квадратов (посмотрим на остатки по модулю 4), противоречие.

Если $p = 4k + 1$, то (как известно) -1 является вычетом по модулю p, поэтому существует натуральное n такое, что $n^2 + 1 = (n + i)(n - i)$ делится на p. Если бы p было простым гауссовым, то $n + i$ или $n - i$ делилось бы на p, что очевидно не верно. Значит, p не простое гауссово.

б) Пусть $n = a^2 + b^2 = (a + bi)(a - bi)$ и $m = c^2 + d^2 = (c + di)(c - di)$, тогда $nm = ((a+bi)(c+di))((a-bi)(c-di)) = ((ac-bd)+(ad+bc)i)((ac-bd)-(ad+bc)i)) = (ac - bd)^2 + (ad + bc)^2$.

в) Рассмотрим минимальное такое n, что $n = x^2 + y^2$ для целых x и y, и при этом не удовлетворяет условию теоремы 2. Тогда n делится на какое-то простое $p = 4k + 3$ в нечетной степени. Но т.к. -1 невычет по модулю p, то из того, что $x^2 + y^2$ делится на p, следует, что x и y делятся на p. Значит, n делится на p^2 и $n/p^2 = (x/p)^2 + (y/p)^2$, причем n/p^2 делится на p в нечетной степени, что противоречит минимальности n. Значит, если натуральное $n = x^2 + y^2$, то оно удовлетворяет условию теоремы 2.

Обратно, если n удовлетворяет условию теоремы 2, то из пункта б) достаточно показать, что 2, простое $p = 4k+1$ и p^2 для простого $p = 4k+3$ — представимы в виде суммы двух квадратов. Действительно, $2 = 1^2+1^2$, $p^2 = p^2 + 0^2$ для любого p, а $p = 4k + 1$ — составное в целых гауссовых, поэтому делится на гауссово простое $q = a + bi$, причем (аналогично пункту а)) $q \neq \pm 1 \pm i$ и $ab \neq 0$, поэтому p делится на $q\bar{q} = a^2 + b^2$. Значит, $p = a^2 + b^2$ из простоты p в целых числах.

Задача 5. Будем считать, что n удовлетворяет условию теоремы 2 (т.е. представляется хотя бы одним способом). Тогда, как видно из решения задачи 4, для любого представления n в виде суммы $x^2 + y^2$ — мы можем сократить на все простые вида $4k + 3$, поэтому можно считать, что n не делится на простые вида $4k + 3$ (число представлений от этого не изменится). Пусть $n = 2^{\alpha_0} p_1^{\alpha_1} \dots p_m^{\alpha_m}$ – разложение на простые в целых числах, тогда, как видно из решения задачи 4, его разложения в целых гауссовых будет иметь вид $n = (1 + i)^{\alpha_0}(1 - i)^{\alpha_0} q_1^{\alpha_1}(\bar{q}_1)^{\alpha_1} \dots q_m^{\alpha_m}(\bar{q}_m)^{\alpha_m}$, где q_i — простой делитель p_i. Каждому представлению n в виде суммы двух квадратов соответствует разложение $n = (x + yi)(x - yi) = z\bar{z}$, где $z = x + yi$ определено с точность до домножения на делители единицы и сопряжения. Количество способов составить z с точностью до делителей единицы, как видно из разложения n на простые гауссовы, равно

$(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ (т.к. $1+i$ и $1-i$ — одинаковые простые). При сопряжении z совпадает с собой (с точностью до делителя единицы) тогда и только тогда, когда z делится на каждое простое в степени, в 2 раза меньшей степени вхождения в n. Такое возможно только в том случае, когда все $\alpha_1,\dots,\alpha_m$ — четные, т.е. $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)$ — нечетное. Значит, окончательная формула количества представлений n в виде суммы двух квадратов — $\lfloor((\alpha_1+1)(\alpha_2+1)\dots(\alpha_m+1)+1)/2\rfloor$.

Задача 6. Докажем, что уравнение $x^3+y^3+z^3=0$ с $xyz\neq 0$ не имеет решений в целых числах. Предположим противное, тогда после сокращения на $\gcd(x,y,z)$ можем считать, что x,y,z взаимно просты в совокупности (а значит, и попарно). Если xyz не делится на 3, то $x^3,y^3,z^3\equiv\pm1 \mod 9$, поэтому $x^3+y^3+z^3\not\equiv 0 \mod 9$. Значит, одно из x,y,z делится на 3 (из взаимной простоты — ровно одно) – без ограничения общности z делится на 3. Заменяя z на $-z$, получаем уравнение $x^3+y^3=z^3$, где z делится на 3. Далее будем работать в $\mathbb{Z}[\xi]$, где $\xi=\frac{-1+\sqrt{-3}}{2}$, и обозначим $\pi=1-\xi$ – простое число, такое что $\pi\bar{\pi}=-\xi^2\pi^2=3$.

Докажем, что если для взаимно простых $x,y,z\in\mathbb{Z}[\xi]$ выполнено $x^3+y^3=uz^3$, где u — делитель единицы, и z делится π, то z делится на π^2. Действительно, $x^3+y^3=(x+y)(x+\xi y)(x+\xi^2y)=(x+y)(x+y-\pi y)(x+y+\pi y-\xi^2\pi^2y)$, поэтому из того, что $x^3+y^3=uz^3$ делится на π, следует, что $x+y$ делится на π, значит, все 3 множителя в разложении делятся на π, причем $x+y\not\equiv x+y-\pi y\not\equiv x+y+\pi y \mod \pi^2$ (т.к. y не делится на π), и каждое число в $\mathbb{Z}[\xi]$ очевидно сравнимо с $0,1$ или 2 по модулю $\pi=1-\xi$. Значит, один из этих множителей делится на π^2, поэтому uz^3 делится на π^4. Значит, z делится на π^2.

Теперь докажем, что если для взаимно простых $x,y,z\in\mathbb{Z}[\xi]$ выполнено $x^3+y^3=uz^3$, где u – делитель единицы, z делится π^k и не делится на π^{k+1} с $k\geq 2$, то существуют взаимно простые $x_1,y_1,z_1\in\mathbb{Z}[\xi]$ с $x_1^3+y_1^3=u_1z_1^3$, где u_1 — делитель единицы, z делится π^{k-1} и не делится на π^k. Разложением $x^3+y^3=(x+y)(x+\xi y)(x+\xi^2y)=(x+y)(x+y-\pi y)(x+y+\pi y-\xi^2\pi^2y)=uz^3$ мы снова получаем, что все 3 множителя в разложении делятся на π, причем ровно один из них делится на π^2 (а значит, на π^{3k-2}). После домножения y на ξ или ξ^2 можно считать, что $x+y$ делится на π^{3k-2}.

Из единственности разложения получаем, что $x+y=u_1\pi^{3k-2}a^3$, $x+\xi y=u_2\pi b^3$, $x+\xi^2y=u_3\pi c^3$, где u_i — делители единицы, и a,b,c не делятся на π. Из равенства $0=(x+y)+\xi(x+\xi y)+\xi^2(x+\xi^2y)$ получаем $u_1\pi^{3k-2}a^3+\xi u_2\pi b^3+\xi^2u_3\pi c^3=0$. После сокращения уравнение можно привести к виду $b^3+u_4c^3=u_5(a\pi^{k-1})^3$, где u_4 и u_5 — делители единицы. Докажем, что $u_4=\pm1$. Действительно, заметим, что если $b=n+m\xi$,

где n, m целые числа, то $b^3 = (n + m\xi)^3 \equiv n^3 + m^3 \equiv \pm 1 \mod 3$, т.к. b не делится на π. Аналогично $c^3 \equiv \pm 1 \mod 3$, и $(\pi^{k-1})^3$ делится на 3 из $k \geq 2$. Значит, $\pm 1 \pm u_4$ делится на 3, поэтому $u_4 = \pm 1$. После замены c на $u_4 c$ получаем $b^3 + c^3 = u_5(a\pi^{k-1})^3$, откуда мы получаем нужные x_1, y_1, z_1.

Теперь можно рассмотреть целочисленное решение $x^3 + y^3 = z^3$ с z, делящимся на 3, и спуском по степени вхождения π в z получить противоречие, т.к. z делится на π^2.

Упражнение 2. Имеем $x^3 - 1 = (x - 1)(x^2 + x + 1) = 0$ и решаем квадратное уравнение.

Задача 7. Заметим, что для $a = x + yi \in \mathbb{Z}[\xi]$ стандартная норма $N(a) = x^2 + y^2$ будет целой, т.к. $a = (z + \sqrt{-3}t)/2$, где z и t — одной четности. Для ненулевого $a \in \mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$ числа, кратные a, образуют решетку в плоскости комплексных чисел, разбивающую её на правильные треугольники со стороной $|a|$. Для любой точки в таком треугольнике квадрат расстояния от неё до любой вершины (кроме остальных в том случае, когда точка совпадает с вершиной) меньше $|a|^2 = N(a)$, откуда следует деление с остатком по норме комплексных чисел (чтобы поделить b на a с остатком, надо вычесть из b ближайшее к нему на комплексной плоскости число вида ac). Аналогично задаче 2, отсюда мы получаем основную теорему арифметики для $\mathbb{Z}[\xi]$.

Задача 8. Для делителей единицы в $\mathbb{Z}[\xi]$ норма должна быть 1 (т.к. у обратного норма должна быть целой). Для $a = (x + \sqrt{-3}y)/2 \in \mathbb{Z}[\xi]$ – $N(a) = (x^2 + 3y^2)/4$, поэтому если a — делитель единицы, то $-2 \leq x \leq 2$ и $-1 \leq y \leq 1$. Перебором получаем, что все делители единицы в $\mathbb{Z}[\xi]$ – это $\pm 1, \pm\xi$ и $\pm\xi^2$.

Упражнение 3. а) Замкнутость относительно умножения следует из равенства $(x + y\sqrt{d})(z + t\sqrt{d}) = (xz + dyt) + (xt + yz)\sqrt{d}$.
б) $\frac{x+y\sqrt{d}}{z+t\sqrt{d}} = \frac{(xz-dyt)+(yz-xt)\sqrt{d}}{z^2-dt^2}$.

Упражнение 4. ξ является целым в $\mathbb{Q}[\sqrt{-3}]$. $\frac{1+i}{2}$ не является целым в $Z[i]$.

Упражнение 5. Очевидно.

Упражнение 6. а) $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha) = (x - \alpha)(x - \bar{\alpha})$. Подставляя в $x = \alpha$, получаем ноль.
б) Вычисление.

Задача 9. По предыдущему упражнению $x + y\sqrt{d}$ цело в $\mathbb{Q}[\sqrt{d}]$ тогда и только тогда, когда числа $2x$ и $x^2 - dy^2$ целы. Легко проверить, что для элементов $Z[\omega]$ это условие выполнено.
Пусть числа $2x$ и $x^2 - dy^2$ целы. Если x целое, то dy^2 целое, откуда y целое и $x + y\sqrt{d} \in Z[\omega]$. Если $x = n/2$, где n нечетно, то $4dy^2$ целое,

откуда $y = m/2$, где m целое. При этом $dm^2 \equiv n^2 \equiv 1 \bmod 4$, откуда m нечетно и $d \equiv 1 \bmod 4$. Тогда $x + y\sqrt{d} = m\omega + (n-m)/2 \in \mathbb{Z}[\omega]$.

Упражнение 7. Если $N(\gamma) = \pm 1$, то $\frac{1}{\gamma} = \pm\bar{\gamma} \in \mathbb{Z}[\omega]$.
Если $\frac{1}{\gamma} \in \mathbb{Z}[\omega]$, то $1 = N(1) = N(\gamma\frac{1}{\gamma}) = N(\gamma)N(\frac{1}{\gamma})$, откуда $N(\gamma) = \pm 1$, поскольку $N(\frac{1}{\gamma}) \in \mathbb{Z}$.

Упражнение 8. Предположим, что γ не просто: $\gamma = ab$, $a, b \in \mathbb{Z}[\omega]$, $N(a) \neq \pm 1$, $N(b) \neq \pm 1$. Тогда $|N(\gamma)| = |N(a)||N(b)|$, откуда одно из (натуральных) чисел $|N(a)|$ и $|N(b)|$ равно 1. Противоречие.
Покажем, что $5 \in Z[\sqrt{3}]$ простое, хотя $N(5) = 25$ – составное число. Пусть $5 = ab$, где $a, b \in \mathbb{Z}[\sqrt{3}]$, $N(a) \neq \pm 1$, $N(b) \neq \pm 1$. Тогда $N(a)N(b) = 25$, откуда $N(a) = \pm 5$. Если $a = x + y\sqrt{3}$, то $x^2 - 3y^2 = \pm 5$. Это уравнение не имеет решений по модулю 3.

Упражнение 9. Индукция по $|N(\gamma)|$.

Задача 10. Поскольку $N(3) = 9$, $N(5) = 25$, $N(1 + \sqrt{-14}) = N(1 - \sqrt{-14}) = 15$, норма неотрицательна, и норма произведения равна произведению норм, то достаточно показать, что не существует числа $\alpha \in \mathbb{Z}[\sqrt{-14}]$ с $N(\alpha) = 3$ или $N(\alpha) = 5$. Пусть $\alpha = x + y\sqrt{-14}$, где x, y — целые. А уравнения $x^2 + 14y^2 = 3$ и $x^2 + 14y^2 = 5$ не имеют решений в целых числах, поскольку $x^2 + 14y^2 > 5 > 3$ при $y \neq 0$.

Задача 11. а) Для ненулевого $b \in \mathbb{Z}[\sqrt{-2}]$ числа, кратные b, образуют решетку в плоскости комплексных чисел, разбивающую её на прямоугольники со сторонами $|b|$ и $\sqrt{2}|b|$. Для любой точки внутри такого прямоугольника существует вершина, для которой квадрат расстояния от неё точки не больше $(\frac{1}{2}|b|)^2 + (\frac{1}{2}\sqrt{2}|b|)^2 = \frac{3}{4}|b|^2 < N(b)$. Из этого, аналогично случаю гауссовых чисел, мы получаем деление с остатком, алгоритм Евклида и единственность разложения на множители.

б) Для ненулевого $b \in \mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ числа, кратные b, образуют решетку в плоскости комплексных чисел, разбивающую её на равнобедренные треугольники с основанием $|b|$ и боковыми сторонами $\sqrt{\frac{1+7}{4}}|b| = \sqrt{2}|b|$. Для равнобедренного треугольника с основанием y и боковыми сторонами x легко получить формулу радиуса описанной окружности $R = x^2/\sqrt{4x^2 - y^2}$, и для любой точки внутри треугольника существует вершина, расстояние до которой не больше R (т.к. в равнобедренном треугольнике с боковыми сторонами R расстояние до одной из двух боковых вершин не больше R). Значит, для доказательства деления с остатком достаточно проверить, что в нашем равнобедренном треугольнике $R < |b|$. Действительно, $x = \sqrt{2}|b|$, $y = |b|$, $R = 2|b|^2/(\sqrt{7})|b| = (2/\sqrt{7})|b| < |b|$. Далее аналогично получаем основную теорему арифметики.

Задача 12. а,б) Заметим, что норма $N(a + \sqrt{-d}b) = a^2 + db^2$ для делителя единицы должна быть равна 1, поэтому при $d > 1$ получаем

$b = 0$, значит $a = \pm 1$, т.е. все делители единицы — это ± 1. Если же $d = 1$, то $-1 \le a, b \le 1$, откуда перебором получаем, что все делители единицы — это ± 1 и $\pm i$.

в) Задача 8.

г) Докажем, что все делители единицы имеют вид $\pm(1+\sqrt{2})^n$ для всех целых n. Т.к. $(1+\sqrt{2})(1-\sqrt{2}) = -1$, то все такие числа — делители единицы. Предположим, что существует какой-то другой делитель единицы $a + b\sqrt{2}$. После домножения на -1 и сопряжения можно считать, что $a, b > 0$ (если $ab = 0$, то $a = \pm 1$ и $b = 0$ из $a^2 - 2b^2 = \pm 1$). Рассмотрим минимальный такой делитель единицы $a + b\sqrt{2}$ (с $a, b \ge 0$ и $a + b\sqrt{2} \ne \pm(1+\sqrt{2})^n$). Тогда $(a + b\sqrt{2})(\sqrt{2} - 1) = (2b - a) + (a - b)\sqrt{2}$. Докажем, что $a > b$ и $2b > a$. Действительно, заметим, что если $b = 1$, то $a^2 = 2 \pm 1$, откуда $a = 1$ и $a + b\sqrt{2} = 1 + \sqrt{2}$, противоречие. Значит, $b > 1$, поэтому $a^2 = 2b^2 \pm 1 > b^2$, откуда $a > b$. Если $a = 1$, то $2b^2 = 1 \pm 1$, откуда $b = 1$ и $a + b\sqrt{2} = 1 + \sqrt{2}$, противоречие. Значит, $a > 1$, поэтому $(2b)^2 = 2(a^2 \pm 1) > a^2$, откуда $2b > a$.

Отсюда получаем $0 < 2b - a < a$ и $0 < a - b < b$, поэтому $(2b - a) + (a - b)\sqrt{2} < a + b\sqrt{2}$, что противоречит минимальности $a + b\sqrt{2}$. Значит, все делители единицы имеют вид $\pm(1+\sqrt{2})^n$.

Задача 13. а,в) Будем доказывать деление с остатком по норме $N(a + b\sqrt{D}) = |a^2 - Db^2|$, где $D = 2$ или 3. Пусть $x = a + b\sqrt{D}$ и $y = c + d\sqrt{D}$, тогда $x/y = (a + b\sqrt{D})/(c + d\sqrt{D}) = (a + b\sqrt{D})(c - d\sqrt{D})/(c^2 - Dd^2) = ((ac - Dbd) + (bc - ad)\sqrt{D})/(c^2 - Dd^2) = n + m\sqrt{D} + (k + l\sqrt{D})/(c^2 - Dd^2)$, где n, m, k, l – целые, и $|k|, |l| \le |(c^2 - Dd^2)|/2$ (обычное деление с остатком $ac - Dbd$ и $bc - ad$ на $c^2 - Dd^2$). Значит, $a + b\sqrt{D} = (c + d\sqrt{D})(n + m\sqrt{D}) + (k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2)$, причем $(k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2) \in \mathbb{Z}[\sqrt{D}]$ и $N(k + l\sqrt{D}) = |k^2 - Dl^2| \le (3/4)(c^2 - Dd^2)^2$, поэтому $N((k + l\sqrt{D})(c + d\sqrt{D})/(c^2 - Dd^2)) = N(k + l\sqrt{D})N(c + d\sqrt{D})/N(c^2 - Dd^2) \le (3/4)N(c + d\sqrt{D}) < N(c + d\sqrt{D})$, из чего следует деление с остатком. Отсюда аналогично предыдущим случаям следует основная теорема арифметики.

б) Заметим, что $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$, причем $N(2) = N(1 + \sqrt{-3}) = N(1 - \sqrt{-3}) = 4$. Докажем, что $2, 1 + \sqrt{-3}$ и $1 - \sqrt{-3}$ — простые в $\mathbb{Z}[\sqrt{-3}]$. Для этого достаточно заметить, что $N(a + b\sqrt{-3}) = a^2 + 3b^2 \ne 2$ при целых a и b. Значит, $2, 1 + \sqrt{-3}$ и $1 - \sqrt{-3}$ не представимы в виде произведения двух чисел с неединичной нормой, поэтому они простые. Значит, разложение 4 на простые в $\mathbb{Z}[\sqrt{-3}]$ — не единственно.

г) Заметим, что $9 = 3 \cdot 3 = (2 + \sqrt{-5})(2 - \sqrt{-5})$, причем $N(3) = N(2 + \sqrt{-5}) = N(2 - \sqrt{-5}) = 9$. Аналогично получаем, что $3 \ne N(a + b\sqrt{-5}) = a^2 + 5b^2$, все числа в разложении 9 — простые, поэтому разложение не единственно.

д) Заметим, что $4 = 2 \cdot 2 = (\sqrt{5}+1)(\sqrt{5}-1)$, причем $N(2) = N(\sqrt{5}+1) = N(\sqrt{5}-1) = 4$. Так как $N(a+b\sqrt{5}) = a^2 - 5b^2 \equiv \pm 1 \mod 5$, то $\pm 2 \neq N(a+b\sqrt{5})$. Значит, все числа в разложении 4 — простые, поэтому разложение не единственно.

е) Заметим, что $9 = 3 \cdot 3 = (\sqrt{10}+1)(\sqrt{10}-1)$, причем $N(3) = N(\sqrt{10}+1) = N(\sqrt{10}-1) = 9$. Так как $N(a+b\sqrt{10}) = a^2 - 10b^2 \equiv \pm 1 \mod 5$, то $\pm 3 \neq N(a+b\sqrt{10})$. Значит, все числа в разложении 9 — простые, поэтому разложение не единственно.

ж) Аналогично пунктам а,в) нам достаточно показать, что если $|a|, |b| \leq 1/2$, то $|N(a+b\omega)| < 1$, где $\omega = \frac{1+\sqrt{5}}{2}$. Действительно, $a+b\omega = ((2a+b)+b\sqrt{5})/2$, поэтому $|N(a+b\omega)| = |((2a+b)^2-5b^2)/4| = |a^2+ab-b^2| \leq 3/4 < 1$.

з) Задача 11б.

и) Абсолютно аналогично случаю $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ получаем $R = \frac{3}{\sqrt{11}}|b| < |b|$, из чего следует деление с остатком и основная теорема арифметики.

к) Для $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ деление с остатком не выполняется, причем не только по стандартной норме, но и по любой (можете попробовать строго доказать это, рассмотрев число, не являющееся делителем единицы, с наименьшей нормой). Будем доказывать более слабое утверждение — что в $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$ все идеалы главные (см. следующую часть). Для ненулевого идеала I рассмотрим его элемент y с наименьшей (стандартной) нормой. Докажем, что для любого $x \in I$ мы можем поделить с остатком x или $2x$ на y. Аналогично с пунктами а,в,ж) $\omega = \frac{1+\sqrt{-19}}{2}$, $x = a+b\omega$ и $y = c+d\omega$, тогда $x/y = (a+b\omega)/(c+d\omega) = n_1 + m_1\omega + (z_1+t_1\omega))$, где n, m — целые, а $|z_1|, |t_1| \leq 1/2$; аналогично $2x/y = n_2 + m_2\omega + (z_2+t_2\omega))$ с $|z_2|, |t_2| \leq 1/2$. Заметим, что одно из $|t_1|$ и $|t_2|$ не больше $1/3$ (будем считать, что $|t_i| \leq 1/3$). Тогда $|N(z_i+t_i\omega)| = |z_i^2 + z_it_i + 5t_i^2| \leq 1/4 + 1/6 + 5/9 = 35/36 < 1$, откуда следует деление с остатком (попробуйте доказать это утверждение в геометрической интерпретации).

Предположим, что $I \neq (y)$, т.е. существует $x \in I$, не делящееся на y. Тогда $2x$ делится на y, поэтому $2x = (a+b\omega)y$ для целых a и b. Значит, существует $z \in I$, не делящееся на y, для которого $2z = (c+d\omega)y$, где $c = 0$ или -1, а d равно 0 или 1 (поделим на $2y$). Заметим, что $d \neq 0$, т.к. иначе $N(z) = N(-y/2) < N(y)$. Значит, $2z = \frac{\pm 1+\sqrt{-19}}{2}y$, поэтому $\frac{\mp 1+\sqrt{-19}}{2}z + 3y = y/2 \in I$, но $N(y/2) < N(y)$, противоречие. Значит, $I = (y)$, т.е. все идеалы главные.

Теперь для доказательства основной теоремы арифметики достаточно доказать, что если x не делится на простое p, то $ax + bp = 1$ для каких-то a и b. Действительно, рассмотрим идеал (x, p), который равен (z) для какого-то z. Значит, p делится на z, поэтому z равен $p\xi$ или ξ, где ξ — делитель единицы. В первом случае получаем, что x делится на p,

противоречие. Во втором случае получаем, что $1 \in (z) = (x, p)$, поэтому $1 = ax + bp$ для каких-то a и b. Далее доказательство основной теоремы арифметики повторяет задачу 2.

Задача 14. Для этого необходимо и достаточно, чтобы $\xi^2 = a\xi + b$ для целых a и b, то есть ξ является корнем приведенного квадратного многочлена с целыми коэффициентами.

Задача 15. а) Если n четно, то $2 = (3^{n/2} + k)(3^{n/2} - k)$, где $3^{n/2} + k$ и $3^{n/2} - k$ имеют одинаковую четность, противоречие. Значит, n не делится на 2.

Разложив обе части на множители в $\mathbb{Z}[\sqrt{-2}]$, получим $(1+\sqrt{-2})^n(1-\sqrt{-2})^n = (k+\sqrt{-2})(k-\sqrt{-2})$. Легко проверить, что $k+\sqrt{-2}$ и $k-\sqrt{-2}$ взаимно просты (т.к. 3^n не делится на 2), и $1 \pm \sqrt{-2}$ — различные простые. Отсюда из выполнения основной теоремы арифметики для $\mathbb{Z}[\sqrt{-2}]$ получаем, что $(1 + \sqrt{-2})^n = \pm k \pm \sqrt{-2}$. Если $(1 + \sqrt{-2})^n = \pm k - \sqrt{-2}$, то по модулю $1 - \sqrt{-2}$ получаем $(1 + \sqrt{-2})^n \equiv 2^n \equiv \pm k - \sqrt{-2} \equiv \pm k - 1$, поэтому $2^n + 1 \equiv \pm k$. Но n нечетно, поэтому $2^n + 1$ делится на $3 = (1 + \sqrt{-2})(1 - \sqrt{-2})$, поэтому и k делится на 3, что очевидно неверно.

Значит, $(1 + \sqrt{-2})^n = \pm k + \sqrt{-2}$, и приравнивая коэффициент при $\sqrt{-2}$, получаем

$$1 = \binom{n}{1} - 2\binom{n}{3} + 4\binom{n}{5} - \ldots \pm 2^{(n-1)/2}.$$

При $n = 1$ – $k = \pm 1$, при $n = 3$ — $k = \pm 5$. Докажем, что при $n \geq 5$ решений нет. Перепишем последнюю формулу:

$$0 = -\frac{(n+1)(n-1)(n-3)}{3} + 4\binom{n}{5} - 8\binom{n}{7} + \ldots \pm 2^{(n-1)/2}.$$

Теперь, аналогично задаче 3, докажем, $\frac{(n+1)(n-1)(n-3)}{3}$ и $2^k\binom{n}{2k+1}$ при $k > 2$ делятся на степень двойки большую, чем $4\binom{n}{5}$, из чего будет следовать противоречие. Для $\frac{(n+1)(n-1)(n-3)}{3}$ это очевидно, т.к. n на делится на 2 и $4\binom{n}{5} = \frac{n(n-1)(n-2)(n-3)(n-4)}{30}$. Перепишем второй тип слагаемых:

$$2^k\binom{n}{2k+1} = 4\binom{n}{5}\binom{n-5}{2k-4}\frac{15 * 2^{k-1}}{(2k-3)(2k-1)(2k+1)(k-1)k}.$$

Осталось заметить, что $2^{k-1} > k > k-1$ при $k > 2$, поэтому $2^{k-1}/(k(k-1))$ делится на 2, из чего следует наше утверждение.

б) Если n четно, то $7 = (2^{n/2}+k)(2^{n/2}-k)$, поэтому $2^{n/2} = 4$ и $k = \pm 3$, т.е. $n = 4, k = \pm 3$ – единственное решение при четном n. Далее считаем n нечетным.

Разложив обе части уравнения $2^{n-2} = (k^2+7)/4$ на множители в $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, получаем

$$((1+\sqrt{-7})/2)^{n-2}((1-\sqrt{-7})/2)^{n-2} = ((k+\sqrt{-7})/2)((k-\sqrt{-7})/2),$$

где $(1+\sqrt{-7})/2$ и $(1-\sqrt{-7})/2$ — различные простые, $(k+\sqrt{-7})/2$ и $(k-\sqrt{-7})/2$ – взаимно просты. Обозначим $m = n-2$, тогда из выполнения основной теоремы арифметики для $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ получаем, что $((1+\sqrt{-7})/2)^m = (\pm k \pm \sqrt{-7})/2$. Если $m = 1$, то $n = 3$ и $k = \pm 1$. Докажем, что если $m > 1$, то $((1+\sqrt{-7})/2)^m = (\pm k - \sqrt{-7})/2$. Действительно, иначе $((1+\sqrt{-7})/2)^m - ((1-\sqrt{-7})/2)^m = \sqrt{-7}$, и по модулю $(-3-\sqrt{-7})/2 = ((1-\sqrt{-7})/2)^2$ получаем, что $((1+\sqrt{-7})/2)^m - ((1-\sqrt{-7})/2)^m \equiv (-1)^m \equiv -1 \equiv \sqrt{-7}$, поэтому $1+\sqrt{-7} = ((1+\sqrt{-7})/2)^2(1-\sqrt{-7})/2)$ делится на $((1-\sqrt{-7})/2)^2$, противоречие.

Значит, $((1+\sqrt{-7})/2)^m = (\pm k - \sqrt{-7})/2$, и приравнивая коэффициенты при $\sqrt{-7}$ по модулю 7, получаем $-2^{m-1} \equiv m \mod 7$. Т.к. 2 является вычетом по модулю 7, то $m \equiv 3, 5, 6 \mod 7$, при этом $m \equiv 0, 2, 1 \mod 3$ соответственно. Значит, $m \equiv 3, 5, 13 \mod 21$, при этом $m = 3, 5, 13$ подходят — им соответствуют решения $n = 5, k = \pm 5$; $n = 7, k = \pm 11$; $n = 15, k = \pm 181$. Докажем, что это все решения.

Предположим противное, тогда $m \equiv m_0 \mod 21$, где $m_0 = 3, 5$ или 13, и $m > m_0$. Пусть $r = m - m_0$ делится на 7^α и не делится на $7^{\alpha+1}$. Тогда по модулю $7^{\alpha+1}$ получаем

$$(1+\sqrt{-7})^r = 1 + r\sqrt{-7} + \ldots + (\sqrt{-7})^l \binom{r}{l} + \ldots + (\sqrt{-7})^r \equiv 1 + r\sqrt{-7},$$

т.к. $l!$ делится на 7 в степени, меньшей $l/6 = l/7 + l/49 + \ldots$. Также $2^r \equiv (8)^{r/3} \equiv 1 \mod 7^{\alpha+1}$. Значит,

$$((1+\sqrt{-7})/2)^m = ((1+\sqrt{-7})/2)^{m_0}((1+\sqrt{-7})/2)^r \equiv ((k_0-\sqrt{-7})/2)(1+r\sqrt{-7}) \equiv$$

$$\equiv ((k_0+7r) + (k_0 r - 1)\sqrt{-7})/2 \equiv (k - \sqrt{-7})/2 \mod 7^{\alpha+1},$$

поэтому $k_0 r$ делится на $7^{\alpha+1}$. Но тогда k_0 делится на 7, противоречие (т.к. иначе 2^n делится на 7). Значит, других решений нет.

Задача 16. Мы будем использовать задачи 27 и 28.
а) В $\mathbb{Z}[\sqrt{-5}]$ имеется разложение $(x+\sqrt{-5})(x-\sqrt{-5}) = y^3$. Т.е. произведение идеалов $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ является кубом идеала (y). Если идеалы $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ не взаимно просты, то они имеют общий простой делитель I. Тогда идеал, порожденный $2\sqrt{-5} = (x+\sqrt{-5}) - (x-\sqrt{-5})$ делит I. Разложим $(2\sqrt{-5}) = (2, 1+\sqrt{-5})^2(\sqrt{-5})$. Т.е. $I = (2, 1+\sqrt{-5})$

или $I = (\sqrt{-5})$. В первом случае x нечетно, откуда $x^2+5 = y^3$ делится на 2, но не делится на 4, противоречие. Во втором случае x делится на 5, откуда $x^2+5 = y^3$ делится на 5, но не делится на 25, противоречие. Значит, идеалы $(x+\sqrt{-5})$ и $(x-\sqrt{-5})$ взаимно просты и каждый из них является кубом некоторого идеала. Используя задачу 28 нетрудно проверить, что куб неглавного идеала будет неглавным, откуда $(x+\sqrt{-5})$ — куб главного идеала. Т.е. $(x+\sqrt{-5}) = (a+b\sqrt{-5})^3$, поскольку делители единицы в $\mathbb{Z}[\sqrt{-5}]$ имеют вид ± 1 и являются кубами. Раскрывая скобки и приравнивая коэффициенты при $\sqrt{-5}$ получаем $(3a^2 - 5b^2)b = 3a^2b - 5b^3 = 1$. Отсюда $b = \pm 1$. Легко видеть, что оба случая невозможны. Следовательно, уравнение не имеет решений.

б) Заменяя x на $z-1$ получаем уравнение $z^2 + 6 = y^3$. Решений нет, доказательство аналогично пункту а).

в) Разложим $5x^2+1 = (1+x\sqrt{-5})(1-x\sqrt{-5}) = y^3$. Аналогично пункту а) x четно и идеалы $(1+x\sqrt{-5})$ и $(1-x\sqrt{-5})$ взаимно просты. Тогда $(1+x\sqrt{-5}) = (a+b\sqrt{-5})^3$. Раскрывая скобки и приравнивая вещественные части получаем $a(a^2-15b^2) = a^3-15ab^2 = 1$. Если $a = 1$, то $b = 0$, откуда $x = 0$, $y = 1$. Случай $a = -1$ невозможен. Т.е. $x = 0$, $y = 1$.

г) Заменяя x на $z-1$ получаем уравнение $6z^2 + 1 = y^3$. Решение единственно: $x = 0$, $y = 1$, доказательство аналогично пункту в).

д) Приведем решение, не использующее идеалы. Похожие решения есть и для пунктов а,б).

Прибавим 8 и разложим на множители: $x^2 + 2 = (y+2)(y^2-2y+4)$. Рассмотрев остатки по модулю 4 получим, что x нечетно, откуда $x^2 + 2 \equiv 3 \bmod 8$. Используем, что -2 является квадратичным невычетом по модулю простого p тогда и только тогда, когда $p \equiv 1$ или $3 \bmod 8$ (это следует, например, из квадратичного закона взаимности). Тогда все простые делители x^2+2 имеют вид $8k+1$ или $8k+3$, т.е. все делители $x^2+2 = (y+2)(y^2-2y+4)$ дают остатки 1 или 3 при делении на 8. Т.к. $y+2$ дает остаток 1 или 3 по модулю 8, то y дает остаток ± 1. Из этих двух случаев (y^2-2y+4) дает остаток 1 или 3 только если $y \equiv 1 \bmod 8$. Отсюда $x^2+2 = y^3+8 \equiv 1 \bmod 8$. Противоречие.

Упражнение 10. Очевидно.

Упражнение 11. Если $a, b \in I \cap J$, то $a+b \in I$, т.к. $a, b \in I$; аналогично $a+b \in J$. Отсюда $a+b \in I \cap J$.

Если $a \in I \cap J, b \in \mathbb{Z}$, то $ab \in I \cap J$ по аналогичной причине.

Задача 17. а,б) Следует из линейного представления НОД.

в) Пусть d — наименьшее натуральное число в идеале I (если такого нет, то $I = (0)$). Если $I \neq (d)$, то I содержит число a, не делящееся на d. Остаток от деления a на d лежит в I и меньше d. Противоречие.

Упражнение 12. Заметим, что (α) состоит из чисел вида αx, где

$x \in \mathbb{Z}[\omega]$, а также $(\alpha) \subset (\beta) \Leftrightarrow \alpha \in (\beta) \Leftrightarrow \alpha/\beta \in \mathbb{Z}[\omega]$. Имеем

$(\alpha) = (\beta) \Leftrightarrow \alpha \in (\beta)$ и $\beta \in (\alpha) \Leftrightarrow \alpha/\beta \in \mathbb{Z}[\omega]$ и $\beta/\alpha \in \mathbb{Z}[\omega] \Leftrightarrow \alpha/\beta$ – делитель единицы

Упражнение 13. Очевидно.

Задача 18. Заметим, что $(2, \sqrt{-14}) = \{x + y\sqrt{-14} \mid x$ четно, $y \in \mathbb{Z}\}$ (проверьте!) Отсюда имеем, что, $1 \notin (2, \sqrt{-14}))$ и $(2, \sqrt{-14}) \neq (2)$. Предположим, что $(2, \sqrt{-14}) = (\alpha)$. Тогда $2 = \alpha x$, $x \in \mathbb{Z}[\sqrt{-14}]$, откуда $4 = N(2) = N(\alpha)N(x)$.
Если $N(\alpha) = 1$, то $1 = \alpha\bar{\alpha} \in (\alpha)$, т.е. $(1) \in (\alpha) = (2, \sqrt{-14})$, противоречие.
$N(\alpha) \neq 2$, т.к. уравнение $x^2 + 14y^2 = 2$ не имеет решений в целых числах.
Если $N(\alpha) = 4$, то $N(\sqrt{-14}) = 14$ не делится на $N(\alpha)$, т.е. $\sqrt{-14} \notin (\alpha)$.

Задача 19. Пусть α — наименьшее натуральное число в I, $\beta = a + b\omega$ — число с наименьшим положительным коэффициентом b при ω. Несложно проверить, что $I = (\alpha, \beta)$.

Упражнения 14-15. Вычисления, не приводим.

Упражнение 16. Из упражнения 13 достаточно найти ответ в $\mathbb{Z}$: (360), (2), (180).

Упражнение 17. Вычисления, мы приведем доказательство для $I + J$. Если $a, b \in I + J$, то $a = i_1 + j_1$, $b = i_2 + j_2$, где $i_1, i_2 \in I$, $j_1, j_2 \in J$. Тогда $a + b = (i_1 + i_2) + (j_1 + j_2) \in I + J$, т.к. $i_1 + i_2 \in I$, $j_1 + j_2 \in J$.
Для $c \in \mathbb{Z}[\omega]$ имеем $ac = (i_1 + j_1)c = i_1c + j_1c \in I + J$, т.к. $i_1c \in I$, $j_1c \in J$.

Задача 20. Поскольку $N(a_i)$ и $\mathrm{Tr}(a_i\bar{a}_j)$ — целые числа, то имеем $(N(a_i), \mathrm{Tr}(a_i\bar{a}_j))_{1 \leq i,j \leq n} = (a)$, где $a = \text{НОД}(N(a_i), \mathrm{Tr}(a_i\bar{a}_j))$. Заметим, что $N(a_i)$ и $\mathrm{Tr}(a_i\bar{a}_j)$ делятся на a. Т.к. $N(a_i) = a_i\bar{a}_i$ и $\mathrm{Tr}(a_i\bar{a}_j) = a_i\bar{a}_j + a_j\bar{a}_i$, то

$$(a) = (N(a_i), \mathrm{Tr}(a_i\bar{a}_j))_{1 \leq i,j \leq n} \subset (a_1, ..., a_n)(\bar{a}_1, ..., \bar{a}_n)$$

Достаточно доказать, что $a_i\bar{a}_j \in (a)$ для всех $1 \leq i, j \leq n$, т.е. что $a_i\bar{a}_j/a$ — целое алгебраическое. По упражнению 6 достаточно показать, что его норма и след целые. $N(a_i\bar{a}_j/a) = \frac{a_i\bar{a}_j a_j\bar{a}_i}{a^2} = \frac{N(a_i)N(a_j)}{a^2}$ целое, т.к. $N(a_i)$ и $N(a_j)$ делятся на a. $\mathrm{Tr}(a_i\bar{a}_j/a) = \mathrm{Tr}(a_i\bar{a}_j)/a$ целое, т.к. $\mathrm{Tr}(a_i\bar{a}_j)$ делится на a.

Задача 21. Если I делится на J, то $I = JH \subset J$.
Пусть $I \subset J$. По задаче 20 (которая применима, т.к. $J = (\alpha, \beta)$ по задаче 19) имеем $J\bar{J} = (a)$, т.е. $I\bar{J} \subset J\bar{J} = (a)$. Тогда все элементы $I\bar{J}$ делятся на a, откуда $H = I\bar{J}/a = \{x/a \mid x \in I\bar{J}\}$ — идеал. Получаем $JH = (I\bar{J}/a)J = (I\bar{J}J)/a = (I(a))/a = I$, т.е. I делится на J.

Упражнение 18. Доказано в решении задачи 20.

Задача 22. По задаче 21 достаточно доказать, что

$$I \subset H \text{ и } J \subset H \Leftrightarrow I + J \subset H$$

Из левого следует правое, поскольку H замкнут относительно сложения; из правого левое — поскольку $I, J \subset I + J$.

Упражнение 19. $(a)\overline{(a)} = (a\bar{a}) = (N(a)) = (|N(a)|)$ и $|N(a)| \geq 0$, т.е. $N((a)) = |N(a)|$.

Упражнение 20. Т.к. $N(I)N(J) \geq 0$, то достаточно показать, что $(N(I)N(J)) = I\overline{IJ}$. Но $(N(I)N(J)) = (N(I))(N(J)) = I\bar{I}J\bar{J} = I\overline{IJ}$.

Упражнение 21. Если $J = IH$, то $N(J) = N(I)N(H)$ по упражнению 20, откуда $N(I)$ делит $N(J)$.

Упражнение 22. Если $I = (1)$, то $(N(I)) = I\bar{I} = (1)$, т.е. $N(I) = 1$. Если $N(I) = 1$, то $1 \in I\bar{I} \subset I$, т.е. $I = (1)$.

Упражнение 23. Идеал I прост $\Leftrightarrow$ любой идеал, делящий I, совпадает либо с I, либо с (1) $\Leftrightarrow$ (по задаче 21) любой идеал, содержащий I, совпадает либо с I, либо с (1) $\Leftrightarrow$ идеал I максимален.

Упражнение 24. Пусть p_1, p_2 — различные простые идеалы. По упражнению 23 ни один из них не содержится в другом. Тогда $p_1 + p_2$ — идеал, содержащий каждый из них и не совпадающий ни с одним из них. По упражнению 23 получаем $p_1 + p_2 = (1)$.

Задача 23. Заметим, что если $N(I)$ — простое число, то I — простой идеал (по упражнениям 21 и 22) и вычислим нормы: $N(p_1) = N(p_2) = 3$, $N(p_3) = N(p_4) = 5$.

Задача 24. Используем индукцию по $N(I)$ и упражнение 20.

Задача 25. По задаче 21 мы знаем, что $JH \subset I$ и хотим доказать что $H \subset I$. Пусть $h \in H$. Т.к. $I + J = (1)$, то найдутся $i \in I$, $J \in J$, что $i + j = 1$. Тогда $jh \in JH \subset I$ и по определению идеала $ih \in I$. Значит, $h = jh + ih \in I$, что и требовалось.

Задача 26. Пункт а) очевиден.
б) $HI = HJ \Rightarrow (N(H))I = H\bar{H}I = H\bar{H}J = (N(H))J$. Теперь применим пункт а) для $a = N(H)$.

Задача 27. Предположим, что какой-то идеал имеет два различных разложения на простые идеалы. Если какой-то простой идеал встречается в обоих разложениях, то на него по предыдущей задаче можно сократить. Будем сокращать, пока не получим два разложения идеала $p_1...p_n = I = q_1...q_n$ на простые идеалы, такое что все q_i отличны от p_1. Тогда p_1 делит $q_1...q_{n-1}q_n$; p_1 и q_n взаимно просты по упражнению 24. По задаче 25 p_1 делит $q_1...q_{n-1}$. Используем индукцию и получаем противоречие.

Задача 28. а) Пусть $I \subset \mathbb{Z}[\sqrt{-5}]$ — идеал, $x \in I$ — элемент с минимальной ненулевой нормой. Числа, кратные x, образуют на комплексной плоскости решетку из прямоугольников со сторонами 1 и $\sqrt{5}$. Если I не содержит других чисел, то I главный. Пусть $y \in I$, причем y не делится

на x. После параллельного переноса на число, кратное x, можно считать, что y лежит в прямоугольнике с вершинами 0, x, $(1+\sqrt{-5})x$, $\sqrt{-5}x$. Мнимая часть y/x лежит между 0 и $\sqrt{5}$. Если она меньше $\sqrt{3}/2$ или больше $\sqrt{5}-\sqrt{3}/2$, то расстояние от y до одной из вершин прямоугольника меньше $|x|$, что невозможно. Поэтому $\frac{\sqrt{3}}{2} \le \operatorname{Im}\frac{y}{x} \le \sqrt{5}-\frac{\sqrt{3}}{2}$. Значит, $\sqrt{5}-\frac{\sqrt{3}}{2} < \sqrt{3} \le 2\operatorname{Im}\frac{y}{x} \le 2\sqrt{5}-\sqrt{3} < \sqrt{5}+\frac{\sqrt{3}}{2}$. Отсюда следует, что расстояние от $2y$ до одного из чисел $\sqrt{-5}x$, $(1+\sqrt{-5})x$, $(2+\sqrt{-5})x$ меньше $|x|$, т.е. должно равняться нулю. Значит, y равняется $\sqrt{-5}x/2$, $(1+\sqrt{-5})x/2$, либо $(2+\sqrt{-5})x/2$. В первом и третьем случае $-5x/2 \in I$, откуда $x/2 \in I$, что невозможно. То есть $y = (1+\sqrt{-5})x/2$ и $I = ((1+\sqrt{-5})a, 2a)$, где $a = x/2$.

б) Взяв x и y аналогично пункту а) получим, что y равняется $\sqrt{-6}x/2$, $(1+\sqrt{-6})x/2$, либо $(2+\sqrt{-6})x/2$. Во втором случае $\sqrt{-6}(1+\sqrt{-6})x/2 = \sqrt{-6}x/2 - 3x \in I$, откуда $\sqrt{-6}x/2 \in I$, откуда $x/2 = (1+\sqrt{-6})x/2 - \sqrt{-6}x/2 \in I$, что невозможно. В первом и третьем случае получаем $I = (\sqrt{-6}a, 2a)$, где $a = x/2$.

Задача 29. Пусть $0 \ne a \in I$. Тогда $0 \ne a\bar{a} \in I \cap \mathbb{Z}$.

Задача 30. Пусть p — минимальное натуральное число в I, которое существует по предыдущей задаче. Если $p = ab$, где a, b натуральные, то $(a)(b) = (ab)$ содержится в I, т.е. по задаче 21 $(a)(b)$ делится на I, но (a) и (b) не делятся на I. Противоречие.

Задача 31. Возьмем p из предыдущей задачи. $(p) \subset I$, т.е. по задаче 21 (p) делится на I, откуда $N((p)) = p^2$ делится на $N(I)$. По упражнению 22 $N(I) \ne 1$, откуда $N(I)$ равняется p или p^2.

Задача 32. Следует из решения предыдущей задачи.

Задача 33. Если идеал $(p) \subset \mathbb{Z}[\omega]$ не прост, то $(p) = IJ$, где I, J отличны от (1). тогда $N(I)N(J) = N((p)) = p^2$, т.е. $N(I) = p$, откуда $I\bar{I} = (N(I)) = (p)$, что и требовалось.

Задача 34. Предположим, что $0 \le a < p$ является решением уравнения $P_\omega(a) \equiv 0 \bmod p$. Заметим, что $P_\omega(a) = (a-\omega)(a-\bar{\omega})$ делится на p. Тогда $(p, a-\omega)\overline{(p, a-\omega)} = (p^2, p(a-\omega), p(a-\bar{\omega}, (a-\omega)(a-\bar{\omega})) \subset (p)$, откуда $(p) \ne (p, a-\omega) \ne (1)$, при этом $(p, a-\omega)$ содержит (p), т.е. делит (p). Значит, (p) не прост.

В обратную сторону, если (p) не прост, то $(p) = I\bar{I}$, причем $p \in I$. Т.к. $p \in I$, то $p\omega \in I$. Т.к. $I \ne (p)$, то I содежит элемент $x + y\omega$, в котором y не делится на p. Применяя алгоритм Евклида к y и p, получим, что I содержит элемент $b + \omega$ для некоторого $b \in \mathbb{Z}$. Тогда для $a = -b$ имеем $a - \omega \in I$. Из решения задачи 19 следует, что $I = (p, a-\omega)$. Т.к. $(p, a-\omega)\overline{(p, a-\omega)} = (p)$, то $P_\omega(a) = (a-\omega)(a-\bar{\omega})$ делится на p, т.е. a является решением уравнения $P_\omega(a) \equiv 0 \bmod p$.

Задача 35. Предположим противное, то есть существуют рациональное $a = p/q$, где $q > 1$ и $\gcd(p, q) = 1$, и приведённый многочлен $P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0$ с целыми коэффициентами такой, что $P(a) = 0$. Тогда $q^nP(a) = p^n + a_{n-1}p^{n-1}q + \ldots + a_1pq^{n-1} + a_0q^n = p^n + q(a_{n-1}p^{n-1} + \ldots + a_1pq^{n-2} + a_0q^{n-1}) = 0$, значит, p^n делится на q. Но $gcd(p, q) = 1$, противоречие.

Задача 36. Пусть $a, b \in \bar{\mathbb{Q}}$, тогда существуют приведённые многочлены $P(x), Q(x)$ с рациональными коэффициентами такие, что $P(a) = Q(b) = 0$. Пусть $P(x) = (x - \alpha_1)(x - \alpha_2)\ldots(x - \alpha_n)$ и $Q(x) = (x - \beta_1)(x - \beta_2)\ldots(x - \beta_m)$, где $\alpha_1, \alpha_2 \ldots \alpha_n$ и $\beta_1, \beta_2 \ldots \beta_m$ – корни $P(x)$ и $Q(x)$ соответственно, причем $a = \alpha_1$ и $b = \beta_1$. Тогда коэффициентами $P(x)$ и $Q(x)$ будут (с точностью до знака) элементарные симметрические многочлены от $\alpha_1, \alpha_2 \ldots \alpha_n$ и $\beta_1, \beta_2 \ldots \beta_m$ соответственно. Докажем, что $a + b \in \bar{\mathbb{Q}}$. Заметим, что $a + b$ является корнем многочлена $R(x) = \prod\limits_{\substack{1\le i\le n\\ 1\le j\le m}} (x - \alpha_i - \beta_j)$, коэффициенты которого есть многочлены от $\alpha_1 \ldots \alpha_n, \beta_1 \ldots \beta_m$ с рациональными коэффициентами. Из того, что для любых $1 \le i, j \le n$ при перестановке α_i и α_j многочлен $R(x, \alpha_1, \ldots, \beta_m)$ сохраняется, следует, что коэффициенты $R(x)$ – многочлены от $\beta_1 \ldots \beta_m$, коэффициенты которых есть симметрические многочлены от $\alpha_1 \ldots \alpha_n$ с рациональными коэффициентами.

Из основной теоремы о симметрических многочленах и того, что элементарные симметрические многочлены от $\alpha_1, \alpha_2 \ldots \alpha_n$ — рациональные коэффициенты $P(x)$, следует, что коэффициенты $R(x)$ — многочлены от $\beta_1 \ldots \beta_m$ с рациональными коэффициентами. Повторяя последнее рассуждение для $\beta_1 \ldots \beta_m$, получаем, что коэффициенты $R(x)$ — симметрические многочлены от $\beta_1 \ldots \beta_m$ с рациональными коэффициентами, и, как следует из теоремы и рациональности элементарных симметрических многочленов от $\beta_1 \ldots \beta_m$, они рациональны. Значит, $R(x)$ имеет рациональные коэффициенты и корень $a + b$, поэтому $a + b \in \bar{\mathbb{Q}}$.

Доказательство $ab \in \bar{\mathbb{Q}}$ дословно повторяет доказательство для $a+b$ с заменой $R(x)$ на $\prod\limits_{\substack{1\le i\le n\\ 1\le j\le m}} (x-\alpha_i\beta_j)$. Осталось заметить, что $-b$ и $1/b$ являются корнями многочленов $Q(-x)$ и $x^mQ(1/x)$ с рациональными коэффициентами соответственно, поэтому $a - b = a + (-b) \in \bar{\mathbb{Q}}$ и $a/b = a(1/b) \in \bar{\mathbb{Q}}$.

Задача 37. Будем считать $a_n \neq 0$. Пусть a_i — корень приведённого многочлена рациональными коэффициентами $P_i(x) = \prod\limits_{1\le j\le n_i} (x - \alpha_{ij})$, причем $a_i = \alpha_{i1}$ и все $\alpha_{nj} \neq 0$ (иначе поделим $P_n(x)$ на x в максимальной возможной степени). Рассмотрим все наборы $J = (j_0, j_1, \ldots, j_n)$ из

$n+1$ натурального числа с $1 \le j_k \le n_k$, и многочлен $R(x) = \prod\limits_J (\alpha_{nj_n} x^n + \alpha_{n-1j_{n-1}} x^{n-1} + \dots \alpha_{1j_1} x + \alpha_{0j_0})$. Тогда $R(x)$ делится на $a_n x^n + \dots a_1 x + a_0$, и, следовательно, $R(b) = 0$. Теперь, аналогично решению задачи 36, заметим, что из того, что многочлен $R(x)$ сохраняется при перестановках α_{ki} и α_{kj}, следует, что коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i \le n$, $0 \le j \le n_i$ с рациональными коэффициентами, причем для любого i — они симметрические от α_{ij} , $1 \le j \le n_i$.

Теперь индукцией по $k \le n+1$ покажем, что коэффициенты $R(x)$ — многочлены от α_{ij}, $0 \le i \le n-k$, $0 \le j \le n_i$ с рациональными коэффициентами, причем для $0 \le i \le n-k$ — они симметрические от α_{ij} , $1 \le j \le n_i$. База $k = 0$ — указана выше, переход от k к $k+1$ при $k \le n$ — по предположению индукции коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i < n-k$, $1 \le j \le n_i$ с коэффициентами – симметрическими многочленами с рациональными коэффициентами от α_{n-kj}, $1 \le j \le n_{n-k}$, причем для $0 \le i < n-k$ — они симметрические от α_{ij} , $1 \le j \le n_i$. Из теоремы 1 и рациональности коэффициентов $P_{n-k}(x)$ следует, что коэффициенты коэффициентов $R(x)$ как многочленов от α_{ij}, $0 \le i < n-k$, $1 \le j \le n_i$ — рациональны. Значит, коэффициенты $R(x)$ – многочлены от α_{ij}, $0 \le i \le n-k-1$, $1 \le j \le n_i$ с рациональными коэффициентами, причем для $0 \le i \le n-k-1$ — они симметрические от α_{ij} , $1 \le j \le n_i$ — переход доказан.

При $k = n+1$ получаем, что коэффициенты $R(x)$ рациональны, и $R(x) \ne 0$, т.к. все $\alpha_{nj} \ne 0$. Значит, b является корнем ненулевого многочлена с рациональными коэффициентами, поэтому $b \in \bar{\mathbb{Q}}$.

Задача 38. а) Для нормы $N(P) = \deg(P)$ делением с остатком будет обычное деление многочленов столбиком.

б) В данном случае делителями единицы будут ненулевые рациональные числа, а простыми — неприводимые непостоянные многочлены. Какое-то разложение на простые можно получить делением многочлена на простые меньшей степени (пока это возможно). Предположим, что у какого-то многочлена R есть два различных (с точностью до домножения на единицы) разложения на простые $R = P_1 P_2 \dots P_n = Q_1 Q_2 \dots Q_m$. Сократив на одинаковые (с точностью до домножения на делители единицы) простые в разложениях, получим, что для какого-то P_i выполнено $P_i | Q'_1 Q'_2 \dots Q'_k$, где $Q'_1 Q'_2 \dots Q'_k$ — оставшиеся простые в правой части. Пусть α — корень P_i, тогда $Q'_1(\alpha) Q'_2(\alpha) \dots Q'_k(\alpha) = 0$, значит $Q'_j(\alpha) = 0$ для какого-то j. Но тогда P_i и Q'_i делятся на минимальный многочлен для α, неприводимы и различны (с точностью до домножения на делители единицы), противоречие. Значит, разложение единственно.

Задача 39. Для многочлена $P(x)$ с рациональными коэффициентами

определим его содержание C_P как положительное рациональное число, такое, что все коэффициенты многочлена $P(x)/C_P$ целые, и их наибольший общий делитель равен 1. Такое число существует, т.к. $P(x)$ можно сначала умножить на наименьшее общее кратное знаменателей всех его коэффициентов, а потом поделить на наибольший общий делитель всех коэффициентов — тогда у получившегося многочлена будут целые коэффициенты с наибольшим общим делителем, равным 1. При этом получившийся многочлен перестает иметь целые коэффициенты при умножении на нецелое рациональное число x/y (т.к. если y делится на простое p, то существует коэффициент a_i, не делящийся на p, поэтому $a_i(x/y)$ не будет целым), и перестает иметь тривиальный наибольший общий делитель всех коэффициентов при умножении на целое число, не равное ± 1. Из этого следует, что такое C_P единственно, поэтому оно корректно определено.

Как видно из определения, достаточно доказать, что если P и Q имеют целые коэффициенты с тривиальным наибольшим общим делителем (то есть $C_P = C_Q = 1$), то их произведение PQ обладает тем же свойством ($C_{PQ} = 1$). Предположим противное, тогда существует простое p, делящее все коэффициенты PQ. Пусть $P(x) = a_n x^n + \dots a_0$ и $Q(x) = b_m x^m + \dots b_0$, и пусть k и r — наименьшие неотрицательные целые числа, такие, что a_k и b_r не делятся на p (такие k и r существуют, иначе p делит все коэффициенты $P(x)$ или $Q(x)$). Тогда коэффициент при x^{k+r} у PQ равен сумме $a_0 b_{k+r} + a_1 b_{k+r-1} + \dots + a_k b_r + \dots + a_{k+r} b_0$, все слагаемые которой, кроме $a_k b_r$, делятся на p из минимальности k и r. Значит, этот коэффициент у PQ не делится на p, противоречие.

Задача 40. Деление с остатком в многочленах с целыми коэффициентами по степени уже не работает (x не делится с остатком на $2x$), но верна единственность разложения — из задачи 38 следует, что любые два разложения на простые в целых числах отличаются домножением на рациональные. Все наибольшие общие делители непостоянных многочленов разложения равны 1, значит по лемме Гаусса многочлены в двух разложениях совпадают с точностью ± 1, поэтому разложения одинаковы.

Как мы видели, из наличия деления с остатком следует, что любой идеал главный. В множестве многочленов от переменной x с целыми коэффициентами имеется не главный идеал $(2, x)$, а в множестве многочленов от двух переменных x, y имеется не главный идеал (x, y).

Задача 41. Поделив с остатком $Q(x)$ на $P_a(x)$, мы получим $Q(x) = R(x)P_a(x) + T(x)$, где $R(x)$ и $T(x)$ — многочлены с рациональными коэффициентами, причем $deg(T) < deg(P_a)$, поэтому $T(a) \neq 0$ при $T(x) \neq 0$. Но подставив $x = a$, получим $Q(a) = 0 = R(a)P_a(a) + T(a) = T(a)$, значит

$T(x) = 0$ и $Q(x) = R(x)P_a(x)$, поэтому $Q(x)$ делится на $P_a(x)$.

Задача 42. Доказательство повторяет доказательство задачи 36 с учетом того, что симметрический многочлен с целыми коэффициентами представляется как многочлен с целыми коэффициентами от элементарных симметрических.

Задача 43. Достаточно доказать, что $\frac{1}{b} \in \mathbb{Q}[a_1, ..., a_n]$. Как следует из задачи 36, b — алгебраическое. Пусть $P(x) = c_n x^n + \ldots + c_1 x + c_0$ — минимальный приведенный многочлен с рациональными коэффициентами для b, тогда $c_0 \neq 0$ минимальности, поэтому $\frac{1}{b} = -\frac{c_n}{c_0} b^{n-1} - \ldots - \frac{c_1}{c_0} \in \mathbb{Q}[a_1, ..., a_n]$.

Задача 44. Пусть a является корнем приведённого многочлена $P(x)$ с целыми коэффициентами, по задаче 41 имеем $P(x) = R(x)Q(x)$, где $R(x)$ — приведённый многочлен с рациональными коэффициентами (т.к. P и Q — приведённые). Заметим, что $C_P = 1$, т.к. он приведённый с целыми коэффициентами, и $1/C_Q$ и $1/C_R$ — натуральные, т.к. они приведённые. По лемме Гаусса $(1/C_Q)(1/C_R) = 1$, поэтому $C_Q = C_R = 1$, значит $Q(x)$ имеет целые коэффициенты.

Также можно было заметить, что коэффициенты $Q(x)$ — многочлены от корней $P(x)$ с целыми коэффициентами, поэтому они целые алгебраические. Но т.к. $Q(x)$ имеет рациональные коэффициенты, то по задаче 35 — они целые.

Задача 45. Пусть $\alpha_1, \ldots, \alpha_n$ — корни многочлена $P(x) = (x-\alpha_1)(x-\alpha_2)\ldots(x-\alpha_n)$ с целыми коэффициентами, причем $|\alpha_1| = \ldots = |\alpha_n| = 1$. Тогда заметим, что $P_k(x) = (x-\alpha_1^k)(x-\alpha_2^k)\ldots(x-\alpha_n^k)$ также имеет целые коэффициенты (т.к. они являются симметрическими многочленами от $\alpha_1, \ldots, \alpha_n$ с целыми коэффициентами), и его корни по модулю равны 1. Заметим, что по теореме Виета коэффициент $P_k(x)$ при x^{n-m} не превосходит по модулю $\binom{n}{m}$. Значит, наборы коэффициентов $P_k(x)$ принимают конечное число значений, поэтому какой-то из этих наборов встречается бесконечное число раз при натуральных k. Из единственности разложения многочлена на линейные множители в комплексных числах следует, что для бесконечного числа k набор $\{\alpha_1^k, \ldots, \alpha_n^k\}$ равен какому-то набору $\{\beta_1, \ldots, \beta_n\}$ с точностью до перестановки. Значит, для каких-то различных k_1 и k_2 — $\alpha_i^{k_1} = \alpha_i^{k_2}$ для всех i (из конечности числа перестановок), поэтому $\alpha_i^{k_1-k_2} = 1$ для всех i. Значит, все корни $P(x)$ — корни из 1, ч.т.д.

Задача 46. Достаточно проверить транзитивность — пусть $A \sim B$ и $B \sim C$, тогда $(a)A = (b)B$ и $(d)B = (c)C$, поэтому $(ad)A = (bc)C$ и $A \sim C$.

Задача 47. Если все идеалы главные, то для любых двух идеалов (α) и (β) — $(\beta)(\alpha) = (\alpha)(\beta)$, поэтому $(\alpha) \sim (\beta)$, т.е. все идеалы эквивалентны.

Обратно, если число классов равно 1, то любой идеал I эквивалентен (1), поэтому $(\alpha) = I(\beta)$. Значит, $\alpha = i\beta$ для какого-то $i \in I$, поэтому $I = (\alpha/\beta) = (i)$, т.е. все идеалы главные.

Задача 48. Если $(a)I_1 = (b)I_2$ и $(c)J_1 = (d)J_2$, то $(ac)I_1J_1 = (bd)I_2J_2$, поэтому $I_1J_1 \sim I_2J_2$.

Задача 49. По задаче 28 в обоих случаях есть 2 различных класса — (a) и $((1+\sqrt{-5})a, 2a)$ в $\mathbb{Z}[\sqrt{-5}]$, и (a) и $(\sqrt{-6}a, 2a)$ в $\mathbb{Z}[\sqrt{-6}]$ (для таких a, что это идеал). Обозначим главные идеалы — 0-ым классом, а оставшийся класс — 1-ым. Тогда произведение 0-ых — 0-ой, произведение 0-ого на 1-ого — 1-ый, а произведение 1-ых — 0-ой, т.к. $((1+\sqrt{-5})a, 2a)((1+\sqrt{-5})b, 2b) = ((-4+2\sqrt{-5})ab, (2+2\sqrt{-5})ab, 4ab) = (2ab)$ и $(\sqrt{-6}a, 2a)(\sqrt{-6}b, 2b) = (-6ab, 2\sqrt{-6}ab, 4ab) = (2ab)$. Значит, умножение классов устроено так же, как сложение по модулю 2.

Задача 50. Это множество лежит в $\widetilde{\mathbb{Z}}$, замкнуто относительно сложения и умножения на $\widetilde{\mathbb{Z}}$ (т.к. I — идеал), поэтому $(1/\alpha)I$ — идеал.

Задача 51. Пусть $P_\alpha(x)$ — минимальный приведенный многочлен для α степени n, тогда набор $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ является базисом в $\mathbb{Q}[\alpha]$, т.к. любой многочлен сравним с многочленом степени меньше n по модулю $P(x)$, и если два различных многочлена от α степени меньше n равны, то $P(x)$ — не минимальный.

Задача 52. Аналогично, пусть $P_i(x)$ — минимальный приведенный многочлен для α_i степени n_i, тогда набор одночленов $\alpha_1^{r_1}\alpha_2^{r_2}\ldots\alpha_k^{r_k}$, где $0 \le r_i < n_i$ — позволяет представить любой элемент $\widetilde{\mathbb{Q}}$ в виде суммы элементов набора с рациональными коэффициентами. Предположим, что какой-то элемент $\widetilde{\mathbb{Q}}$ можно представить таким образом двумя различными способами. Тогда из равенства этих сумм следует, что какой-то элемент набора можно выразить в виде суммы остальных (с рациональными коэффициентами) — выкинем этот элемент из набора. Будем продолжать эту операцию, пока возможно — элементов в наборе конечное число, поэтому этот процесс закончится, и мы получим набор, для которого любой элемент $\widetilde{\mathbb{Q}}$ единственным образом представляется в виде суммы элементов набора с рациональными коэффициентами. Значит, мы получили базис $\widetilde{\mathbb{Q}}$ над $\mathbb{Q}$.

Задача 53. Пусть α является корнем многочлена с целыми коэффициентами $P(x) = a_m x^m + \ldots + a_0$ (возьмем минимальный многочлен и умножим на НОК знаменателей всех коэффициентов). Тогда $a_m^{m-1}P(x) = (a_m x)^m + a_{m-1}(a_m x)^{m-1} + \ldots + a_1 a_m^{m-2}(a_m x) + a_0 a_m^{m-1}$, поэтому число $a_m\alpha$ является корнем многочлена с целыми коэффициентами.

Задача 54. Для начала заметим, что для любого $\alpha \in \widetilde{\mathbb{Q}}$ существует целое ненулевое n, такое что $n\alpha \in I$. Действительно, пусть $\beta \in I$,

$\beta \neq 0$, тогда для β/α существует такое n, что $n\alpha/\beta \in \widetilde{\mathbb{Z}}$, значит $n\alpha = (n\alpha/\beta)\beta \in I$. Отсюда следует, что взяв произвольный базис $\widetilde{\mathbb{Q}}$ над $\mathbb{Q}$ и умножив его элементы на натуральные числа, мы сможем получить базис, элементы которого лежат в I. Возьмем такой базис $\beta_1, \ldots, \beta_n$, тогда каждый элемент $\alpha \in I$ единственным образом записывается в виде $\alpha = x_1\beta_1 + \ldots + x_n\beta_n$, где $x_1, \ldots, x_n$ - рациональные (набор $(x_1, \ldots, x_n)$ будем называть координатами α).

Для каждого $\alpha \in I$ рассмотрим набор его координат по модулю 1, то есть $(\{x_1\}, \{x_2\}, \ldots, \{x_n\})$, являющийся координатами $\alpha - \lfloor x_1 \rfloor \beta_1 - \lfloor x_2 \rfloor \beta_2 - \ldots - \lfloor x_n \rfloor \beta_n \in I$. Как видно из определения, все такие наборы лежат в единичном кубе размерности n. Если таких различных наборов конечное число, то возьмем соответствующие им $\alpha_1, \ldots, \alpha_m \in I$, тогда набор $\beta_1, \ldots, \beta_n, \alpha_1, \ldots, \alpha_m$ — удовлетворяет утверждению задачи.

Предположим, что таких различных наборов бесконечно много. Тогда существует $\alpha \in I$ со сколь угодно маленькими по модулю всеми координатами. Действительно, для любого натурального N разобьем единичный куб на N^n меньших кубов со стороной $1/N$. Из бесконечности числа различных наборов — в каком-то меньшем кубе найдутся 2 различных набора $(x_1, \ldots, x_n)$ и $(y_1, \ldots, y_n)$, тогда $(y_1 - x_1, \ldots, y_n - x_n)$ — координаты какого-то $\alpha \in I$, причем $|y_i - x_i| \leq 1/N$ для всех i. Но N можно выбрать сколь угодно большим (т.е. $1/N$ — сколь угодно маленьким), из чего следует наше утверждение.

Осталось доказать, что у $\alpha \in I$ не могут все координаты быть сколь угодно малыми по модулю. Пусть $P_i(x)$ – минимальный приведенный многочлен с целыми коэффициентами для β_i, и $\beta_{i1}, \beta_{i2}, \ldots, \beta_{in_i}$ – его корни. Рассмотрим все наборы $J = (j_1, \ldots, j_n)$ из $n+1$ натурального числа с $1 \leq j_k \leq n_k$, и многочлен $R(t, x_1, \ldots, x_n) = \prod_J (t - (x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}))$. Этот многочлен сохраняется при перестановках β_{ij} и β_{ik}, поэтому (аналогично с решением задачи 6) он имеет целые коэффициенты. Рассмотрим ненулевое $\alpha \in I$ и подставим в $R(t, x_1, \ldots, x_n)$ его координаты — получим приведенный многочлен $R_\alpha(t)$ с рациональными коэффициентами с корнем α. Значит, $R_\alpha(t)$ делится на минимальный приведенный многочлен $Q_\alpha(t)$ с целыми коэффициентами. В частности, произведение каких-то $x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}$ с точностью до знака совпадает со свободным членом $Q_\alpha(t)$, т.е. равно целому ненулевому числу. Пусть $\epsilon = 1/(n \max_{i,j}(|\beta_{ij}|))$, тогда если $|x_i| < \epsilon$ для всех i, то для всех J — $|x_1\beta_{1j_1} + x_2\beta_{2j_2} + \ldots + x_n\beta_{nj_n}| < 1$, поэтому и модуль их произведения < 1. Но он должен быть целым ненулевым, противоречие.

Значит, все координаты α не могут быть по модулю меньше ϵ, поэтому различных наборов конечное число. Как мы уже показали, в этом случае

выполняется утверждение задачи. Задача решена.

Задача 55. Зафиксируем базис $\gamma_1, \ldots, \gamma_n$ в $\mathbb{Q}[\alpha]$, и рассмотрим $\alpha_1, \ldots, \alpha_N$ из предыдущей задачи. Тогда координаты элементов I в нашем базисе порождаются коэффициентами $\alpha_1, \ldots, \alpha_N$ (т.е. их конечными суммами). Рассмотрим первые координаты всех элементов I — они порождаются первыми координатами $\alpha_1, \ldots, \alpha_N$, поэтому они имеют вид $q_1 r$ для фиксированного рационального q_1 и всех целых r (применим алгоритм Евклида к первым координатам $\alpha_1, \ldots, \alpha_N$). Возьмем какой-то $\beta_1 \in I$ с первой координатой q_1 (если $q_1 = 0$, о возьмем $\beta_1 = 0$), и вычтем из элементов I (различные) числа $k\beta_1$ с целым k так, чтобы все первые координаты стали равны 0. Потом применим эту операцию ко второй координате, и так далее. В конце мы получим набор $\beta_1, \ldots, \beta_n$, ненулевые элементы которого удовлетворяют условию задачи: любое $\alpha \in I$ можно представить в нужном виде, т.к. мы можем последовательно вычитать из α числа $k_i\beta_i$ с целыми k_i так, чтобы обнулялись i-ые координаты, и в конце получим 0. При этом такое представление единственно, иначе для каких-то целых k_i – $k_1\beta_1 + \ldots + k_l\beta_l = 0$, причем не все $k_i\beta_i$ равны 0. Пусть $k_r\beta_r$ — ненулевое слагаемое с минимальным r, тогда r-ая координата у $k_r\beta_r$ не равна 0, а у всех остальных слагаемых — нулевая по построению β_i, противоречие.

Задача 56. Это сразу следует из первого утверждения в решении задачи 54 и того, что для элементов целого базиса $\alpha_1, \ldots, \alpha_n$ не существуют целых k_i таких, что $k_1\alpha_1 + \ldots + k_n\alpha = 0$, причем не все k_i равны 0.

Задача 57. Очевидно.

Задача 58. Можно показать, что искомое количество равно $N(I)$.

Задача 59. Применим первое утверждение в решении задачи 54 к $\alpha = 1$.

Задача 60. Пусть целое $m \in I$, и $\alpha_1, \ldots, \alpha_n$ — целый базис $\widetilde{\mathbb{Z}}$. Тогда элементы $\widetilde{\mathbb{Z}}/I$ имеют представителей среди $k_1\alpha_1 + \ldots + k_n\alpha$, где $0 \leq k_i < m$, т.к. $m\alpha_i \in I$. Значит, $\widetilde{\mathbb{Z}}/I$ — конечное множество.

Задача 61. Любой идеал I, содержащий (α), полностью определяется элементами $\widetilde{\mathbb{Z}}/(\alpha)$, которые содержаться в I (если I содержит одного представителя, то он содержит весь класс эквивалентности). Т.к. $\widetilde{\mathbb{Z}}/(\alpha)$ конечно, то и множество его подмножеств конечно, поэтому таких идеалов — конечное число.

Задача 62. Из задачи 56 следует, что вектора элементов целого базиса I являются базисом рационального n-мерного пространства над $\mathbb{Q}$.

Задача 63. Возьмем $M_1 = \max_{i,j}(\|\alpha_i\alpha_j\|) + 1$ и $\beta_i = \alpha_i\beta$. Тогда если $\beta = x_1\alpha_1 + \ldots + x_n\alpha_n$, то $\|\beta_i\| = \|x_1\alpha_1\alpha_i + \ldots + x_n\alpha_n\alpha_i\| \leq \|x_1\alpha_1\alpha_i\| +$

$\ldots + \|x_n\alpha_n\alpha_i\| < M_1(x_1 + \ldots + x_n) = M_1\|\beta\|$, ч.т.д.

Задача 64. Из задачи 56 следует, что для β_i из предыдущей задачи существуют и единственны такие рациональные x_i, что $\alpha = x_1\beta_1 + \ldots + x_n\beta_n$. Возьмем такое $c \in \widetilde{\mathbb{Z}}$, что $c\beta = \lfloor x_1 \rfloor \beta_1 + \ldots + \lfloor x_n \rfloor \beta_n$, тогда $\|\alpha - c\beta\| = \|\{x_1\}\beta_1 + \ldots + \{x_n\}\beta_n\| < \|\beta_1\| + \ldots + \|\beta_n\| < nM_1\|\beta\|$, ч.т.д.

Задача 65. Для каждого натурального $k \leq M_2$ рассмотрим $\alpha'_k = k\alpha - c_k\beta$ такое, что $\|\alpha'_k\| < nM_1\|\beta\|$. Векторы всех α'_k лежат в кубе с центром в 0 и со стороной $2nM_1\|\beta\|$. Разобьем его на $(2n(n+1)M_1)^n$ кубов со стороной $\|\beta\|/(n+1)$, тогда среди $M_2 = (2n(n+1)M_1)^n + 1$ векторов α'_k какие-то α'_k и α'_r, $k \neq r$, лежат в одном кубе со стороной $\|\beta\|/(n+1)$. Значит, $\|\alpha'_k - \alpha'_r\| \leq \|\beta\| n/(n+1) < \|\beta\|$, но $\alpha'_k - \alpha'_r = (k-r)\alpha - c\beta$, где $|k-r| < M_2$. Значит, $m = |k-r|$ подходит.

Задача 66. Выберем β как ненулевой элемент I с минимальным $\|\beta\|$. Тогда для любого $\alpha \in I$ существует $m \leq M_2$ и $c \in \widetilde{\mathbb{Z}}$ такие, что $\|m\alpha - c\beta\| < \|\beta\|$. Но $m\alpha - c\beta \in I$, поэтому $m\alpha = c\beta$. Значит, для любого $\alpha \in I$ существует $c \in \widetilde{\mathbb{Z}}$ такое, что $M_2!\alpha = c\beta$, поэтому $M_2!I \subseteq (\beta)$. Следовательно, $(1/\beta)M_2!I$ — идеал, и $M_2 = (1/\beta)M_2!\beta \in (1/\beta)M_2!I$.

Задача 67. По задаче 61 — идеалов, содержащих $M_2!$, конечное число, и каждый идеал I по предыдущей задаче эквивалентен одному из них, т.к. $(M!)I = (\beta)((1/\beta)M_2!I)$. Значит, классов эквивалентности идеалов — конечное число.

Задача 68. Пусть $\beta_1, \ldots, \beta_n$ — целый базис I, тогда если $\alpha I \subseteq I$, то $\alpha\beta_i = a_{i1}\beta_1 + a_{i2}\beta_2 + \ldots + a_{in}\beta_n$ для всех i, где все a_{ij} — целые. Перепишем эти уравнения как

$$a_{i1}\beta_1 + a_{i2}\beta_2 + \ldots + a_{i,i-1}\beta_{i-1} + (a_{i,i} - \alpha)\beta_i + a_{i,i+1}\beta_{i+1} \ldots + a_{in}\beta_n = 0,$$

и получим систему однородных линейных уравнений на переменные $\beta_1, \ldots, \beta_n$. Запишем её коэффициенты в виде матрицы

$$\begin{pmatrix} a_{11} - \alpha & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} - \alpha & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} - \alpha \end{pmatrix}$$

Те из вас, кто знаком с понятием определителя, могут сразу заметить, что определитель этой матрицы — это приведенный многочлен от α с целыми коэффициентами, и при этом определитель равен 0 ввиду наличия ненулевого решения $(\beta_1, \ldots, \beta_n)$. Из этого мы сразу получаем, что α — целое алгебраическое. Но так как (возможно) не все из вас знакомы

с определителем, то мы проведем несколько более громоздкое рассуждение, использую метод Гаусса решения системы линейных уравнений, или просто метод последовательного исключения переменных. На самом деле, оно будет довольно близко к доказательству одного из основных свойств определителя (что система имеет нетривиальное решение тогда и только тогда, когда определитель равен 0), поэтому принципиально от предыдущего оно ничем не отличается.

Предположим, что α — не целое алгебраическое, т.е. любой ненулевой приведенный многочлен с целыми коэффициентами от α не равен 0. Как известно и очевидно, множество решений системы уравнений не изменится, если мы умножим одно уравнение на ненулевую константу или вычтем из одного уравнения другое, умноженное на константу.

Давайте исключим переменную β_1 из всех уравнений, кроме первого — по предположению $a_{11} - \alpha \neq 0$, поэтому мы можем умножить все остальные уравнения на $a_{11} - \alpha$, а потом вычесть из i-ого уравнения 1-ое, умноженное на a_{i1}. Коэффициенты новой системы будут иметь вид

$$\begin{pmatrix} a_{11}-\alpha & a_{12} & \dots & a_{1n} \\ 0 & (a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12} & \dots & a_{2n}(a_{11}-\alpha) - a_{21}a_{1n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2}(a_{11}-\alpha) - a_{n1}a_{12} & \dots & (a_{nn}-\alpha)(a_{11}-\alpha) - a_{n1}a_{1n} \end{pmatrix}$$

Теперь можно исключить переменную β_2 из всех уравнений, кроме первого и второго — по предположению коэффициент при β_2 во втором уравнении $(a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12} \neq 0$, поэтому мы можем умножить все уравнения после 2-ого на $(a_{22}-\alpha)(a_{11}-\alpha) - a_{21}a_{12}$, а потом вычесть из i-ого, $i > 2$ уравнения 2-ое, умноженное на старый (до последнего умножения) коэффициент i-ого уравнения при β_2. Покажем по индукции, что мы и дальше сможем по очереди исключать переменные.

Предположим, что для натурального $1 \leq k \leq n$ – при $1 \leq i \leq k$, мы уже исключили i-ую переменную из уравнений с номером, большим i, и коэффициенты уравнений являются многочленами с целыми коэффициентами от α, причем коэффициенты уравнений с номером $i > k$ при β_i – степени 2^k, степени остальных коэффициентов уравнений с номером $i > k$ строго меньше 2^k, и все коэффициенты i-ых уравнений при β_i — с точностью до знака приведенные многочлены:

$$\begin{pmatrix} P_{11}(\alpha) & P_{12}(\alpha) & \dots & & & & & \\ 0 & P_{22}(\alpha) & \dots & & & & & \\ \vdots & \vdots & \ddots & & & & & \\ 0 & 0 & \dots & P_{k,k}(\alpha) & P_{k,k+1}(\alpha) & P_{k,k+2}(\alpha) & \dots & P_{k,n}(\alpha) \\ 0 & 0 & \dots & 0 & P_{k+1,k+1}(\alpha) & P_{k+1,k+2}(\alpha) & \dots & P_{k+1,n}(\alpha) \\ 0 & 0 & \dots & 0 & P_{k+2,k+1}(\alpha) & P_{k+2,k+2}(\alpha) & \dots & P_{k+2,n}(\alpha) \\ \vdots & \vdots & \dots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & P_{n,k+1}(\alpha) & P_{n,k+2}(\alpha) & \dots & P_{n,n}(\alpha) \end{pmatrix},$$

где $\deg(P_{ii}) = 2^k$ при $i > k$, и $\deg(P_{ij}) < 2^k$ при $i, j > k$ и $i \neq j$, причем P_{ii} — приведенный с точностью до знака. Рассмотрим уравнения с номерами $i > k$ от β_i с $i > k$:

$$\begin{pmatrix} P_{k+1,k+1}(\alpha) & P_{k+1,k+2}(\alpha) & \dots & P_{k+1,n}(\alpha) \\ P_{k+2,k+1}(\alpha) & P_{k+2,k+2}(\alpha) & \dots & P_{k+2,n}(\alpha) \\ \vdots & \vdots & \ddots & \vdots \\ P_{n,k+1}(\alpha) & P_{n,k+2}(\alpha) & \dots & P_{n,n}(\alpha) \end{pmatrix}$$

Для краткости обозначим $Q_{ij} = P_{k+i,k+j}(\alpha)$. По предположению $Q_{11} \neq 0$, поэтому мы можем умножить все уравнения после 1-ого на Q_{11}, а потом вычесть из i-ого, $i > 1$ уравнения 1-ое, умноженное на старый (до последнего умножения) коэффициент i-ого уравнения при β_{k+1}:

$$\begin{pmatrix} Q_{11} & Q_{12} & \dots & Q_{1,n-k} \\ 0 & Q_{22}Q_{11} - Q_{21}Q_{12} & \dots & Q_{2,n-k}Q_{11} - Q_{21}Q_{1,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & Q_{n-k,2}Q_{11} - Q_{n-k,1}Q_{12} & \dots & Q_{n-k,n-k}Q_{11} - Q_{n-k,1}Q_{1,n-k} \end{pmatrix}$$

Тогда $\deg(Q_{ii}Q_{11} - Q_{i,1}Q_{1,i}) = 2^{k+1}$, он приведенный с точностью до знака, и $\deg(Q_{ij}Q_{11} - Q_{i,1}Q_{1,j}) < 2^{k+1}$ при $i \neq j$. Мы исключили β_{k+1} из уравнений с номером $i > k+1$ с сохранением условий на коэффициенты, тем самым переход индукции доказан (база $k = 0$).

Подставляя $k = n$, получим систему уравнений на $\beta_1, \dots, \beta_n$, последнее уравнение которой имеет вид $P_{n,n}(\alpha)\beta_n = 0$, где $P_{n,n}$ – приведенный многочлен с целыми коэффициентами. Значит, $P_{n,n}(\alpha) \neq 0$ и $\beta_n \neq 0$, противоречие. Значит, α — целое алгебраическое, ч.т.д.

Задача 69. Пусть $\alpha_1, \dots, \alpha_n$ — целый базис I, тогда если $JI = I$, то для каждого i существуют такие $\beta_{i1}, \dots, \beta_{in} \in J$, что $\alpha_i = \beta_{i1}\alpha_1 +$

$\ldots + \beta_{in}\alpha_n$. Тем самым мы получаем систему линейных уравнений на $\alpha_1, \ldots, \alpha_n$ с коэффициентами

$$\begin{pmatrix} \beta_{11}-1 & \beta_{12} & \ldots & \beta_{1n} \\ \beta_{21} & \beta_{22}-1 & \ldots & \beta_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \beta_{n1} & \beta_{n2} & \ldots & \beta_{nn}-1 \end{pmatrix}$$

Заметим, что ситуация аналогична с предыдущей задачей — целые числа заменены на идеал J, а α — на 1. Аналогично с предыдущей задачей мы можем доказать, что 1 — корень приведенного многочленами с коэффициентами в J, из чего будет следовать, что $1 \in J$, поэтому $J = (1)$.

Задача 70. Очевидно следует из конечности числа классов идеалов.

Задача 71. По предыдущей задаче $(\alpha)I^k = (\beta)I^m$ для каких-то ненулевых α и β. Деля на β, получаем $(\alpha/\beta)I^k = I^m$, и т.к. $I^m \subseteq I^k$, то $(\alpha/\beta)I^k \subseteq I^k$. По задаче 68 получаем, что $\gamma = \alpha/\beta \in \widetilde{\mathbb{Z}}$, т.е. $(\gamma)I^k = I^m = I^k I^{m-k}$. Для любого $\alpha \in I^{m-k}$ получаем $(\alpha)I^k \subseteq (\gamma)I^k$, значит $(\alpha/\gamma)I^k \subseteq I^k$, и по задаче 68 $\alpha/\gamma \in \widetilde{\mathbb{Z}}$, т.е. все элементы I^{m-k} делятся на γ. Поэтому $(1/\gamma)I^{m-k}$ — идеал, и $I^k = (1/\gamma)I^{m-k}I^k$. Значит, по задаче 69 мы получаем $(1/\gamma)I^{m-k} = (1)$, поэтому $I^{m-k} = (\gamma)$.

В частности, для $J = I^{m-k-1}$ — $IJ = (\gamma)$.

Задача 72. Если I делится на J, то $I = JH$ для какого-то идеала H, поэтому $I \subseteq J$.

Обратно, если $I \subseteq J$, то возьмем по предыдущей задаче такой идеал J', что $JJ' = (\alpha)$ для ненулевого α. Тогда $IJ' \subseteq JJ' = (\alpha)$, поэтому $H = (1/\alpha)IJ'$ – идеал, и $I = (1/\alpha)JJ'I = JH$. Значит, I делится на J.

Задача 73. Для ненулевого идеала I обозначим $N(I) = |\widetilde{\mathbb{Z}}/I|$ — количество элементов в $\widetilde{\mathbb{Z}}/I$. Если $I \subset J$, то $N(I) > N(J)$, т.к. классы эквивалентности $\widetilde{\mathbb{Z}}/J$ являются объединением каких-то классов эквивалентности $\widetilde{\mathbb{Z}}/I$, причем класс J содержит больше одного класса $\widetilde{\mathbb{Z}}/I$, т.к. $I \neq J$.

Для ненулевого идеала I найдем какой-то его простой делитель, продолжая по индукции цепочку вложенных собственных идеалов $I \subset I_1 \subset I_2 \subset \ldots$ — т.к. $N(I_k)$ уменьшается, то в какой-то момент мы не сможем её продолжить, тогда последний член в цепочке будет простым идеалом P_1 (т.к. он не содержится в других собственных идеалах). По предыдущей задаче $I = P_1 H$ для какого-то идеала H, причем $N(H) < N(I)$. Аналогично для H получаем $H = P_2 R$, т.е. $I = P_1 P_2 R$ с $N(R) < N(H)$. Продолжая эту операцию, пока можем (т.е. $N > 1$), мы получаем разложение $I = P_1 P_2 \ldots P_n$ на простые идеалы.

Задачи 74 - 78. Аналогично задачам 25 – 27.

Generalizations of the fundamental theorem of arithmetic

Vera Bulankina, Ivan Frolov, Timofei Zaitsev,
Aleksei Petukhov, Ruslan Salimov*

Introduction

The goal of this project is to generalize the fundamental theorem of arithmetic from integers to some more "advanced" objects. For solving the problems of the project, it is possible to team up with other participants.

The fundamental theorem of arithmetic (Theorem 1 below, see also Theorems 4, 5, 7) is useful for finding integer solutions of various polynomial equations, i.e. Diophantine equations. For example they are useful in some proofs of Fermat's theorem on sum of two squares (Theorem 2) and Fermat's Last Theorem (Theorem 3) for $n = 3$. You can try to prove them right now, but most probably it is better to return to them after the relevant sections of the project. Also you will see that the uniqueness of the prime factorization does not always hold for analogs of integers.

In the second part of the project we consider the version of the fundamental theorem of arithmetic which works for numbers of the form $a + b\sqrt{d}$, where d is a fixed integer and a, b are any integer variables (to do this, we need a concept of ideal). This technique will be applied to Diophantine equations.

In the third part we will discuss a more general statement on arbitrary algebraic numbers.

Finally, there is an additional list of problems in which we will try to apply the general theory to Fermat's Last Theorem. We will discuss the so-called first case of the Fermat's Last Theorem for the regular prime numbers. Using similar ideas one can prove the second case of the Fermat's Last Theorem for any n, which is divisible by a regular prime number p. All prime number up to 37 are regular, see books of M. Postinkov or J. Milne or Wikipedia.

We would like to mention that Andrew Wiles general proof of the Fermat's Last Theorem is based on essentially different methods and ideas.

We have have used books of K. Ireland and M. Rosen, J. Milne, M. Postnikov, L. Washington, notes of K. Conrad and Wikipedia to prepare the project. We also added a few references [SS, Go, ZSS] that may be of interest to the reader who wants to learn more about this subject.

Theorem 1. The fundamental theorem of arithmetic.
Every integer $n > 1$ is a product $n = p_1 \cdot \ldots \cdot p_k$ of prime numbers $p_1, \ldots, p_k$. Moreover, this presentation is unique, up to an order of the factors.

Theorem 2. Fermat's theorem on sum of two squares.
An integer $n > 0$ can be expressed as a sum of two squares if and only if all prime numbers of the form $4k + 3$ participate the prime decomposition of n even number of times.

Theorem 3. Fermat's Last Theorem.
The equation $x^n + y^n = z^n$ has no solution in positive integers x, y and z for $n > 2$.

*We also wish to thank Mikhail Skopenkov, Ilya Bogdanov and Keith Conrad for a variety of useful comments on this project.

1 Gaussian integers

In this part of the project we want to discuss Gaussian integers. This is a generalization of integers which uses $\sqrt{-1}$. If you can't solve some of the problems from this section, then try to solve problems from other sections of the project and come back here later.

Definition. *Gaussian integers* is the set of complex numbers of the form $a + bi$, where $a, b \in \mathbb{Z}$, $i = \sqrt{-1}$. We denote the set of Gaussian integers by $\mathbb{Z}[i]$.

Problem 1. Prove that the sum of any two Gaussian integers (and the product of any two Gaussian integers) is a Gaussian integer.

To proceed with the unique factorization for Gaussian integers we need a more exact formulation of the fundamental theorem of arithmetic. Strictly speaking, a straightforward analog of the statement of Theorem 1 is not literally correct even for integers: $2 \cdot 3 = 6 = (-2) \cdot (-3)$. For the new formulation we need few more definitions.

Definition. We say that an element $z \in \mathbb{Z}[i]$ is *invertible* if there is $b \in \mathbb{Z}[i]$ such that $ab = 1$. The invertible elements of $\mathbb{Z}$ are defined in the same way.

Exercise 1. Prove that the invertible elements in integers are 1 and -1. Prove that the invertible elements in Gaussian integers are 1, -1 and also $i, -i$.

Definition. A Gaussian integer is called *prime*, if for any it's factorization into two factors strictly one of these factors is an invertible element.

Definition. Two factorizations into prime numbers are *the same* if they have the same number of factors and if we can change the order of factors in such a way that the ratio of the corresponding prime factors is an invertible element. For example $7 \cdot 3, (-3) \cdot (-7)$ and $(-7i) \cdot (3i)$ are the same factorizations of 21 in Gaussian integers.

Our immediate goal is to prove and to discuss the following theorem.

Theorem 4. The fundamental theorem of arithmetic for the Gaussian integers.
Any two factorizations of a Gaussian integer into prime numbers are the same.

Problem 2.* Define a division-with-remainder for $\mathbb{Z}[i]$. Use it to prove Theorem 4.
Hint: use magnitude of complex numbers and graphical (Gaussian) interpretation of complex numbers.

Problem 3. Find all integer solutions of the equation $x^2 + 1 = y^n$.

Problem 4. a) Let $p \in \mathbb{Z}$ be prime. Prove that p is a prime Gaussian integer if and only if $p + 1$ is divisible by 4.

b) If $n, m \in \mathbb{Z}$ can be expressed as a sum of two squares, then mn can be expressed as a sum of two squares.

c) Prove Fermat's theorem on sum of two squares (Theorem 2).

Problem 5. Let n be an integer. Count the number of ways in which n can be decomposed into the sum of squares? Hint: try to use the prime factorization of n.

Eisenstein integers

The goal of this section is to solve of the following problem.

Problem 6*. Prove Theorem 3 for $n = 3$ using the following formula

$$x^3 + y^3 = (x + y)\left(x + \frac{-1 + \sqrt{-3}}{2}y\right)\left(x + \frac{-1 - \sqrt{-3}}{2}y\right).$$

Let's introduce several definitions and consider several ancillary problems to achieve this goal. Denote by ξ a cubic root of unity such that $\xi \neq 1$.

Exercise 2. Prove that $\xi = \frac{-1\pm\sqrt{-3}}{2}$.

Put $\mathbb{Z}[\xi] := \{a + b\xi : \ a, b \in \mathbb{Z}\}$. Such numbers are called *Eisenstein integers*.

Definition. An Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ *is divisible* by $\beta \in \mathbb{Z}[\xi]$ if and only if there is $\gamma \in \mathbb{Z}[\xi]$ such that $\alpha = \beta\gamma$.

The invertible elements of $\mathbb{Z}[\xi]$ are defined similarly to the invertible elements of $\mathbb{Z}$ and of $\mathbb{Z}[i]$.

Definition. An Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ is *composite* if $\alpha = \beta\gamma$ where β and $\gamma \in \mathbb{Z}[\xi]$ aren't invertible. An nonzero Eisenstein integer $\alpha \in \mathbb{Z}[\xi]$ is *prime*, if α is neither composite nor invertible.

Problem 7. Find out all invertible elements of $\mathbb{Z}[\xi]$.

Problem 8. Define a division-with-remainder procedure for $\mathbb{Z}[\xi]$. Use it to formulate and to prove the fundamental theorem of arithmetic for $\mathbb{Z}[\xi]$.

Quadratic fields

In this section we consider quadratic fields. They generalise Gaussian integers and Eisenstein integers.

Definition. For complex numbers $a_1, \ldots, a_n$ let $\mathbb{Z}[a_1, \ldots, a_n]$ denote the smallest subset of $\mathbb{C}$ containing $\mathbb{Z}$ and $a_1, \ldots, a_n$ which is closed under addition, subtraction and multiplication.

Define $\mathbb{Q}[a_1, \ldots, a_n]$ similarly (replace $\mathbb{Z}$ by $\mathbb{Q}$). The sets $\mathbb{Z}[a_1, \ldots, a_n]$ play an analogous role in $\mathbb{Q}[a_1, \ldots, a_n]$ as the ordinary integers do in $\mathbb{Q}$. (Their elements can be added and multiplied).

Fix a square-free integer $d \neq 1$.

Remark. There are two main examples for d: $d = -3$ and $d = 2$. It can be useful to first check all problems of this section for these values of d, and then proceed to the general case.

Exercise 3. a) Prove that

$$\mathbb{Q}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Q}\} \text{ and } \mathbb{Z}[\sqrt{d}] = \{x + y\sqrt{d} : x, y \in \mathbb{Z}\}.$$

b) Prove that if $a, b \in \mathbb{Q}[\sqrt{d}]$ and $b \neq 0$, then $\frac{a}{b} \in \mathbb{Q}[\sqrt{d}]$.

Definition. *Integers in* $\mathbb{Q}[\sqrt{d}]$ are numbers $\alpha \in \mathbb{Q}[\sqrt{d}]$, satisfying $\alpha^2 + p\alpha + q = 0$ with $p, q \in \mathbb{Z}$.

Exercise 4. Is ξ an integer in $\mathbb{Q}[\sqrt{-3}]$? Is $\frac{1+i}{2}$ an integer in $\mathbb{Q}[i]$?

Set $\omega = \sqrt{d}$ when $d \equiv 2, 3 \bmod 4$, and $\omega = \frac{\sqrt{d}+1}{2}$ when $d \equiv 1 \bmod 4$.

The unique factorization into prime numbers can fail for $\mathbb{Z}[\omega]$, but there are several valid modifications of it. Further we will discuss one of them. For any $\alpha = a+b\sqrt{d}$, where $a, b \in \mathbb{Q}$, we define its conjugate $\overline{\alpha} = a - b\sqrt{d}$, its norm $N(\alpha) = \alpha\overline{\alpha}$ and its trace $\mathrm{Tr}(\alpha) = \alpha + \overline{\alpha}$.

Exercise 5. Prove that $\overline{a+b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\overline{b}$.

Exercise 6. a) Prove that $\alpha \in \mathbb{Q}[\sqrt{d}]$ is a root of the polynomial $x^2 - \mathrm{Tr}(\alpha)x + N(\alpha)$.
b) Prove that $\alpha \in \mathbb{Q}[\sqrt{d}]$ is an integer in $\mathbb{Q}[\sqrt{d}]$ if and only if $N(\alpha) \in \mathbb{Z}$ and $\mathrm{Tr}(\alpha) \in \mathbb{Z}$.

Problem 9. Prove that the set of integers in $\mathbb{Q}[\sqrt{d}]$ coincides with $\mathbb{Z}[\omega]$.

The invertible elements of $\mathbb{Z}[\omega]$ are defined similarly to the invertible elements of $\mathbb{Z}$ and $\mathbb{Z}[i]$.

Exercise 7. Prove that $\gamma \in \mathbb{Z}[\omega]$ satisfies $N(\gamma) = \pm 1$ if and only if γ is invertible.

Definition. A number $\alpha \in \mathbb{Z}[\omega]$ *is divisible* by $\beta \in \mathbb{Z}[\omega]$ if there exists $\gamma \in \mathbb{Z}[\omega]$ such that $\alpha = \beta\gamma$.

Definition. A nonzero number $\alpha \in \mathbb{Z}[\omega]$ is *composite* if $\alpha = \beta\gamma$, where β and $\gamma \in \mathbb{Z}[\omega]$ are not invertible. A number $\alpha \in \mathbb{Z}[\omega]$ is *prime* if α is neither composite nor invertible.

Exercise 8. For $\gamma \in \mathbb{Z}[\omega]$ prove that if $|N(\gamma)| \in \mathbb{Z}$ is prime then γ is prime in $\mathbb{Z}[w]$. Show that the converse is false in $\mathbb{Z}[\sqrt{3}]$.

Exercise 9. Prove that if $\gamma \in \mathbb{Z}[\omega]$ is not invertible, then γ is a product of primes in $\mathbb{Z}[\omega]$.

Problem 10. Prove that all factors in the following decomposition of 15 in $\mathbb{Z}[\sqrt{-14}]$ are prime.

$$15 = 3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14})$$

Problem 11. Define a version of Euclidean algorithm for a) $\mathbb{Z}[\sqrt{-2}]$; b) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$. Use it to prove the unique factorization in $\mathbb{Z}[\sqrt{-2}]$ and $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$.

Problem 12. Find all invertible elements of

a) $\mathbb{Z}[\sqrt{-1}]$, b) $\mathbb{Z}[\sqrt{-d}]$ with $d \geq 2$, c) $\mathbb{Z}[\frac{1+\sqrt{-3}}{2}]$, d*) $\mathbb{Z}[\sqrt{2}]$.

Problem 13. Does unique factorization hold in

a) $\mathbb{Z}[\sqrt{2}]$, b) $\mathbb{Z}[\sqrt{-3}]$, c) $\mathbb{Z}[\sqrt{3}]$, d) $\mathbb{Z}[\sqrt{-5}]$, e) $\mathbb{Z}[\sqrt{5}]$, f) $\mathbb{Z}[\sqrt{10}]$, g) $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$,
h) $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$, i) $\mathbb{Z}[\frac{1+\sqrt{-11}}{2}]$, j*) $\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$?

Problem 14. For which complex numbers ξ the sum and the product of any numbers of the form $a + b\xi$ with $a, b \in \mathbb{Z}$ have the same form?

Problem 15.* Find all positive integer solutions of
a) $3^n = k^2 + 2$ b) $2^n = k^2 + 7$.

Ideals

In the following sections we give an approach to the following problems.

Problem 16. Find all integer solutions of
a) $x^2+5=y^3$, b) $x^2+2x+7=y^3$ c) $5x^2+1=y^3$, d) $6x^2-12x+7=y^3$, e*) $x^2-6=y^3$.

Definition. A nonempty subset $I \in \mathbb{Z}$ is called an *ideal* if it is closed under addition, subtraction and multiplication by integers:

$$a,b \in I \implies a \pm b \in I, \quad a \in I, b \in \mathbb{Z} \implies ab \in I.$$

Remark. The notion of ideal was invented by Richard Dedekind as a replacement for the ideal numbers of Ernst Kummer (these numbers turn out to be useful to solve some cases Fermat's last theorem). One can check whether or not a given number is divisible by an ideal number even if this ideal number is not well defined. A similar idea is behind the definition of Dedekind cut of rational numbers.

Exercise 10. a) Prove that any ideal contains 0. b) Prove that $a \in I$ implies $-a \in I$. c) Prove that the set of all even integers form an ideal in $\mathbb{Z}$. d) Prove that the set $\{2018m : m \in \mathbb{Z}\}$ is an ideal in $\mathbb{Z}$.

Exercise 11. Prove that the intersection of several ideals is an ideal.

We denote by $(a_1, \dots, a_n)$ the smallest ideal (intersection of all ideals) containing $a_1, \dots, a_n \in \mathbb{Z}$.

Problem 17. a) Let a, b be relatively prime numbers. Prove that $(a,b) = (1) = \mathbb{Z}$.
b) Prove that $(a,b) = (g)$, where $a, b \in \mathbb{Z}$ and g is the greatest common divisor of a, b.
c) Prove that every ideal $I \neq \{0\}$ in $\mathbb{Z}$ is (g) for some $g \in \mathbb{Z}$.

As in the previous section we set $\omega = \sqrt{d}$ when $d \equiv 2, 3 \bmod 4$, and $\omega = \frac{\sqrt{d}+1}{2}$ when $d \equiv 1 \bmod 4$. An ideal in $\mathbb{Z}[\omega]$ is defined similarly to $\mathbb{Z}$ ($\mathbb{Z}$ is replaced by $\mathbb{Z}[\omega]$). Similarly, numbers $\alpha_1, \dots, \alpha_n \in \mathbb{Z}[\omega]$ define an ideal $(\alpha_1, \dots, \alpha_n)$ in $\mathbb{Z}[\omega]$. In particular, every element $\alpha \in \mathbb{Z}[\omega]$ defines the ideal (α).

Exercise 12. Prove that for nonzero α and β in $\mathbb{Z}[w]$ $(\alpha) = (\beta)$ if and only if $\alpha/\beta, \beta/\alpha \in \mathbb{Z}[\omega]$ (i.e. α/β is invertible in $\mathbb{Z}[\omega]$).

Exercise 13. Let $a, x, y \in \mathbb{Z}$. Prove that $x + y\omega \in (a)$ if and only if $a \mid x$ and $a \mid y$.

Definition. An ideal of the form (α) for some $\alpha \in \mathbb{Z}[\omega]$ is called *principal*. As we have seen in Problem 17, all ideals in $\mathbb{Z}$ are principal.

Problem 18. Show that $(2, \sqrt{-14})$ is not a principal ideal in $\mathbb{Z}[\sqrt{-14}]$.

Problem 19. Prove that, for each ideal I in $\mathbb{Z}[\omega]$, there exist $\alpha, \beta \in \mathbb{Z}[\omega]$ such that

$$I = \{x\alpha + y\beta : \quad x, y \in \mathbb{Z}\}.$$

Definition. For two ideals $I, J \in \mathbb{Z}[\omega]$ we set

$$I + J := \{i_1 + i_2 : i_1 \in I_1, i_2 \in J\}, \quad \overline{I} := \{\overline{i} : i \in I\},$$
$$IJ := \{i_1 j_1 + \dots + i_k j_k : i_1, \dots, i_k \in I, j_1, \dots, j_k \in J\}.$$

Exercise 14. In $\mathbb{Z}[\sqrt{-14}]$ compute the product of ideals $I = (5 + \sqrt{-14}, 2 + \sqrt{-14})$ and $J = (4 + \sqrt{-14}, 2 - \sqrt{-14})$.

Exercise 15. Show that

$$(3) = p_1 p_2, \quad (5) = p_3 p_4, \quad (1 + \sqrt{-14}) = p_1 p_3, \quad (1 - \sqrt{-14}) = p_2 p_4,$$

where

$$p_1 = (3, 1 + \sqrt{-14}),\ p_2 = (3, 1 - \sqrt{-14}),\ p_3 = (5, 1 + \sqrt{-14}),\ p_4 = (5, 1 - \sqrt{-14}).$$

Exercise 16. Compute $(20)(18)$, $(20) + (18)$, $(20) \cap (18)$ in $\mathbb{Z}[\omega]$ for all d.

Exercise 17. Prove that $I + J, \overline{I}, IJ$ are ideals in $\mathbb{Z}[\omega]$ for all ideals $I, J \subset \mathbb{Z}[\omega]$.

2 Unique factorization: quadratic fields

In Problem 10 we saw that the straightforward version of the unique factorization fails for $\mathbb{Z}[\sqrt{-14}]$:

$$3 \cdot 5 = (1 + \sqrt{-14})(1 - \sqrt{-14}).$$

On the other hand, by Exercise 15,

$$(3) = p_1 p_2, \quad (5) = p_3 p_4, \quad (1 + \sqrt{-14}) = p_1 p_3, \quad (1 - \sqrt{-14}) = p_2 p_4,$$

where

$$p_1 = (3, 1 + \sqrt{-14}), p_2 = (3, 1 - \sqrt{-14}), p_3 = (5, 1 + \sqrt{-14}), p_4 = (5, 1 - \sqrt{-14}),$$

i.e. $(15) = p_1 p_2 p_3 p_4$. The ideals p_1, p_2, p_3, p_4 are a replacement of prime numbers, see Problem 23, and the factorization $(15) = p_1 p_2 p_3 p_4$ is unique up to the order of the factors, as the following theorem shows.

Theorem 5. Fundamental theorem of arithmetic for quadratic fields.
For every ideal $I \subset \mathbb{Z}[\omega]$ that is not (0) or (1) there exists a factorization of I as a product of prime ideals into prime ideals

$$I = p_1 \cdots p_s \subset \mathbb{Z}[\omega].$$

This factorization is unique up to an order of the factors.

Theorem 5 has two parts: existence of the factorization and its uniqueness. The former is proved in Problem 24 and the latter in Problem 27. As an example, this theorem can be used to solve Problem 16. See also the section on Fermat's Last Theorem.

Corollary. For every $m \in \mathbb{Z}[\omega]$ that is not 0 or invertible there exists a factorization of the ideal (m) into a product of prime ideals $p_1, \ldots, p_s \subset \mathbb{Z}[\omega]$, unique up to the order of the factors.

The proof is divided into the following problems.

Problem 20. For every $a_1, \ldots, a_n \in \mathbb{Z}[\omega]$ prove that

$$(a_1, \ldots, a_n)(\overline{a}_1, \ldots, \overline{a}_n) = (N(a_i), \mathrm{Tr}(a_i \overline{a_j}))_{1 \le i,j \le n}.$$

Hint: consider the case of an ideal generated by two elements.

Definition. We say that an ideal I *is divisible by* an ideal J if there exists an ideal H in $\mathbb{Z}[\omega]$ such that $I = JH$.

Problem 21. For any two ideals I, J in $\mathbb{Z}[\omega]$ prove that I is divisible by J if and only if I is contained in J.
Hint: use the previous problem.

Exercise 18. Use Problem 20 to prove that, for every nonzero ideal $I \subset \mathbb{Z}[\omega]$, there exists a positive integer $N(I)$ such that $I\overline{I} = (N(I))$.

Problem 22. Prove that an ideal H divides I and J if and only if it divides $I + J$.

Exercise 19. Prove that $N((a)) = |N(a)|$ for every nonzero $a \in \mathbb{Z}[\omega]$.

Exercise 20. Prove that $N(I)N(J) = N(IJ)$ for all nonzero ideals I, J in $\mathbb{Z}[w]$.

Exercise 21. Prove that if an ideal I divides an ideal J, than $N(I)$ divides $N(J)$.

Exercise 22. Prove that $N(I) = 1$ if and only if $I = (1)$.

An ideal I in $\mathbb{Z}[\omega]$ is called *prime* if it is not (1) and it is divisible by exactly two ideals: itself and (1).

Exercise 23. Prove that an ideal I is prime if and only if it is maximal, i.e. the only bigger ideal is (1).

Two ideals I, J are called *relatively prime* if $I + J = (1)$.

Exercise 24. Prove that any two distinct prime ideals are relatively prime.

Problem 23. Show that the following ideals are prime in $\mathbb{Z}[\sqrt{-14}]$:

$$p_1 = (3, 1 + \sqrt{-14}),\ p_2 = (3, 1 - \sqrt{-14}),\ p_3 = (5, 1 + \sqrt{-14}),\ p_4 = (5, 1 - \sqrt{-14}).$$

Problem 24. Prove that every nonzero ideal I in $\mathbb{Z}[\omega]$ besides (1) equals the product of several prime ideals.

Problem 25. Prove that if ideals I, J in $\mathbb{Z}[\omega]$ are relatively prime and I divides HJ for an ideal H, then I divides H.

Problem 26. a) Suppose that $a \in \mathbb{Z}[\omega]\backslash\{0\}$ and $(a)I = (a)J$ for ideals $I, J \subset \mathbb{Z}[\omega]$. Prove that $I = J$.
b) Suppose that ideals I, H, J satisfy $H \neq (0)$ and $HI = HJ$. Prove that $I = J$.

Problem 27. Prove that the factorization in Problem 24 is unique up to the order of the factors.

Prime ideals and prime numbers

Problem 28. a) Prove, that every ideal in $\mathbb{Z}[\sqrt{-5}]$ either is principal or equals $((1 + \sqrt{-5})a, 2a)$ for some $a \in \mathbb{Q}[\sqrt{-5}]$.
b) Prove that every ideal in $\mathbb{Z}[\sqrt{-6}]$ either is principal or equals $(\sqrt{-6}a, 2a)$ for some $a \in \mathbb{Q}[\sqrt{-6}]$.

Problem 29. Prove that every nonzero ideal in $\mathbb{Z}[\omega]$ contains a positive integer.

Problem 30. Prove that every prime ideal I in $\mathbb{Z}[\omega]$ contains a unique prime number $p \in \mathbb{Z}, p > 0$.

Problem 31. Suppose I is a prime ideal. Prove that $N(I)$ equals either p or p^2 for some prime number $p \in \mathbb{Z}$.

Problem 32. Prove that prime numbers p in two previous problems coincide.

Problem 33. Prove that for any prime number $p \in \mathbb{Z}$ the ideal $(p) \subset \mathbb{Z}[\omega]$ either is prime or equals to a product of two (not nessesarily distinct) conjugate prime ideals.

Problem 34. Let $P_\omega(x)$ be monic quadratic polynomial with integer coefficients such that $P_\omega(\omega) = 0$. In assumptions of previous problem prove that former case takes place if and only if the equation $P_\omega(x) = 0$ do not have solutions modulo p.

Algebraic numbers

In this section we wish to discuss algebraic numbers together with techniques and problems arising from this notion.

The content of this section is present (as a general rule) in number theory courses of university level, but we believe that this content can be managed by advanced high school students as well.

Definition. A complex number $\alpha \in \mathbb{C}$ is called *algebraic* if it is a root of a nonzero polynomial with rational coefficients. An algebraic number $\alpha \in \mathbb{C}$ is an *algebraic integer* if it is a root of a monic polynomial with integer coefficients. We denote the set of algebraic numbers by $\overline{\mathbb{Q}}$. We denote the set of algebraic integers by $\overline{\mathbb{Z}}$.

Problem 35. Pick $a \in \mathbb{Q}$. Show that if $a \in \overline{\mathbb{Z}}$ then $a \in \mathbb{Z}$.

Problem 36.* Pick $\alpha, \beta \in \overline{\mathbb{Q}}$. Show that $\alpha \pm \beta \in \overline{\mathbb{Q}}$, $\alpha\beta \in \overline{\mathbb{Q}}$, $\alpha/\beta \in \overline{\mathbb{Q}}$ (in the latter case we assume that $b \neq 0$). Hint: use Vieta's formulas.

Problem 37.* Let β be a root of $\alpha_n x^n + \cdots + \alpha_0$ where $\alpha_0, \ldots, \alpha_n \in \overline{\mathbb{Q}}$. Show that $b \in \overline{\mathbb{Q}}$.

Problem 38. a) Define a division-with-remainder procedure for the set of polynomials (in one variable) with coefficients in real numbers, complex numbers and rational numbers.

b) Prove that the unique factorization property holds for the set of polynomials (in one variable) with rational coefficients.

Problem 39. Gauss's lemma for polynomials
Let c_g be the greatest common divisor of the coefficients of $g(x) \in \mathbb{Z}[x]$. Show that, for all nonzero $g_1(x), g_2(x) \in \mathbb{Z}[x]$, we have $c_{g_1 g_2} = c_{g_1} c_{g_2}$.

Problem 40. Can the constructions and the statements of Problem 38 be applied to the set of polynomials with integer coefficients? What about the set of polynomials in two variables with complex coefficients?

Problem 41. Pick an algebraic number α. Let $P_\alpha(x)$ be a monic irreducible polynomial of the least degree such that $P_\alpha(\alpha) = 0$. Prove that if $Q(\alpha) = 0$ for a polynomial $Q(x)$ then P_α divides Q.

Problem 42.* Pick $\alpha, \beta \in \overline{\mathbb{Z}}$. Show that $\alpha \pm \beta \in \overline{\mathbb{Z}}$, $\alpha\beta \in \overline{\mathbb{Z}}$. Hint: use Vieta's formulas.

Problem 43.* Let $\alpha_1, \ldots, \alpha_n$ be algebraic numbers. Show that if $\alpha, \beta \in \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ and $\beta \neq 0$ then $\frac{\alpha}{\beta} \in \mathbb{Q}[\alpha_1, \ldots, \alpha_n]$.

Problem 44.* Pick an algebraic integer α. Let $Q(x)$ be a monic irreducible polynomial with rational coefficients of minimal degree such that $Q(\alpha) = 0$. Prove that the coeffecients of $Q(x)$ are integers.

Problem 45.* Let $f(x)$ be a monic polynomial with integer coefficients such that the absolute values of all roots of $f(x)$ in $\mathbb{C}$ are 1. Show that all roots of $f(x)$ are roots of unity.

3 Ideal classes

Definition. Let $\alpha_1, \ldots, \alpha_k$ be algebraic numbers. Set $\widetilde{\mathbb{Q}} := \mathbb{Q}[\alpha_1, \ldots, \alpha_k]$ and $\widetilde{\mathbb{Z}} := \overline{\mathbb{Z}} \cap \widetilde{\mathbb{Q}}$. Note that subsets of $\mathbb{C}$ which are closed under addition, subtraction and multiplication are called *rings*.

Definition. A nonempty subset I of $\widetilde{\mathbb{Z}}$ is called *ideal* if it is closed under addition, subtraction and multiplication by the elements of $\widetilde{\mathbb{Z}}$.

Definition. We say that two nonzero ideals $I, J \subseteq \widetilde{\mathbb{Z}}$ are *equivalent* ($I \sim J$) if there exist nonzero $\alpha, \beta \in \widetilde{\mathbb{Z}}$ such that $(\alpha)I = (\beta)J$.

Problem 46. Check that $\sim$ is an equivalence relation.

Definition. The equivalence classes of ideals are called *ideal classes* of $\widetilde{\mathbb{Z}}$.

Problem 47. Show that the number of ideal classes in $\widetilde{\mathbb{Z}}$ equals 1 if and only if all ideals in $\widetilde{\mathbb{Z}}$ are principal.

Problem 48. Let I_1, I_2, J_1, J_2 be nonzero ideals in $\widetilde{\mathbb{Z}}$ such that $I_1 \sim I_2$ and $J_1 \sim J_2$. Show that $I_1 J_1 \sim I_2 J_2$.

Problem 49. Describe the ideal classes of $\mathbb{Z}[\sqrt{-5}]$ and $\mathbb{Z}[\sqrt{-6}]$. Can you say anything about the multiplication of these classes?

Problem 50. Let I be a nonzero ideal in $\widetilde{\mathbb{Z}}$ and pick $\alpha \in \widetilde{\mathbb{Z}}$. If $I \subseteq (\alpha)$ then the set $(1/\alpha)I$ is an ideal of $\widetilde{\mathbb{Z}}$.

In the rest of this section we will discuss one the most fundamental statements of Algebraic Number Theory. This statement will play a key role in our proof of a version of the fundamental theorem of arithmetic. The latter proof will be discussed in the subsequent section under the assumption that Theorem 6 is already proven.

Theorem 6. The number of ideal classes in $\widetilde{\mathbb{Z}}$ is finite.

Definition. Consider $x_1, \ldots, x_n \in \widetilde{\mathbb{Q}}$. We say that $\{x_1, \ldots, x_n\}$ is a $\mathbb{Q}$-*basis* of $\widetilde{\mathbb{Q}}$ if every element $\alpha \in \widetilde{\mathbb{Q}}$ can be expressed uniqely in the form

$$m_1 x_1 + \cdots + m_n x_n$$

where $m_1, \ldots, m_n \in \mathbb{Q}$.

Problem 51. Pick an algebraic number α. Show that $\mathbb{Q}[\alpha]$ has a finite $\mathbb{Q}$-basis.

Problem 52. Show that $\widetilde{\mathbb{Q}}$ has a finite $\mathbb{Q}$-basis.

Problem 53. Pick an algebraic number α. Show that there exists a nonzero $n \in \mathbb{Z}$ such that $n\alpha$ is an algebraic integer.

Problem 54. Let $I \subset \widetilde{\mathbb{Z}}$ be a nonzero ideal. Show that there exists a finite set $\alpha_1, \ldots, \alpha_N \in I$ such that every $\alpha \in I$ equals $m_1\alpha_1 + m_2\alpha_2 + \ldots + m_N\alpha_N$ where $m_1, \ldots, m_N \in \mathbb{Z}$ (such $m_1, \ldots, m_N$ need not be unique).

Hint: show that, for a fixed $\mathbb{Q}$-basis of $\widetilde{\mathbb{Q}}$, the coefficients $\alpha \in I$ can't be too small.

Problem 55. Prove that there exists $\alpha_1, \ldots, \alpha_n \in I$ as in Problem 54 such that the respective representation is unique. Hint: use induction on the size of basis.

Definition. We say that $\{\alpha_1, \ldots, \alpha_n\} \subset I$ is an *integer basis* of I if they satisfy the conditions of Problem 55.

Problem 56. Prove that an integer $\mathbb{Q}$-basis of I is a $\mathbb{Q}$-basis of $\widetilde{\mathbb{Q}}$.

Definition. Denote by $\widetilde{\mathbb{Z}}/I$ the equivalence classes of the elements of $\widetilde{\mathbb{Z}}$ with respect to the equivalence relation

$$z_1 \equiv z_2 \mod I \iff z_1 - z_2 \in I.$$

The respective equivalence classes $\widetilde{\mathbb{Z}}/I$ are called *residue classes modulo* I.

Problem 57. Check that residue classes define equivalence classes and that if $\widetilde{\mathbb{Z}} = \mathbb{Z}$ the notion of residue class coincides with congruence classes in modular ariphmetic.

Problem 58. What is the number of elements of $\widetilde{\mathbb{Z}}/I$ for quadratic extensions?

Problem 59. Prove that every $I \neq \{0\}$ contains a nonzero integer.

Problem 60. Prove that the number of elements of $\widetilde{\mathbb{Z}}/I$ is finite.

Problem 61. Pick $\alpha \in \widetilde{\mathbb{Z}} \backslash \{0\}$. Prove that there are only finitely many ideals I such that $\alpha \in I$.

Fix an integer basis $\{\alpha_1, \ldots, \alpha_n$ of $(1) = \widetilde{\mathbb{Z}}\}$. We attach to every $\alpha \in \widetilde{\mathbb{Z}}$ the sequence of integers $(x_1, \ldots, x_n)$ such that $\alpha = x_1\alpha_1 + \ldots + x_n\alpha_n$.

Definition. We say that such a sequence $(x_1, \ldots, x_n)$ is a *vector*. Set $||\alpha|| = |x_1| + |x_2| + \ldots + |x_n|$.

Problem 62. Prove that there exists $M_1 > 0$ such that, for every $\beta \in \widetilde{\mathbb{Z}} \backslash \{0\}$ there exists an integer basis $\{\beta_1, \ldots \beta_n$ of the ideal $(\beta)\}$ such that $||\beta_i|| < M_1||\beta||$ for all i.

Problem 63. Fix $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$. Show that there exists $c \in \widetilde{\mathbb{Z}}$ such that $||\alpha - c\beta|| < nM_1||\beta||$.

Problem 64. Fix $\alpha, \beta \in \widetilde{\mathbb{Z}}$, $\beta \neq 0$. Prove that there exists a positive integer $m \leq (2n^2M_1+1)^n+1 = M_2$ and a nonzero $c \in \widetilde{\mathbb{Z}}$ such that $||m\alpha - c\beta|| < ||\beta||$.

Problem 65. Pick a nonzero ideal $I \subset \widetilde{\mathbb{Z}}$. Show that there exists $\beta \in I$ such that $M_2!I \subseteq (\beta)$. In particular, $M_2! \in (1/\beta)M_2!I$.

Problem 66. Prove that the number of ideal classes in $\widetilde{\mathbb{Z}}$ is finite.

Fundamental Theorem of Arithmetic
The general case

Theorem 7. The Fundamental Theorem of Arithmetic for algebraic integers.
Let $a_1, \ldots, a_n$ be a collection of algebraic integers such that $\mathbb{Z}[a_1, \ldots, a_n]$ coincides with the integers of $\mathbb{Q}[a_1, \ldots, a_n]$. Then, for every nonzero ideal $I \subset \mathbb{Z}[a_1, \ldots, a_n]$, there exists a unique (up to a permutation of the factors) decomposition of I into the product of prime ideals

$$I = p_1 \cdots p_s \subset \mathbb{Z}[a_1, \ldots, a_n].$$

The proof of Theorem 7 splits into two parts: existence of a decomposition and uniqueness of the decomposition. The first part will be solved in Problem 71; the second part will be solved in Problem 76.

Problem 67. Consider $\alpha \in \widetilde{\mathbb{Q}}$ such that $\alpha I \subseteq I$. Show that $\alpha \in \widetilde{\mathbb{Z}}$.
Hint: use an integer basis of I to reformulate the conditions of the theorem. Then use Gauss's method of solving linear equations to construct a monic polynomial $f(x)$ with integer coefficients such that α is a root of $f(x)$.

Problem 68. Let $I, J \subset \widetilde{\mathbb{Z}}$ be nonzdero ideals such that $JI = I$. Show that $J = (1)$. Hint: use ideas of the proof of Problem 67.

Problem 69. a) Let $I \subset \widetilde{\mathbb{Z}}$ be a nonzero ideal. Show that there are positive integers $m > k$ such that $I^k \sim I^m$.

b) Prove that there exists $\alpha \in \widetilde{\mathbb{Z}}$ such that $I^{m-k} = (\alpha)$.

c) Show that for every nonzero ideal $I \subseteq \widetilde{\mathbb{Z}}$ there exist a nonzero ideal $J \subseteq \widetilde{\mathbb{Z}}$ and nonzero $\alpha \in \widetilde{\mathbb{Z}}$ such that $IJ = (\alpha)$.

Problem 70. Let $I, J \subset \widetilde{\mathbb{Z}}$ be nonzero ideals. Show that J divides I if and only if I is contained in J.

Problem 71. Show that every nonzero ideal $I \subseteq \widetilde{\mathbb{Z}}$ is a product of finitely many prime ideals in $\widetilde{\mathbb{Z}}$.

Problem 72. Let I, J, H be nonzero ideals in $\widetilde{\mathbb{Z}}$ such that I and J are relatively prime. Show that if $JH \subseteq I$ then $H \subseteq I$.

Problem 73. Let $p_1, p_2 \subset \widetilde{\mathbb{Z}}$ be prime ideals and $p_1 \neq p_2$. Show that p_1 and p_2 are relatively prime.

Problem 74. Let $I, J \subset \widetilde{\mathbb{Z}}$ such that I is prime. Show that if $I^m \subseteq J$ then $J = I^k$ for some $k \leq m$.

Problem 75. Show that any two powers of two relatively prime ideals are relatively prime.

Problem 76. Prove that the prime ideal factorisation of I in Problem 71 is unique up to a permutation of the factors.

Fundamental Theorem of Arithmetic and Fermat's Last Theorem

Fix $p > 2$ and denote by ζ_p a complex pth root of unity with $\zeta_p \neq 1$. The goal of this part of the project is to prove the following theorem.

Theorem 8. Assume nonzero integers x, y, z satisfy $x^p + y^p = z^p$ and the number of ideal classes of $\mathbb{Z}[\zeta_p]$ is not divisible by p. Then p divides xyz.

We hope that the participants of the project can prove Theorem 8 if they solve the following problems.

Exercise 25. Prove that $1 + \zeta_p + \zeta_p^2 + \cdots + \zeta_p^{p-1} = 0$.

Problem 77. a) Provide a monic polynomial f of degree $p-1$ with integer coefficients such that $1 - \zeta_p$ is a root of f.
b) Show that p divides all the coefficients of this polynomial (except the first one).
c) Prove that f is irreducible in $\mathbb{Q}[x]$.

Exercise 26. Consider rational numbers $a_0, \ldots, a_{p-1}, b_0, \ldots, b_{p-1}$. Show that

$$\Sigma_{i=0}^{p-1} a_i \zeta_p^i = \Sigma_{i=0}^{p-1} b_i \zeta_p^i$$

if and only if

$$a_0 - b_0 = a_1 - b_1 = \cdots = a_{p-1} - b_{p-1}.$$

We say that $\gamma \in \overline{\mathbb{Z}}$ is invertible if $\gamma, 1/\gamma \in \overline{\mathbb{Z}}$.

Problem 78. Prove that $\frac{1-\zeta_p^n}{1-\zeta_p}$ is invertible if $p \nmid n$.

Problem 79. Prove the following equalities of ideals $(1-\zeta_p)^p = (p)$.

Exercise 27. Consider $\alpha \in \mathbb{Z}[\zeta_p]$. Show that if $p \mid \alpha$ then $(1-\zeta_p) \mid \alpha$.

Let $\alpha_0, \ldots, \alpha = \alpha_0 + \cdots + \alpha_{p-1}\zeta_p^{p-1}$.

Problem 80. Prove that all coefficients of the following polynomial are rational:

$$P(a_0, \ldots, a_{p-1}; x) := \Pi_{k=1}^{p-1}(x - \Sigma_{i=0}^{p-1} a_i \zeta_p^{ki}).$$

Recall that $P_\alpha(x)$ denotes the monic polynomial of minimal degree with coefficients in $\mathbb{R}$ such that $P_\alpha(\alpha) = 0$.

Problem 81.* Prove that $P(a_0, \ldots, a_{p-1}; x) = P_a(x)^d$ for some positive integer d.

Problem 82. Assume $P_\alpha(x)$ has integer coefficients. Then for $1 \leq k \leq p-1$ and $l \in \mathbb{Z}$, the sum $\Sigma_{i=0}^{p-1} \alpha_i \zeta_p^{ki+l}$ is an algebraic integer.

Problem 83. Assume $P_\alpha(x)$ has integer coefficients. Prove that $p(a_i - a_j) \in \mathbb{Z}$ for all $0 \leq i, j \leq p-1$.

Problem 84. Show that $1/(1-\zeta_p)$ is not an algebraic integer.

Problem 85. Prove that $\mathbb{Z}[\zeta_p]$ coincides with the set of algebraic integers of $\mathbb{Q}[\zeta_p]$.
Hint: use Exercise 27.

Problem 86. Show that there exists $b \in \mathbb{Z}$ such that $p \mid (\alpha^p - b)$.

Problem 87. a) Prove that $\sqrt{-1} \notin \mathbb{Z}[\zeta_p]$.
b) Consider an odd prime $q \neq p$. Denote by ζ_q a qth root of unity with $q \neq 1$. Show that $\zeta_q \notin \mathbb{Z}[\zeta_p]$.
c) Denote by ζ_{p^2} a root of unity of degree p^2 with $\zeta_{p^2}^p \neq 1$. Show that $\zeta_{p^2} \notin \mathbb{Z}[\zeta_p]$.
d) Find all roots of unity in $\mathbb{Z}[\zeta_p]$.

Problem 88.* Prove that for every invertible element $u \in \mathbb{Z}[\zeta_p]$, there exist $i \in \mathbb{Z}$ and $v \in \mathbb{R}$ such that $u = \zeta_p^i v$.

Let x, y, z, p be as in Theorem 8.

Problem 89. Show that ideals $(x + \zeta_p^i y)$, for $0 \leq i \leq p-1$, are relatively prime to each other.

Problem 90. Prove Theorem 8.

References

[IR] K. Ireland, M. Rosen, *A classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics **84**, Springer-Verlag.

[Mi] J. Milne, *Algebraic number theory*, http://jmilne.org/math/CourseNotes/ANT.pdf.

[C1] K. Conrad, *Factoring in quadratic fields*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/quadraticgrad.pdf.

[C2] K. Conrad, *Ideal factorization*, http://www.math.uconn.edu/∼kconrad/blurbs/gradnumthy/idealfactor.pdf.

[Wa] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer-Verlag, 1996.

[Po] М. Постников, *Теорема Ферма*, Наука, 1978,.

[Go] А. Гончаров, *Арифметика гауссовых чисел*, Журнал "Квант" 12 (1985), http://kvant.mccme.ru/1985/12/.

[SS] В. Сендеров, А. Спивак, *Суммы квадратов и целые гауссовы числа*, Журнал "Квант" 3 (1993), см. также http://kvant.mccme.ru/pdf/1999/03/.

[ZSS] А. Заславский, А. Скопенков, М. Скопенков (редакторы), *Элементы математики в задачах - через олимпиады и кружки к профессии*, 2-ое изд., издательство МЦНМО, 2017.

Замечательные точки многоугольников

А.Заславский, О.Заславский, П.Кожевников, Б.Френкин[1]

Был замысел хорош на диво,
Но рока не перехитришь.
Распорядился он глумливо,
И от горы родилась мышь.

А.Великий

Хорошо известно, что каждый треугольник обладает множеством более или менее интересных свойств. Например, количество так называемых *замечательных точек* в энциклопедии [1] уже перевалило за 10000. Эти точки определяют ряд прямых окружностей и других связанных с треугольником объектов. **Цель проекта (мечта идиота)** — найти аналоги этих объектов в произвольном многоугольнике. Разумеется, реализована она будет в очень малой степени, зато у участников Конференции останется значительный простор для собственных исследований.

1 Центры тяжести многоугольников

Центром тяжести треугольника принято называть точку M пересечения его медиан. Действительно, если расположить в вершинах треугольника равные массы, то их центр тяжести M_0 совпадет с M. В этой же точке находится центр тяжести M_2 треугольника, вырезанного, например, из картона. Однако, для треугольника, сделанного из проволоки, центром тяжести будет другая точка, обозначим ее M_1. Найти ее можно, воспользовавшись следующим общим свойством центров тяжести.

Основное свойство. Пусть фигура F является объединением двух непересекающихся фигур F' и F''. Тогда центр тяжести M фигуры F лежит на отрезке $M'M''$, где M', M'' — центры тяжести F', F'', причем отношение отрезков MM'/MM'' равно отношению m_2/m_1 масс F'' и F'. При этом, если в качестве фигур F', F'' рассматриваются ломаные, то масса фигуры равна ее длине, а для плоских фигур массы равны их площадям.

Строгие определения центров тяжести приведены в приложении.

1.1. Найдите центр тяжести M_1 проволочного треугольника.

1.2. Докажите, что точка M_1, точка пересечения медиан M_0 и центр I вписанной окружности ABC лежат на одной прямой (**прямая Нагеля**), причем M_0 делит отрезок IM_1 в отношении $2:1$.

1.3. Докажите, что M_1 — радикальный центр трех вневписанных окружностей ABC, т.е. касательные, проведенные из M_1 к этим окружностям равны.

[1]Авторы благодарят Д.Крекова за помощь в подготовке проекта

1.4. Докажите, что каждая из прямых A_0M_1, B_0M_1, C_0M_1, где A_0, B_0, C_0 — середины сторон BC, CA, AB соответственно, делит периметр треугольника ABC пополам.

Итак для треугольника можно определить два центра тяжести M_0 и M_1, между которыми существует определенная связь. У произвольного многоугольника может существовать уже три центра тяжести: центр тяжести M_0 его вершин, центр тяжести M_1 периметра и центр тяжести M_2 сплошного многоугольника (для треугольника $M_2 = M_0$).

1.5. Для четырехугольника $ABCD$ найдите точки M_0 и M_2.

1.6. Докажите, что M_0 лежит на отрезке LM_2, где L — точка пересечения диагоналей четырехугольника, и делит его в отношении $3 : 1$.

1.7. Для четырехугольника $ABCD$ найдите точку M_1.

Похоже, что в общем случае точка M_1 не обладает никакими интересными свойствами. Но, если в четырехугольник $ABCD$ можно вписать окружность, то ситуация меняется.

1.8.

a) Докажите, что M_2 лежит на отрезке IM_1, где I центр вписанной окружности, и делит его в отношении $2 : 1$.

b) Докажите, что это свойство верно для любого описанного многоугольника.

1.9. Докажите, что в любом четырехугольнике точка M_0 является серединой отрезка M_1W, где W — середина IL.

Будем теперь рассматривать четырехугольник, который является не только описанным, но и вписанным. По теореме Понселе можно, зафиксировав описанную и вписанную окружности, "вращать" четырехугольник между ними.

1.10. Какие кривые описывают при этом центры тяжести?

Приложение. Определение центров тяжести

Сдавать решения приведенных здесь упражнений необязательно, но за каждое сданное решение участник получает бонус — право рассказать решение одной из задач проекта устно.

Определение 0. Материальной точкой называется пара (X, m), где X — точка плоскости, а m — положительное число ("масса" точки).

Определение 1. Центром масс материальных точек $(X_1, m_1), \ldots, (X_n, m_n)$ называется такая точка M, что

$$m_1\vec{MX}_1 + \cdots + m_n\vec{MX}_n = \vec{0}.$$

Упражнение 1. Докажите существование и единственность центра масс.

Упражнение 2. Докажите, что для любой точки O

$$vecOM = \frac{m_1\vec{OX}_1 + \cdots + m_n\vec{OX}_n}{m_1 + \cdots + m_n}.$$

Упражнение 3. Докажите, что центр масс материальных точек (A, m_1) и (B, m_2) лежит на отрезке AB и делит его в отношении $m_2 : m_1$.

Упражнение 4. Докажите, что центром масс материальных точек $(A, 1)$, $(B, 1)$, $(C, 1)$ является точка пересечения медиан треугольника ABC.

Упражнение 5. Докажите, что центр масс материальных точек $(X_1, m_1), \ldots,$ (X_n, m_n), (X_{n+1}, m_{n+1}) совпадает с центром масс материальных точек $(M, m_1 + \cdots + m_n)$, (X_{n+1}, m_{n+1}), где M — центр масс материальных точек $(X_1, m_1), \ldots,$ (X_n, m_n).

Определение 2. Центром масс n отрезков, каждые два из которых имеют не более одной общей точки называется центр масс материальных точек $(M_1, l_1), \ldots, (M_n, l_n)$, где M_i — середина i-го отрезка, а l_i — его длина.

Определение 3. Пусть фигура F является объединением n треугольников, никакие два из которых не имеют общих внутренних точек. **Центром масс** фигуры F называется центр масс материальных точек $(M_1, S_1), \ldots, (M_n, S_n)$, где M_i — точка пересечения медиан i-го треугольника, а S_i — его площадь.

Упражнение 6. Докажите, что при любом разбиении многоугольника на треугольники центром масс объединения этих треугольников будет одна и та же точка (эта точка называется центром масс многоугольника).

Упражнение 7*. Пусть прямые AB и CD пересекаются в точке E, а прямые AD и BC — в точке F. Докажите, что середины отрезков AC, BD и EF лежат на одной прямой (**прямая Гаусса** четырехугольника $ABCD$).

В проекте под центром тяжести M_0 многоугольника $A_1 \ldots A_n$ подразумевается центр масс материальных точек $(A_1, 1), \ldots, (A_n, 1)$, под центром тяжести M_1 — центр масс отрезков $A_1A_2, \ldots, A_{n-1}A_n, A_nA_1$, под центром тяжести M_2 — центр масс многоугольника.

2 Прямые Эйлера и Нагеля

Известно, что в любом треугольнике центр описанной окружности O, центр тяжести M_0 и ортоцентр H лежат на одной прямой, которая называется **прямой Эйлера**, причем M_0 делит отрезок OH в отношении $1:2$. Также, если A_1, B_1, C_1 — точки касания вписанной окружности со сторонами BC, CA, AB, а точки A_2, B_2, C_2 симметричны A_1, B_1, C_1 относительно середин соответствующих сторон (в этих точках стороны касаются соответствующих вневписанных окружностей), то прямые AA_2, BB_2, CC_2 пересекаются в одной точке N, которая называется **точкой Нагеля**. При этом M_0 лежит на отрезке IN и делит его в отношении $1:2$. Отметим также, что каждая из прямых AA_2, BB_2, CC_2 делит периметр треугольника пополам. Наша цель — найти аналоги прямой Эйлера для вписанного многоугольника и прямой Нагеля для описанного.

2.1. (А.Мякишев, II Олимпиада им. И.Ф.Шарыгина) Пусть четырехугольник $ABCD$ вписан в окружность с центром O; H_a, H_b, H_c, H_d — ортоцентры треугольников BCD, CDA, DAB, ABC соответственно; H — точка пересечения прямых H_aH_c и H_bH_d. Докажите, что центр тяжести M_2 лежит на отрезке OH и делит его в отношении $1:2$.

2.2. (А.Мякишев, II Олимпиада им. И.Ф.Шарыгина) Пусть четырехугольник $ABCD$ описан около окружности с центром I; точки T, U, V, W симметричны точкам касания окружности со сторонами AB, BC, CD, DA относительно середин этих сторон.

a) Докажите, что каждая из прямых TV и UW делит периметр четырехугольника пополам.

b) Пусть N — точка пересечения прямых TV и UW. Докажите, что M_2 лежит на отрезке IN и делит его в отношении $1:2$.

Другой подход к определению прямой Эйлера предложил И.Романов [4].

Определим ортоцентр вписанного n-угольника $A_1 \dots A_n$ по индукции. Пусть $H_1, \dots, H_n$ — ортоцентры $(n-1)$-угольников $A_2 \dots A_n, \dots, A_1 \dots A_{n-1}$ соответственно.

2.3. Докажите, что прямые $A_1H_1, \dots, A_nH_n$ пересекаются в одной точке.

2.4. Назовем полученную в предыдущей задаче точку H ортоцентром n-угольника. Докажите, что центр тяжести M_0 лежит на отрезке OH и делит его в отношении $(n-2):2$.

2.5. Пусть $ABCD$ — произвольный четырехугольник.

Рассматриваем два обобщения ортоцентра:

H^* — центр параллелограмма, образованного ортоцентрами треугольников ABL, BCL, CDL, DAL.

$H^{**} = H_aH_c \cap H_bH_d$, где, как обычно, H_a — ортоцентр треугольника BCD, и т.д..

Далее обобщаем O как $O^{**} = O_aO_c \cap O_bO_d$, где O_a — центр описанной окружности треугольника BCD, и т.д.. (иначе говоря, O^{**} — пересечение серединных перпендикуляров к AC и BD).

Докажите, что

a) M_0 — середина $O^{**}H^*$;

b) (Я. Ганин, А. Мякишев) M_2 лежит на отрезке $O^{**}H^{**}$ и делит его в отношении $1:2$.

c) H^* — середина LH^{**}.

3 Квазицентры описанной и вписанной окружностей

В этой части мы попытаемся для произвольного четырехугольника определить точки O, I, обладающие свойствами центров описанной и вписанной окружностей. Разумеется, для вписанного (описанного) четырехугольника точка O (I) должна совпадать с центром описанной (вписанной) окружности.

3.1. Докажите, что для любого вписанно-описанного четырехугольника $ABCD$ центры O, I и точка пересечения диагоналей L лежат на одной прямой.

3.2. Пусть диагонали четырехугольника $PQRS$ пересекаются в точке I; точки A, B, C, D — проекции I на PQ, QR, RS, SP соответственно. Докажите, что

a) четырехугольник $ABCD$ описанный тогда и только тогда, когда четырехугольник $PQRS$ вписанный;

b) если четырехугольник $ABCD$ описанный, то I — центр его вписанной окружности;

Пусть прямые IA, IB, IC, ID пересекают RS, SP, PQ, QR соответственно в точках A', B', C', D'.

3.3. Докажите, что

a) четырехугольник $ABCD$ вписанный тогда и только тогда, когда $PR \perp QS$;

b) если $PR \perp QS$, то $A'B'C'D'$ — прямоугольник и точки A, B, C, D, A', B', C', D' лежат на одной окружности.

3.4. Восстановите четырехугольник $PQRS$ по точкам A, B, C, D, если известно, что точка I лежит внутри четырехугольника $ABCD$.

Определение. Назовем **квазицентром вписанной окружности** выпуклого четырехугольника $ABCD$ построенную в предыдущей задаче точку I, а **квазицентром описанной окружности** точку O пересечения прямых $A'C'$ и $B'D'$. (Будем считать, что I лежит внутри $ABCD$)

3.5. Докажите, что квазицентры O, I и точка пересечения диагоналей L лежат на одной прямой.

3.6. Для вписанно-описанного четырехугольника выразите радиусы описанной и вписанной окружностей через длины отрезков OI и OL.

Последняя задача позволяет определить для произвольного четырехугольника квазивписанную и квазиописанную окружности. Пока неизвестно, обладают ли эти окружности какими-либо интересными свойствами.

Опишем другой подход к определению квазицентров.

3.7. Пусть I_a, I_b, I_c — центры вневписанных окружностей треугольника ABC; J — центр описанной окружности треугольника $I_aI_bI_c$. Докажите, что O — середина отрезка IJ.

3.8. Докажите, что для произвольного четырехугольника биссектрисы его внутренних углов образуют вписанный четырехугольник и биссектрисы внешних углов также образуют вписанный четырехугольник.

Обозначим центры окружностей четырехугольников, образованных биссектрисам внутренних и внешних углов через I и J соответственно.

3.9. (VII Олимпиада им. И.Ф.Шарыгина) Докажите, что для четырехугольника, вписанного в окружность с центром O точки I и J симметричны относительно O.

Теперь в качестве квазицентров вписанной и описанной окружностей можно взять точку I и середину O отрезка IJ соответственно. К сожалению, определенная таким образом прямая OI может не проходить через точку пересечения диагоналей L.

Еще один подход к определению квазицентра описанной окружности предложен в [6].

3.10. Пусть прямые AB и CD пересекаются в точке X, AD и BC — в точке Y, AC и BD — в точке Z; M_X — точка Микеля прямых AD, BC, AC и BD, M_Y — точка Микеля прямых AB, BD, AC и BD, M_Z — точка Микеля прямых AD, BC, AB и CD. Докажите, что

a) прямые XM_X, YM_Y и ZM_Z пересекаются в одной точке;

b) если точки A, B, C, D лежат на одной окружности, то эти прямые пересекаются в ее центре.

Соответственно полученную в последней задаче точку также можно считать квазицентром описанной окружности.

4 Дополнительные задачи

4.1. Пусть $ABCD$ — четырехугольник, не имеющий параллельных сторон, описанный около окружности с центром I. Точки X, Y, Z, T — точки касания окружности со сторонами AB, BC, CD, DA соответственно. Как всегда, $L = AC \cap BD$ (а также $L = XZ \cap YT$). X' симметрична X относительно середины M_{AB} стороны AB; Y', Z', T' определяются аналогично. $N = X'Z' \cap Y'T'$ — точка Нагеля.

Докажите, что условие $M_0 = I$ эквивалентно следующим условиям:

a) $AX + CZ = BY + DT$;

b) $XZ \parallel X'Z'$ (или $XZ \parallel M_{AB}M_{CD}$);

c) X', Z' и $BC \cap AD$ лежат на одной прямой;

d) L, I, N лежат на одной прямой;

e) (А. Заславский, М. Исаев, Д. Цветов, Всероссийская олимпиада 2005 г.) $IA \cdot IC = IB \cdot ID$.

4.2. (А.Мякишев) Треугольники ABC и $A'B'C'$ называются **ортологичными**, если перпендикуляры, опущенные из A', B', C' соответственно на BC, CA, AB, пересекаются в одной точке. Четырехугольники $ABCD$ и $A'B'C'D'$ называются ортологичными, если ортологичны треугольники ABC и $A'B'C'$, BCD и $B'C'D'$, CDA и $C'D'A'$, DAB и $D'A'B'$. Пусть четырехугольники $ABCD$ и

$A'B'C'D'$ ортологичны, диагонали AC и BD пересекаются в точке L, $A'C'$ и $B'D'$ — в точке L'. Докажите, что $AL : LC = A'L' : L'C'$ и $BL : LD = B'L' : L'D'$ (т.е. ортологичные четырехугольники аффинно эквивалентны).

Список литературы

[1] http://faculty.evansville.edu/ck6/encyclopedia/ETC.html.

[2] Ф.Ивлев. Центры тяжести многоугольников. Доклад на ММКШ. 2008. https://www.mccme.ru/circles/oim/mmks/notes.htm

[3] A.Akopyan. Some remarks on the circumcenter of mass. https://arxiv.org/pdf/1512.08655.pdf

[4] И.Романов. Прямая Эйлера n-угольника. Доклад на ММКШ. 2017. https://www.mccme.ru/circles/oim/mmks/works2017/ignatov2.pdf

[5] А.Заславский. Диагонально-перпендикулярное отображение четырехугольников. Квант. 1998. №4.

[6] M.Rolnek, Le Anh Dung. The Miquel Points, Pseudocircumcenter, and Euler-Poncelet Point of a Complete Quadrilateral. Forum Geometricorum V.14 (2014). https://personal.us.es/rbarroso/trianguloscabri/sol/FG201413.pdf.

Замечательные точки многоугольников
Решения

1 Центры тяжести многоугольников

1.1. **Ответ.** Центр окружности, вписанной в треугольник $A_0B_0C_0$.

Доказательство. Так как точки A_0, B_0, C_0 являются серединами отрезков BC, CA, AB, поместим в них массы, равные длинам этих отрезков. Тогда центром тяжести масс в точках A_0, B_0 будет точка, делящая отрезок A_0B_0 в отношении $AC : BC = A_0C_0 : B_0C_0$, т.е. основание биссектрисы треугольника $A_0B_0C_0$. Следовательно, центр тяжести всех трех масс лежит на этой биссектрисе. Аналогично получаем, что он лежит и на других биссектрисах треугольника $A_0B_0C_0$ и, значит, совпадает с центром вписанной в этот треугольник окружности (рис.1).

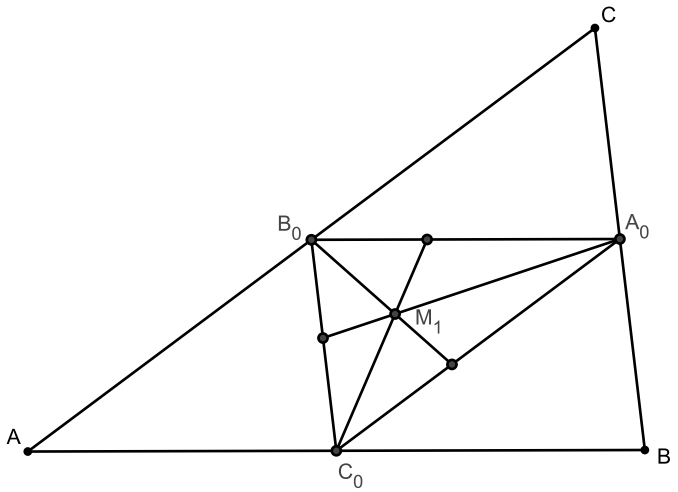


Рис. 1

1.2. Следует из предыдущей задачи и гомотетичности треугольников ABC, $A_0B_0C_0$ относительно I.

1.3. Пусть вневписанные окружности, касающиеся сторон AC и BC, касаются продолжений стороны AB в точках X, Y. Тогда $BX = AY = p$ (полупериметр треугольника) и, значит, $C_0X = C_0Y$. Кроме того, линия центров этих окружностей перпендикулярна биссектрисе угла C, а значит, и параллельной ей прямой C_0M_1. Таким образом, M_1 лежит на радикальной оси этих окружностей. Аналогично получаем, что M_1 лежит на радикальной оси любой другой пары вневписанных окружностей.

1.4. Пусть, например, C_0M_1 пересекает сторону AC в точке X. Из предыдущей задачи следует, что X делит пополам отрезок между точками касания прямой AC с вневписанными окружностями, касающимися сторон AC и BC (рис.2). Поскольку расстояния от этих точек до вершины A равны соответственно $p - c$ и p, то $AX = p - c/2$ и $AX + AC_0 = p$.

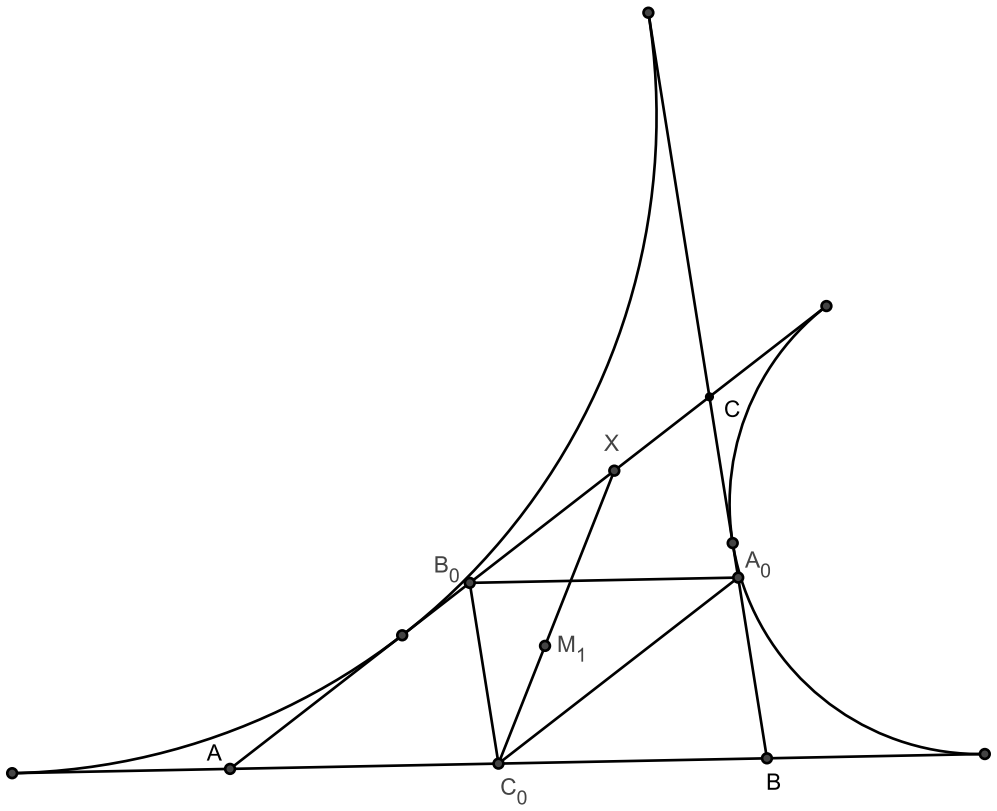


Рис. 2

1.5. **Ответ.** M_0 — центр параллелограмма $PQRS$, где P, Q, R, S — середины сторон AB, BC, CD, DA. M_2 — точка пересечения прямой l_1, соединяющей центры тяжести треугольников ABC и ADC, с прямой l_2, соединяющей центры тяжести треугольников ABD и BCD.

1.6. Пусть U, V — середины диагоналей AC и BD, L — точка их пересечения. Центр тяжести треугольника ABC лежит на его медиане BU и делит ее в отношении $2:1$. Аналогично центр тяжести треугольника ACD лежит на DU и делит ее в том же отношении. Прямая l_1, проходящая через эти центры, параллельна диагонали BD и пересекает диагональ AC в точке, которая делит отрезок UL в отношении $1:2$. Аналогично M_2 лежит на прямой, параллельной AC и делящей отрезок VL в отношении $1:2$. Отметим, что если провести прямые, параллельные AC и BD, через M_0, то они разделят отрезки UL и VL пополам. Отсюда вытекает утверждение задачи (рис.3).

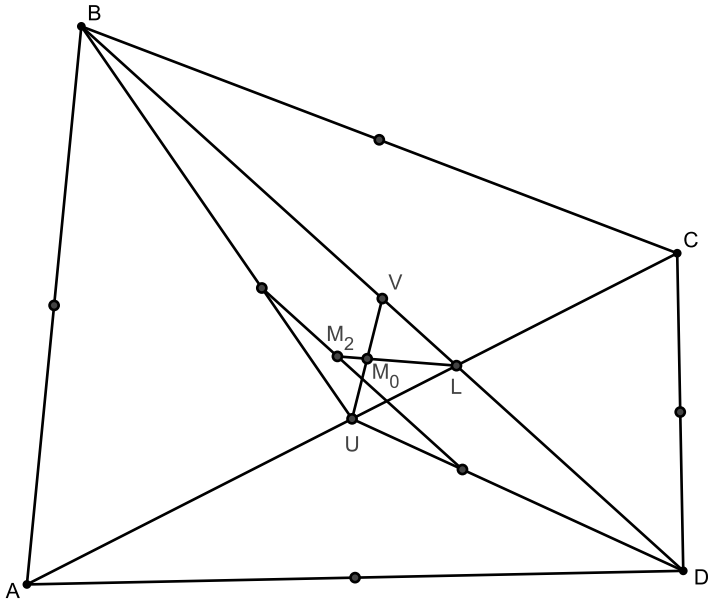


Рис. 3

1.7. Так как P и Q — центры тяжести отрезков AB и BC, центр тяжести X_1 объединения этих отрезков лежит на PQ и $PX_1/QX_1 = BC/AB$. Построить эту точку можно следующим образом: проведем биссектрису BB' треугольника BPQ и найдем точку, симметричную B' относительно середины отрезка PQ. Аналогично строятся центры тяжести X_2, Y_1, Y_2 ломаных CDA, DAB, BCD. M_1 — это точка пересечения прямых X_1X_2 и Y_1Y_2 (рис.4).

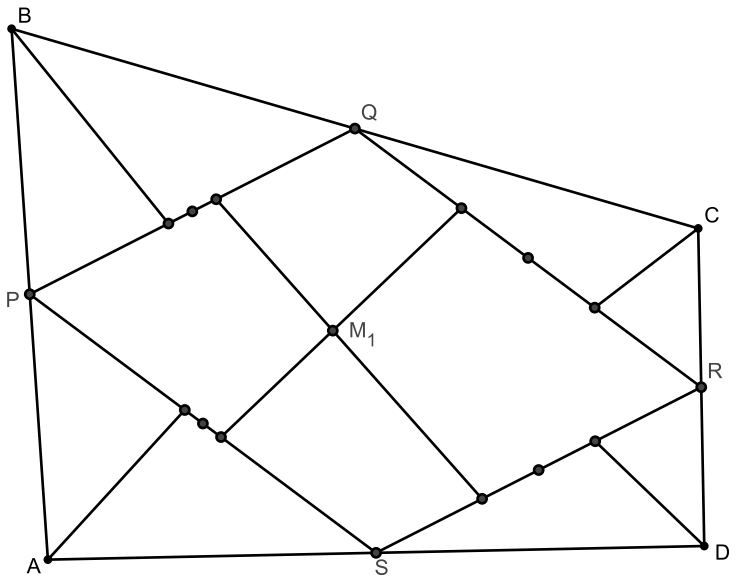


Рис. 4

1.8.

a) Центры тяжести (сплошных) треугольников IAB, IBC, ICD, IDA, где I — центр вписанной окружности, делят их медианы IP, IQ, IR, IS в отношении 2 : 1, т.е. образованный ими четырехугольник гомотетичен $PQRS$ с центром I и коэффициентом $\frac{2}{3}$. Так как площади треугольников IAB, IBC, ICD, IDA относятся так же, как соответствующие стороны $ABCD$, M_1 при этой гомотетии переходит в M_2.

b) Доказательство аналогично.

1.9. Следует из двух предыдущих задач и теоремы о центрах трех гомотетий.

1.10. **Указание.** Точка M_0 — середина отрезка между серединами диагоналей четырехугольника. Используя тот факт, что прямая Гаусса описанного четырехугольника проходит через центр вписанной окружности, нетрудно вывести, что траектория M_0 — окружность. Теперь, применив соответствующие гомотетии, получаем, что и траектории двух других центров — окружности (рис.5).

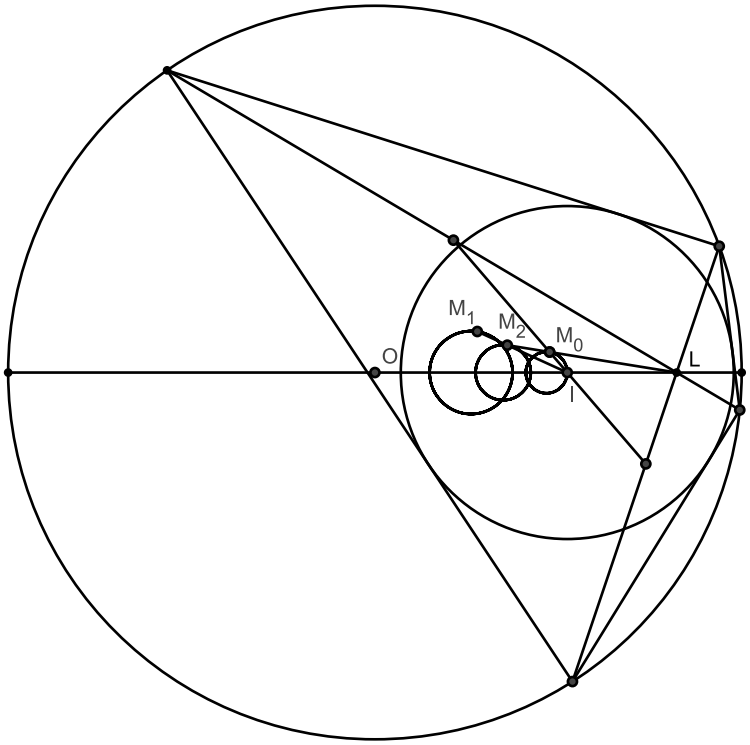


Рис. 5

2 Прямые Эйлера и Нагеля

2.1. Пусть M_a и H_a — соответственно центроид (точка M_2) и ортоцентр треугольника BCD. Центроиды и ортоцентры остальных трех треугольников обозначим аналогично. Все треугольники имеют общую описанную окружность с центром в O. Рассмотрев прямые Эйлера этих треугольников, заметим, что четырехугольник $M_aM_bM_cM_d$ переходит в четырехугольник $H_aH_bH_cH_d$ при гомотетии с центром в O и коэффициентом 3. Соответственно, точки пересечения диагоналей этих четырехугольников переходят друг в друга.

2.2.

a) Из определения следует, что $AT + DV = BC$, $BT + CV = AD$, т.е. $TA + AD + DV = VC + CB + BT$.

b) Пусть a, b, c, d — длины касательных к вписанной окружности из вершин A, B, C, D. Очевидно, что, если поместить в A, B, C, D массы a, b, c, d, то центром тяжести полученной системы будет точка N, а, если поместить в вершины массы $2a+b+d$, $2b+a+c$, $2c+b+d$, $2d+c+a$, то — точка M_1. Осталось показать, что I — центр тяжести масс $b+d$, $a+c$, $b+d$, $a+c$ и воспользоваться утверждением задачи 1.8.

Точка I удовлетворяет соотношению $S_{IAB} - S_{IBC} + S_{ICD} - S_{IDA} = 0$. Этому же соотношению удовлетворяют середины U и V диагоналей четырехугольника. Следовательно, эти три точки лежат на одной прямой (это утверждение называется *теоремой Монжа*). Пусть теперь X, Y — точки касания вписанной окружности со сторонами BC и AD. Тогда прямая XY образует равные углы с этими сторонами и по теореме Брианшона проходит через точку L пересечения диагоналей. Применив теорему синусов к треугольникам LXB и LYD, получим, что $BL/DL = b/d$. Аналогично, $AL/CL = a/c$. Отсюда и из соотношений $S_{UBC}/S_{UAD} = BL/DL$, $S_{VBC}/S_{VAD} = CL/AL$, $S_{IBC}/S_{IAD} = (b+c)/(a+d)$ вытекает, что I делит отрезок AC в отношении $(a+c)/(b+d)$, что и требуется.

2.3. **Указание.** Примените индукцию.

2.4. **Указание.** Примените индукцию.

2.5. a) Пусть M_{AC}, M_{BD} — середины диагоналей AC, BD. Очевидно, что $O^{**}M_{AC} \perp AC$ и $O^{**}M_{BD} \perp BD$. С другой стороны $H^*M_{AC} \perp BD$ и $H^*M_{BD} \perp AC$, потому что H^* — центр параллелограмма, стороны которого перпендикулярны диагоналям четырехугольника и проходят через его вершины. Следовательно, $H^*M_{AC}O^{**}M_{BD}$ — параллелограмм, откуда и следует утверждение задачи.

b) **Указание.** Воспользуйтесь утверждением задачи 4.2.

c) Очевидно следует из двух предыдущих пунктов.

3 Квазицентры описанной и вписанной окружностей

3.1. Воспользуемся следующим утверждением.

Лемма. Пусть точка P лежит внутри окружности с центром O. Два перпендикулярных луча с началом P пересекают окружность в точках X, Y. Тогда геометрическим местом точек пересечения касательных к окружности в X и Y будет окружность с центром, лежащим на OP.

Доказательство. Пусть Z — четвертая вершина прямоугольника $PXZY$. Так как $OP^2 + OZ^2 = OX^2 + OY^2$, Z описывает окружность с центром O. Значит, середина отрезка XY описывает окружность, центром которой является середина OP, и инверсная к ней точка пересечения касательных также описывает окружность.

Теперь утверждение задачи следует из того факта, что прямые, соединяющие точки касания противоположных сторон четырехугольника с вписанной окружностью, перпендикулярны и проходят через точку пересечения его диагоналей.

3.2. Так как четырехугольники $IAQB$, $IBRC$ вписанные, то $\angle IBA = \angle IQA$, $\angle IBC = \angle IRC$, откуда следуют оба утверждения.

3.3. Доказательство аналогично предыдущей задаче.

3.4. Будем считать, что лучи PQ и SR пересекаются в точке X. Тогда $\angle PXS = \angle PIS - \angle IPA - \angle CSI$. Из вписанности четырехугольников $IAPD$, $ICSD$ получаем, что $\angle IPA + \angle CSI = \angle CDA$. Кроме того, $\angle PIS = \angle RIQ = (\angle PAD + \angle DCS + \angle RCB + \angle BAQ)/2 = (\angle ABC + \angle CDA)/2$. Следовательно, $\angle AIC = \pi - \angle PXS = \pi - (\angle ABC - \angle CDA)/2$ (рис.6). Найдя аналогично угол BID мы сможем построить точку I как точку пересечения соответствующих дуг окружностей, а затем и четырехугольник $PQRS$.

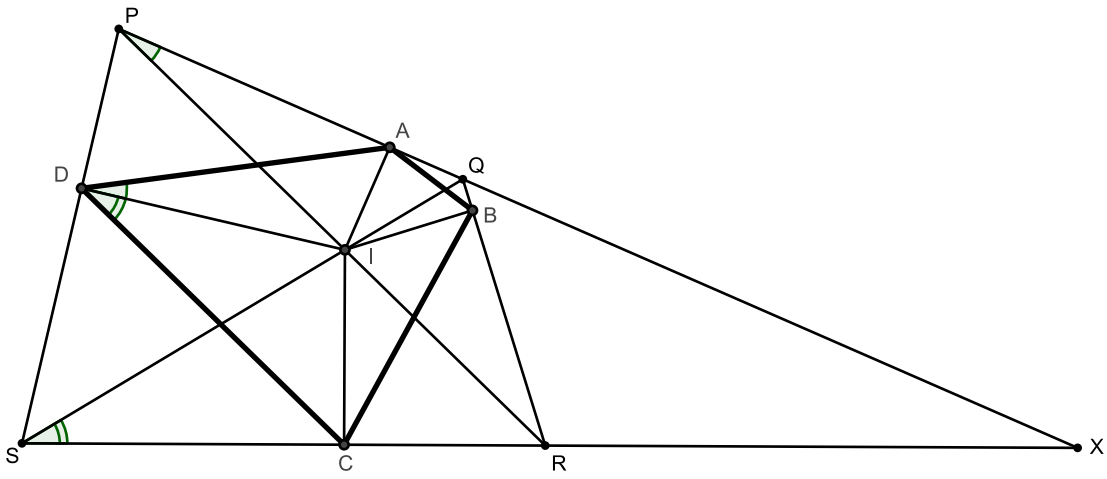


Рис. 6

3.5. **Указание.** Примените центральную проекцию, переводящую точки P, Q, R, S в вершины параллелограмма.

3.6. **Ответ.** $R^2 = \frac{OL \cdot OI^2}{2OI - OL}$, $r^2 = \frac{(R^2 - OI^2)^2}{2(R^2 + OI^2)}$.

Указание. По теореме Понселе достаточно рассмотреть четырехугольник, одна из диагоналей которого является диаметром описанной окружности.

3.7. **Указание.** Докажите, что отрезки I_aJ, I_bJ, I_cJ перпендикулярны соответствующим сторонам треугольника ABC.

3.8. Доказывается непосредственным вычислением углов.

3.9. Пусть биссектрисы углов A и B пересекаются в точке K, B и C — в точке L, C и D — в точке M, D и A — в точке N (рис.9.4). Тогда прямая KM — биссектриса угла между AD и BC. Обозначив этот угол через ϕ, по теореме о внешнем угле получаем, что $\angle LKM = \angle B/2 - \phi/2 = (\pi - \angle A)/2 = \angle C/2$ и, значит, $\angle LIM = \angle C$. С другой стороны, перпендикуляры из L на BC и из M на CD образуют с ML углы, равные $(\pi - \angle C)/2$, т.е. треугольник, образованный этими перпендикулярами и ML, — равнобедренный с углом при вершине, равным углу C. Поэтому вершина этого треугольника совпадает с I. Таким образом, перпендикуляры, опущенные из вершин четырехугольника $KLMN$ на соответствующие стороны $ABCD$, проходят через I (рис.7). Аналогично получаем, что перпендикуляры из вершин четырехугольника, образованного внеш-

ними биссектрисами, проходят через J.

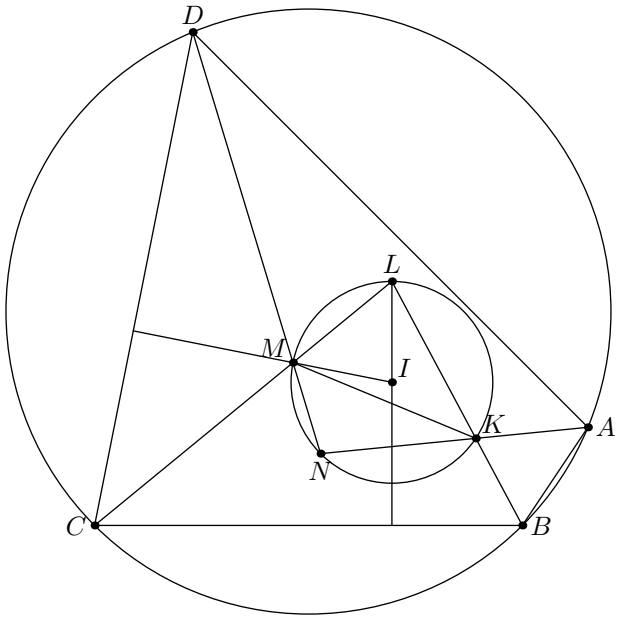


Рис. 7

Пусть теперь K' — точка пересечения биссектрис внешних углов A и B. Так как четырехугольник $AKBK'$ вписан в окружность с диаметром KK', то проекции K и K' на AB симметричны относительно середины AB. Отсюда и из утверждения, доказанного выше, следует, что проекции I и J на каждую из сторон $ABCD$ симметричны относительно середины этой стороны, что равносильно утверждению задачи.

3.10. См. [6].

Список литературы

[1] http://faculty.evansville.edu/ck6/encyclopedia/ETC.html.

[2] Ф.Ивлев. Центры тяжести многоугольников. Доклад на ММКШ. 2008. https://www.mccme.ru/circles/oim/mmks/notes.htm

[3] A.Akopyan. Some remarks on the circumcenter of mass. https://arxiv.org/pdf/1512.08655.pdf

[4] И.Романов. Прямая Эйлера n-угольника. Доклад на ММКШ. 2017. https://www.mccme.ru/circles/oim/mmks/works2017/ignatov2.pdf

[5] А.Заславский. Диагонально-перпендикулярное отображение четырехугольников. Квант. 1998. №4.

[6] M.Rolnek, Le Anh Dung. The Miquel Points, Pseudocircumcenter, and Euler-Poncelet Point of a Complete Quadrilateral. Forum Geometricorum V.14 (2014). https://personal.us.es/rbarroso/trianguloscabri/sol/FG201413.pdf.

Remarkable points of polygons

A.Zaslavsky, B.Frenkin, P.Kozhevnikov, O.Zaslavsky[1]

It is well-known that any triangle has many various, more or less remarkable points. For instance, the number of so-called *triangle centers* in the encyclopedia [1] has already exceeded 10000. These points define various lines, circles and other objects related to the triangle. **The aim of this project (our pipe dream)** is to find analogues of these objects in an arbitrary polygon. Of course, it will be realized in the least, but on the other hand the participants of the Conference will have a large scope for their own research.

1 Barycenters of polygons

The centroid of a triangle is the point M of concurrence of its medians. Indeed, if we place equal weights in the vertices of a triangle, their barycenter M_0 will coincide with M. The same point is the barycenter M_2 of a triangle cut out from cardboard for example. However the barycenter of a triangle made of wire differs from these points. Denote it by M_1. It can be determined using the following general property of barycenters.

The main property. Suppose some figure F is a disjoint union of figures F' and F''. Then the barycenter M of F lies on the segment $M'M''$, where M', M'' are the barycenters of F' and F'' respectively. Moreover, the ratio MM'/MM'' equals the ratio m_2/m_1 of masses of F'' and F'. Here, if the figures F' and F'' are piecewise linear curves, then the weight of a figure is proportional to its length, and for plane figures the weights are proportional to their areas.

1.1. Find the barycenter M_1 of a triangle made of wire.

1.2. Prove that the point M_1, the point M_0 of concurrence of medians and the incenter I of ABC are collinear (the **Nagel line**), moreover M_0 divides IM_1 in the ratio $2:1$.

1.3. Prove that M_1 is the radical center of three excircles of ABC, i.e., the segments of tangents from M_1 to these circles are equal.

1.4. Prove that each of the lines A_0M_1, B_0M_1, C_0M_1, where A_0, B_0, C_0 are the middle points of the segments BC, CA, AB respectively, bisects the perimeter of ABC.

So, for any triangle we can define two barycenters M_0 and M_1, and they are somehow connected to each other. An arbitrary polygon can have three barycenters: the barycenter M_0 of its vertices, the barycenter M_1 of the union of its sides and the barycenter M_2 of the whole polygon (in the degenerate case of a triangle we have $M_2 = M_0$).

1.5. Determine points M_0 and M_2 for a quadrilateral $ABCD$.

1.6. Prove that M_0 lies on the segment LM_2, where L is the intersection point of the diagonals of the quadrilateral, and M_0 divides LM_2 in the ratio $3:1$.

[1]The authors are grateful to D.Krekov for the help in the preparing of the project

1.7. Determine point M_1 for a quadrilateral $ABCD$.

It seems that generally the point M_1 has no remarkable properties. However for a circumscribed $ABCD$ the situation is different.

1.8.

a) Show that M_2 lies on the segment IM_1, where I is the incenter, and divides it in the ratio $2:1$.

b) Show that the same is true for any circumscribed polygon.

1.9. Show that in any quadrilateral, M_0 is the midpoint of the segment M_1W, where W is the midpoint of IL.

Now consider a quadrilateral which is not only circumscribed, but inscribed as well. Poncelet theorem then asserts that one can fix the incircle and the circumcircle and "rotate" the quadrilateral between them.

1.10. What is the locus of each barycenter of the quadrilateral?

Appendix. Definition of barycenters

It is not obligatory to deliver the solutions of exercises given here, but each delivered solution gives a bonus to the participant, namely the right to tell the solution of one problem of the project orally.

Definition 0. Material point is a pair (X, m), where X is a point of the plane, and m is a positive number ("the mass" of the point).

Definition 1. The mass center of material points $(X_1, m_1), \dots, (X_n, m_n)$ is the point M such that

$$m_1\overrightarrow{MX_1} + \cdots + m_n\overrightarrow{MX_n} = \overrightarrow{0}.$$

Exercise 1. Prove that there exists a unique mass center.

Exercise 2. Prove that for any point O

$$\overrightarrow{OM} = \frac{m_1\overrightarrow{OX_1} + \cdots + m_n\overrightarrow{OX_n}}{m_1 + \cdots + m_n}.$$

Exercise 3. Prove that the mass center of material points (A, m_1) and (B, m_2) lies on the segment AB and dissects it in the ratio $m_2 : m_1$.

Exercise 4. Prove that the mass center of material points $(A, 1)$, $(B, 1)$, $(C, 1)$ coincides with the centroid of triangle ABC.

Exercise 5. Prove that the mass center of material points $(X_1, m_1), \dots, (X_n, m_n)$, (X_{n+1}, m_{n+1}) coincides with the mass center of material points $(M, m_1 + \cdots + m_n)$, (X_{n+1}, m_{n+1}), where M is the mass center of $(X_1, m_1), \dots, (X_n, m_n)$.

Definition 2. The mass center of n segments having at most one common point pairwise is the mass center of material points $(M_1, l_1), \dots, (M_n, l_n)$, where M_i is the midpoint of i-th segment, and l_i is its length.

Definition 3. Let F be the union of n triangles having no common inner points pairwise. **The mass center** of F is the mass center of material points $(M_1, S_1), \dots, (M_n, S_n)$, where M_i is the centroid of i-th triangle, and S_i is its area.

Exercise 6. Prove that for any division of a polygon into triangles, the mass center of the union of these triangles is the same point (called the **mass center of the polygon**).

Exercise 7^***.** Let lines AB and CD meet at point E, and lines AD and BC meet at point F. Prove that the midpoints of segments AC, BD and EF are on a line (**the Gauss line** of quadrilateral $ABCD$).

In this project the barycenter M_0 of a polygon $A_1 \dots A_n$ denotes the mass center of material points $(A_1, 1), \dots, (A_n, 1)$, the barycenter M_1 denotes the mass center of segments $A_1A_2, \dots, A_{n-1}A_n, A_nA_1$, and the barycenter M_2 denotes the mass center of the polygon.

2 Euler and Nagel lines

It is well known that in any triangle the circumcenter O, the centroid M_0 and the orthocenter H lie on a line, which is called **Euler line**. Moreover M_0 divides the segment OH in the ratio $1:2$. Furthermore let A_1, B_1, C_1 be the points of tangency of the incircle with the sides BC, CA, AB respectively, and the points A_2, B_2, C_2 are symmetric to A_1, B_1, C_1 with respect to the midpoints of the corresponding sides (these are the points of tangency of the sides with the corresponding excircles). Then the lines AA_2, BB_2, CC_2 concur at the point N which is called **Nagel point**. One can show that M_0 lies on the segment IN and divides it in the ratio $1:2$. Also note that each of the lines AA_2, BB_2, CC_2 divides the perimeter of the triangle in two equal parts. Our goal is to find analogues of the Euler line for an inscribed polygon and the Nagel line for a circumscribed one.

2.1. (A. Myakishev, II Sharygin olimpiad) Let $ABCD$ be an inscribed quadrilateral and O be its circumcenter. Let H_a, H_b, H_c, H_d be the orthocenters of triangles BCD, CDA, DAB, ABC respectively, and H be the intersection point of the lines H_aH_c and H_bH_d. Show that the barycenter M_2 lies on the segment OH and divides it in the ratio $1:2$.

2.2. (A. Myakishev, II Sharygin olympiad) Let $ABCD$ be a circumscribed quadrilateral, and I be its incenter. Let T, U, V, W be the points which are symmetric to the points of tangency of the incircle with the sides AB, BC, CD, DA respectively with respect to their midpoints.

a) Show that any of lines TV and UW divides the perimeter of the quadrilateral into two equal parts.

b) Let N be the point of intersection of lines TV and UW. Prove that M_2 lies on the segment IN and divides it in the ratio $1:2$.

Another approach to the definition of the Euler line was proposed by I.Romanov [4].

Define the orthocenter of an inscribed n-gon $A_1 \dots A_n$ inductively. Let $H_1, \dots, H_n$ be the orthocenters of $(n-1)$-gons $A_2 \dots A_n$,$\dots$,$A_1 \dots A_{n-1}$ respectively.

2.3. Prove that the lines $A_1H_1, \dots, A_nH_n$ are concurrent.

2.4. Let us call the corresponding intersection point H the orthocenter of the n-gon. Show that the barycenter M_0 lies on the segment OH and divides it in the ratio $(n-2):2$.

2.5. Let $ABCD$ be an arbitrary quadrilateral.

Consider two generalizations of the orthocenter:

H^* is the center of the parallelogram formed by the orthocenters of triangles ABL, BCL, CDL, DAL;

$H^{**} = H_aH_c \cap H_bH_d$, where as usual H_a is the orthocenter of triangle BCD, and so on.

Furthermore we generalize O as $O^{**} = O_aO_c \cap O_bO_d$ where O_a is the circumcenter of triangle BCD, and so on (in other words, O^{**} is the intersection of perpendicular bisectors to AC and BD).

Prove that

a) M_0 is the midpoint of $O^{**}H^*$;

b) (Ya. Ganin, A. Myakishev) M_2 lies on the segment $O^{**}H^{**}$ and divides it as $1:2$;

c) H^* is the midpoint of LH^{**}.

3 Quasi-centers of the circumcircle and the incircle

In this section we will try to define the points O and I for an arbitrary quadrilateral, which have the properties similar to those of the circumcenter and the incenter. Of course, for an inscribed (resp. circumscribed) quadrilateral the point O (resp. I) should coincide with the center of the circumcircle (resp. the incircle).

3.1. Show that for any quadrilateral $ABCD$ which is both inscribed and circumscribed, the centers O, I and the intersection point L of diagonals are collinear.

3.2. Let I be the intersection point of the diagonals of a quadrilateral $PQRS$. Denote the projections of I to PQ, QR, RS, SP by A, B, C, D respectively. Show that

a) the quadrilateral $ABCD$ is circumscribed iff the quadrilateral $PQRS$ is inscribed;

b) if the quadrilateral $ABCD$ is circumscribed then I is its incenter.

Let A', B', C', D' be the intersection points of lines IA, IB, IC, ID with RS, SP, PQ, QR respectively.

3.3. Prove that

a) the quadrilateral $ABCD$ is inscribed iff $PR \perp QS$;

b) if $PR \perp QS$, then $A'B'C'D'$ is a rectangle and the points A, B, C, D, A', B', C', D' are concyclic.

3.4. Construct a quadrilateral $PQRS$ by the points A, B, C, D if it is known that I lies inside $ABCD$.

Definition. Define the **quasi-incenter** of a convex quadrilateral $ABCD$ to be the point I constructed in the previous problem, and the **quasi-circumcenter** to be the intersection point O of the lines $A'C'$ and $B'D'$. (We assume that I lies inside $ABCD$)

3.5. Show that the quasi-centers O, I and the intersection point L of the diagonals are collinear.

3.6. For a quadrilateral which is both inscribed and circumscribed express the circumradius and the inradius in terms of lengths of the segments OI and OL.

The last problem enables us to define the quasi-incircle and the quasi-circumcircle for an arbitrary quadrilateral. Up to date it is unknown whether these circles have any interesting properties.

Now let us describe another approach to defining quasi-centers.

3.7. Let I_a, I_b, I_c be the excenters of the triangle ABC, and J be the circumcenter of $I_aI_bI_c$. Prove that O is the midpoint of the segment IJ.

3.8. Prove that for an arbitrary quadrilateral, its internal angle bisectors form an inscribed quadrilateral, and so do the external angle bisectors.

Denote by I and J the circumcenters of the quadrilaterals formed by the internal angle bisectors and the external angle bisectors of $ABCD$ respectively.

3.9. (VII Sharygin olimpiad) Show that for an inscribed quadrilateral with circumcenter O, the points I and J are symmetric with respect to O.

Now we can take I and the midpoint O of the segment IJ to be the quasi-incenter and the quasi-circumcenter. Unfortunately, with this definition the intersection point L of the diagonals can be not contained in the line OI.

One more approach to defining the quasi-circumcenter is proposed in [6].

3.10. Let X be the intersection point of lines AB and CD, Y be the intersection point of AD and BC, Z be the intersection point of AC and BD. Let M_X be the Miquel point of lines AD, BC, AC and BD, $M_Y$be the Miquel point of AB, BD, AC и BD, and M_Z be the Miquel point of AD, BC, AB и CD. Prove that

a) the lines XM_X, YM_Y and ZM_Z are concurrent;

b) if the points A, B, C, D are concyclic then these lines intersect at the circumcenter of $ABCD$.

The obtained point can also be considered as a quasi-circumcenter.

4 Additional problems

4.1. Let $ABCD$ be a quadrilateral without parallel sidelines circumscribed around a circle centered at I. The sides AB, BC, CD, DA touche the incircle at points X, Y, Z, T respectively. As usually $L = AC \cap BD$ (also $L = XZ \cap YT$). Let X' be the reflection of X about the midpoint M_{AB} of side AB; Y', Z', T' are defined similarly; $N = X'Z' \cap Y'T'$ is the Nagel point.

Prove that the condition $M_0 = I$ is equivalent to each of the following conditions:

a) $AX + CZ = BY + DT$;

b) $XZ \parallel X'Z'$ (или $XZ \parallel M_{AB}M_{CD}$);

c) X', Z' and $BC \cap AD$ are collinear;

d) L, I, N a collinear;

e) (A.Zaslavsky, M.Isaev, D.Tsvetov, All-Russian olympiad 2005 г.) $IA \cdot IC = IB \cdot ID$.

4.2. (A.Myakishev) Triangles ABC and $A'B'C'$ are called **ortologic**, if the perpendiculars from A', B', C' to BC, CA, AB respectively concur. Quadrilaterals $ABCD$ and $A'B'C'D'$ are called ortologic, if the triangles ABC and $A'B'C'$, BCD and $B'C'D'$, CDA and $C'D'A'$, DAB and $D'A'B'$ are ortologic. Let $ABCD$ and $A'B'C'D'$ be ortologic, AC and BD meet at L, $A'C'$ and $B'D'$ meet at L'. Prove that $AL : LC = A'L' : L'C'$ and $BL : LD = B'L' : L'D'$ (i.e. ortologic quadrilaterals are affine equivalent).

Список литературы

[1] http://faculty.evansville.edu/ck6/encyclopedia/ETC.html.

[2] Ф.Ивлев. Центры тяжести многоугольников. Доклад на ММКШ. 2008. https://www.mccme.ru/circles/oim/mmks/notes.htm

[3] A.Akopyan. Some remarks on the circumcenter of mass. https://arxiv.org/pdf/1512.08655.pdf

[4] И.Романов. Прямая Эйлера n-угольника. Доклад на ММКШ. 2017. https://www.mccme.ru/circles/oim/mmks/works2017/ignatov2.pdf

[5] А.Заславский. Диагонально-перпендикулярное отображение четырехугольников. Квант. 1998. No. 4.

[6] M.Rolnek, Le Anh Dung. The Miquel Points, Pseudocircumcenter, and Euler-Poncelet Point of a Complete Quadrilateral. Forum Geometricorum. V.14 (2014). https://personal.us.es/rbarroso/trianguloscabri/sol/FG201413.pdf.

Remarkable points of polygons
Solutions

1 Barycenters of polygons

1.1. **Answer.** The incenter of the triangle $A_0B_0C_0$.

Proof. Note that the points A_0, B_0, C_0 are the midpoints of the segments BC, CA, AB, so let us place the weights equal to the lengths of these segments in this points. Then the barycenter of the weights in the points A_0 and B_0 is the point, which divides the segment A_0B_0 in the ratio $AC : BC = A_0C_0 : B_0C_0$, i.e. the base of the angle bisector in $A_0B_0C_0$, therefore the barycenter of all three weights lies on this bisector. Analogously, we deduce that it lies on the other angle bisectors of $A_0B_0C_0$ too, hence it coincides with, its incenter (fig.1).

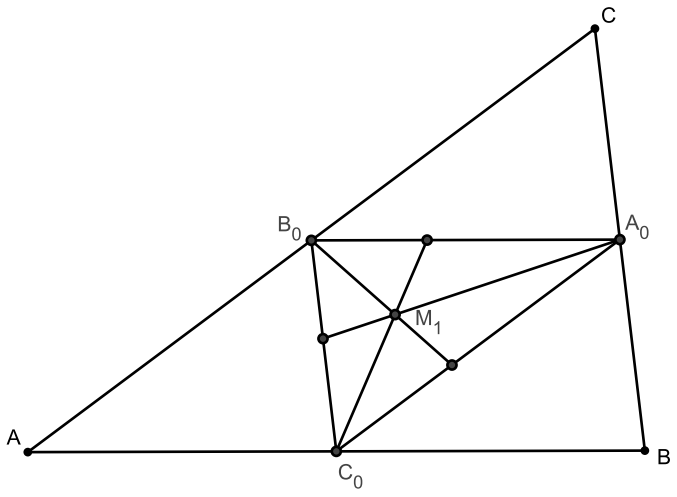


Fig. 1

1.2. It follows from the previous problem and the fact that the triangles ABC and $A_0B_0C_0$ are homothetic with the center at I.

1.3. Denote by X and Y the points of tangency of excircles, which are tangent to the segments AC and BC, with the line AB. We have $BX = AY = p$ (where p

is the semiperimeter of the triangle), hence $C_0X = C_0Y$. Moreover, the line passing through the centers of these circles is orthogonal to the angle bisector of C, hence, it is also orthogonal to the line C_0M_1. THus we obtain that M_1 lies on the radical axis of these teo circles. Arguing in the same way we deduce that M_1 lies on the radical axis of any pair of the three excircles.

1.4. Let X be the intersection of C_0M_1 with the segment AC. It follows from the previous problem that X is the midpoint of the segment with the ends at the tangency points of the line AC with the excircles, which are tangent to the segments AC and BC (fig.2). As the distances from these points to A are equal to $p - c$ and p respectively, we obtain that $AX = p - c/2$ and $AX + AC_0 = p$.

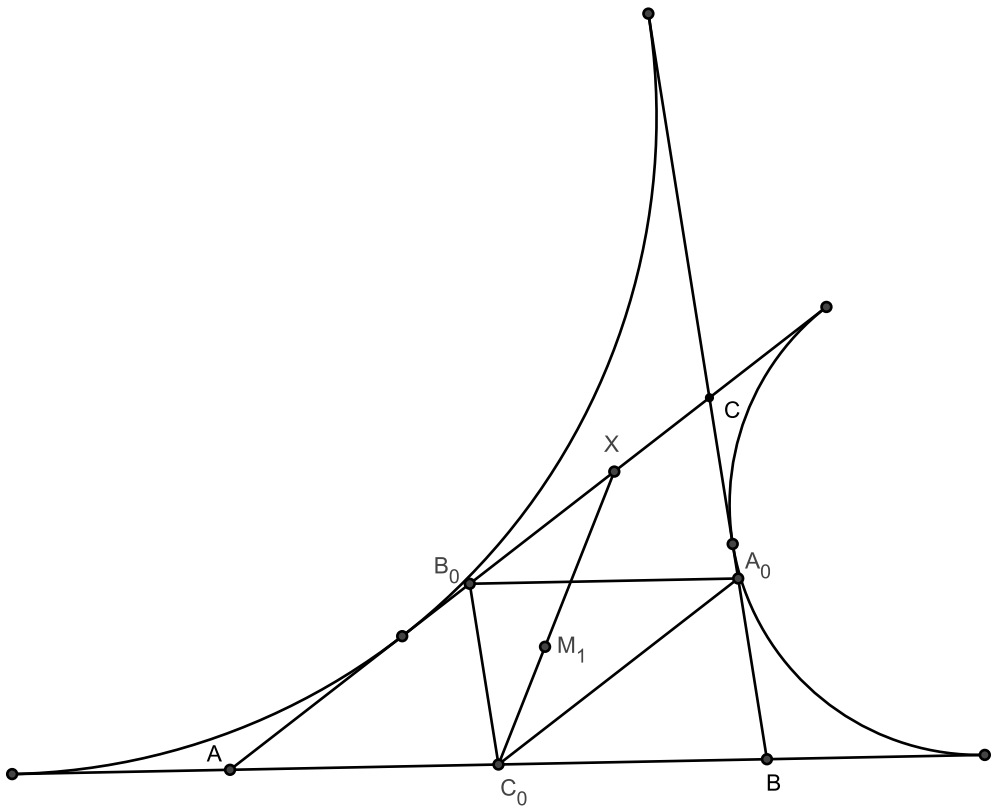


Fig. 2

1.5. **Answer.** M_0 is the center of the parallelogram $PQRS$, where P, Q, R, $S$are the midpoints of AB, BC, CD, DA. $M_2$is the intersection point of the line l_1, passing through the centroids of ABC and ADC, and the line l_2, passing through the centroids of ABD and BCD.

1.6. Let U, V be the midpoints of the diagonals AC and BD respectively and L be their intersection point. The centroid of ABC lies on its median BU and divides

it in the ratio $2:1$. Analogously, the centroid of ACD lies on DU and divides it in the same ratio. The line l_1, passing through these centroids, is parallel to BD and it intersects AC at the point, which divides the segment UL in the ratio $1:2$. In the same way we obtain that M_2 lies on the line, which is parallel to AC and which divides the segment VL in the ratio $1:2$. Note that the lines passing through M_0 parallel to AC and BD pass through the midpoints of the segments UL and VL respectively. The assertion of the problem now follows straightforwardly (fig.3).

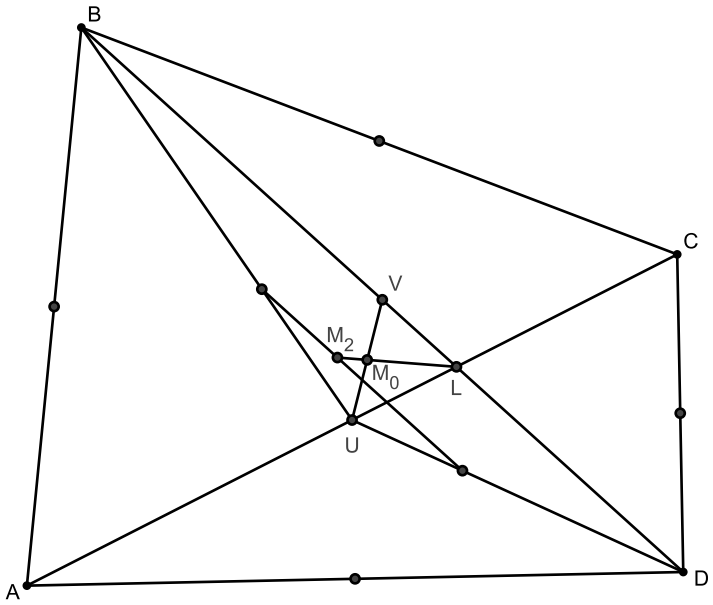


Fig. 3

1.7. As P and Q are the barycenters of the segments AB and BC, we obtain that the barycenter X_1 of their union lies on PQ and $PX_1/QX_1 = BC/AB$. This point mat be constructed in the following way: construct the angle bisector BB' of the triangle BPQ and take a point, which is symmetric to B' with respect to the midpoint of PQ. Analogously one can construct the barycenters X_2, Y_1, Y_2 of the piecewise linear curves CDA, DAB, BCD. Then $M_1$is the intersection point of the lines X_1X_2 and Y_1Y_2 (fig.4).

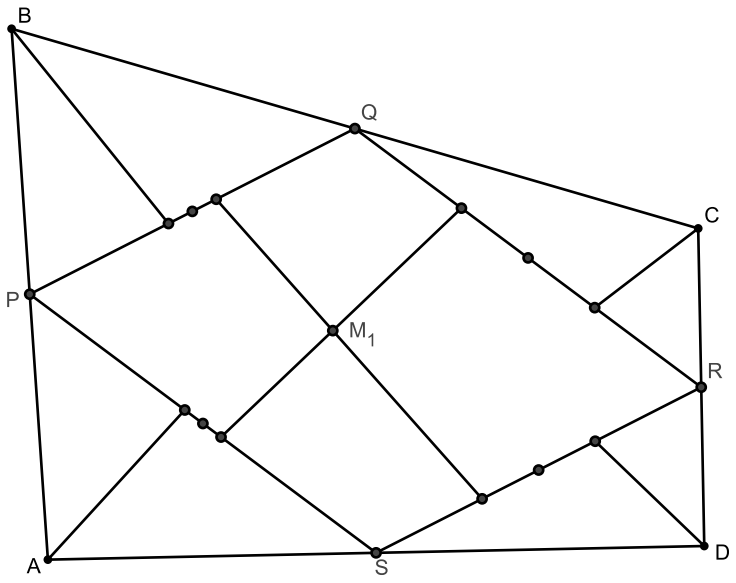


Fig. 4

1.8.

a) Let I be the incenter. The centroids of the (solid) triangles IAB, IBC, ICD, IDA divide their medians IP, IQ, IR, IS in the ratio $2:1$, i.e. the quadrilateral, which is formed by them, is homothetical to $PQRS$ with the center in I and the coefficient $\frac{2}{3}$. As the ratio of the areas of IAB, IBC, ICD, IDA is the same as the ratio of the corresponding sides of $ABCD$, this homothety maps M_1 to M_2.

b) The proof is analogous to the previous one.

1.9. It follows from the previous problems and the theorem about three homothety centers.

1.10. **Hint.** M_0 is the midpoint of the segment, formed by the midpoints of the diagonals of the quadrilateral. Note that the Gauss line of the circumscribed quadrilateral contains its incenter. This fact implies that the locus of M_0 is a circle. Now one can use the corresponding homotheties to deduce that the loci of two other centers are also circles (fig.5).

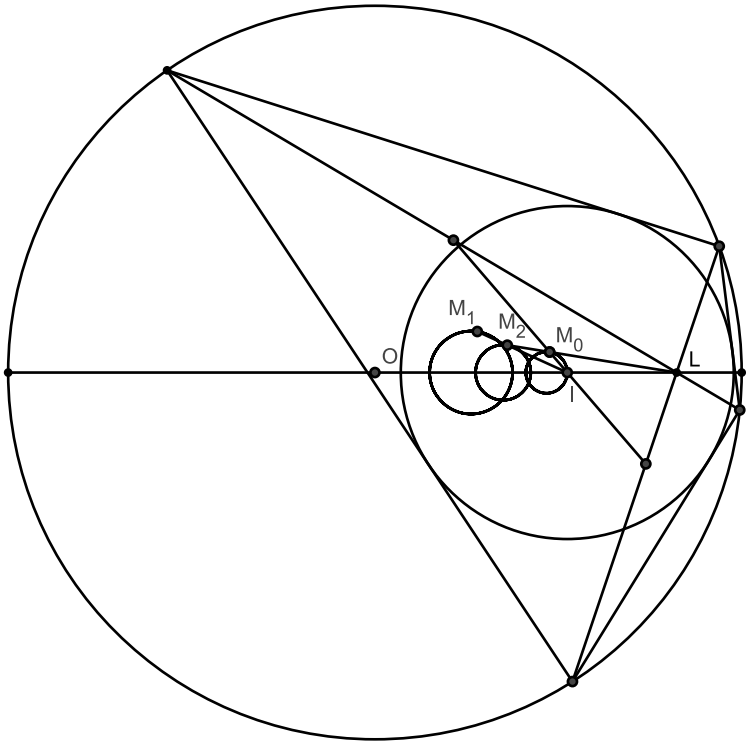


Fig. 5

2 Euler and Nagel points

2.1. Let M_a and H_a be the centroid (the point M_2) and the orthocenter of BCD respectively. Denote the centroids and the orthocenters of the other triangles analogously. All there triangle share a common circumcircle, whose center is O. By considering the Euler lines of these triangles, we note that the quadrilateral $M_aM_bM_cM_d$ is mapped to the quadrilateral $H_aH_bH_cH_d$ under the homothety with the center in O and the coefficient 3, so the intersection points of the corresponding diagonals are mapped to each other analogously.

2.2.

a) It follows from the definition that $AT + DV = BC$, $BT + CV = AD$, i.e. $TA + AD + DV = VC + CB + BT$.

b) Let a, b, c, d be the length of tangent segments to the incircle from the vertices A, B, C, D. It is clear that if one places the weights a, b, c, d into the points A, B, C, D respectively, then the barycenter of the obtained system is the point N, and if one places the weights $2a+b+d$, $2b+a+c$, $2c+b+d$, $2d+c+a$ into those vertices, then the barycenter is the point M_1. It remains to show that I is the barycenter of the weights $b + d$, $a + c$, $b + d$, $a + c$ and apply the assertion of problem 1.8..

The point I satisfies $S_{IAB} - S_{IBC} + S_{ICD} - S_{IDA} = 0$. The same property holds for the midpoints U and V of the diagonals of the quadrilateral, therefore these points are concurrent (this fact is called *the Monge theorem*). Now let X and Y be the tangency points of the incircle with the sides BC and AD respectively. Then the angles formed by the line XY and these sides are equal and also XY passes through the intersection point of the diagonals L by Brianchon's theorem. Applying the laws of sines to the triangles LXB and LYD, we obtain that $BL/DL = b/d$. Similarly, $AL/CL = a/c$. These identities and the equalities $S_{UBC}/S_{UAD} = BL/DL$, $S_{VBC}/S_{VAD} = CL/AL$, $S_{IBC}/S_{IAD} = (b+c)/(a+d)$ imply that I divides the segment AC in the ratio $(a + c)/(b + d)$, QED.

2.3. **Hint.** Use induction.

2.4. **Hint.** Use induction.

2.5. a) Let M_{AC}, M_{BD} be the midpoints of diagonals AC, BD. It is clear that $O^{**}M_{AC} \perp AC$ and $O^{**}M_{BD} \perp BD$. On the other hand $H^*M_{AC} \perp BD$ and $H^*M_{BD} \perp AC$ because H^* is the center of the parallelogram having the sidelines perpendicular to the diagonals of the given quadrilateral and passing through its vertices. Hence $H^*M_{AC}O^{**}M_{BD}$ is a parallelogram which yields the required assertion.

b) **Hint.** Use the assertion of problem 4.2.

c) Clearly follows from two previous assertions.

3 Quasi-centres of the circumcircle and the incircle

3.1. We use the following fact.

Lemma. Suppose the point P lies inside the circle with the center at O. Denote by X and Y the intersection points of the circle with two orthogonal half-lines with the initial point at P. Then the locus of the intersection points of the tangent lines

to the circle at X и Y is a circle with the center, lying on OP.

Proof. Let Zbe the fourth vertex of the rectangle $PXZY$. We have $OP^2+OZ^2 = OX^2 + OY^2$, thus the locus of Z is the circle with the center at O. Hence the locus of the midpoint of the segment XY is a circle with the center at the midpoint of OP, so the locus of the intersection of the tangent lines, which is inverse to it, is also a circle.

Now the assertion follows from the fact that the lines, passing through the tangency points of the opposite sides of the quadrilateral with the incircle, are orthogonal and they both pass through the intersection point of its diagonals.

3.2. As the quadrilaterals $IAQB$ and $IBRC$ are inscribed, we have $\angle IBA = \angle IQA$, $\angle IBC = \angle IRC$, which imply both assertions.

3.3. The proof is similar to the previous problem.

3.4. Suppose that the half-lines PQ and SR intersect at X. Then we have $\angle PXS = \angle PIS - \angle IPA - \angle CSI$. The quadrilaterals $IAPD$ and $ICSD$ are inscribed, thus we obtain that $\angle IPA + \angle CSI = \angle CDA$. Besides, $\angle PIS = \angle RIQ = (\angle PAD + \angle DCS + \angle RCB + \angle BAQ)/2 = (\angle ABC + \angle CDA)/2$. Therefore, $\angle AIC = \pi - \angle PXS = \pi - (\angle ABC - \angle CDA)/2$. Arguing in the same way we can find the angle BID and thus to construct I as the intersection point of the corresponding arcs of the circles, and then we are able to construct the quadrilateral (fig.6).

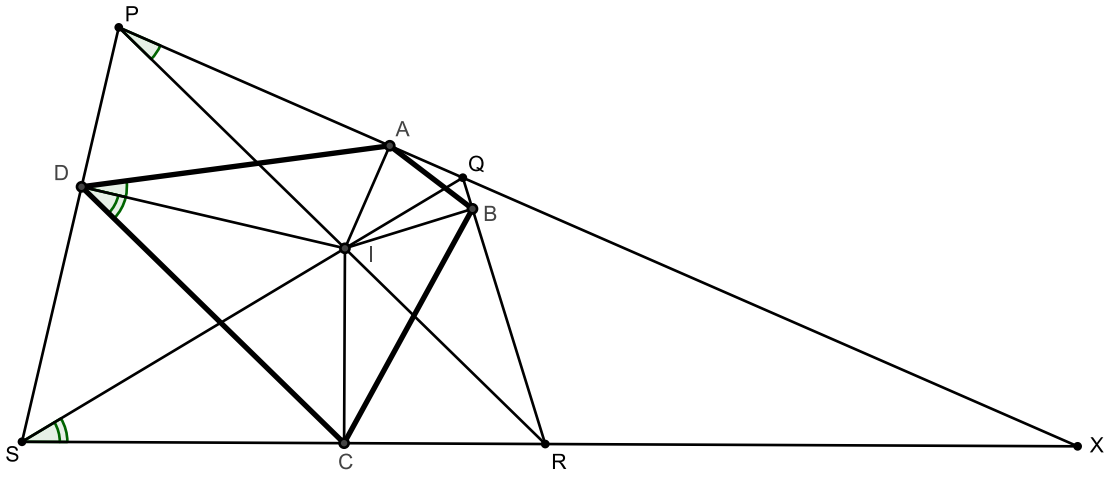


Fig. 6

3.5. **Hint.** Apply the central projection, which maps the points P, Q, R, S to the vertices of a parallelogram.

3.6. **Answer.** $R^2 = \frac{OL \cdot OI^2}{2OI - OL}$, $r^2 = \frac{(R^2 - OI^2)^2}{2(R^2 + OI^2)}$.

Hint. It follows from Poncelet theorem that it is enough to consider the quadrilateral having a diameter of the circumcircle as one of the diagonals.

3.7. **Hint.** Prove that the segments I_aJ, I_bJ, I_cJ are orthogonal to the corresponding sides of the triangle ABC.

3.8. One can prove this by a direct computation of angles.

3.9. Let the angle bisectors of A and B intersect at K, the angle bisectors of B and C — at L, the angle bisectors of C and D — at M, the angle bisectors of D and A — at N (pic.9.4). Then the line KM is the bisector of the angle, formed by AD and BC. Denote this angle by ϕ, exterior angle theorem implies that $\angle LKM = \angle B/2 - \phi/2 = (\pi - \angle A)/2 = \angle C/2$,hence $\angle LIM = \angle C$. On the other side, the line through L orthogonal to BC and the line through M orthogonal to CD form with ML the angles, equal to $(\pi - \angle C)/2$, i.e. the triangle, formed by these lines and ML is isosceles and its vertex angle is equal to C. Thus its vertex coincides with I. Therefore the lines through the vertices of $KLMN$ orthogonal to the respective sides of $ABCD$ pass through I (fig.7). Similarly we obtain that the perpendiculars from the vertices of the quadrilateral formed by the exterior angle bisectors pass through J.

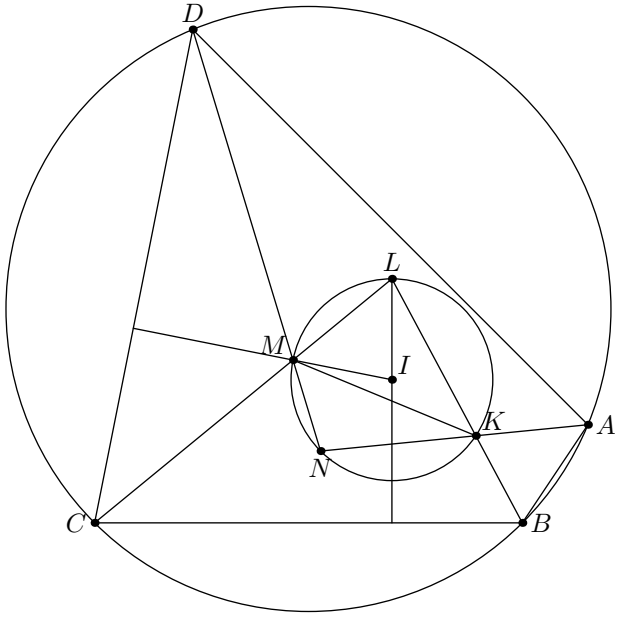


Fig. 7

Now let K'be the intersection points of the exterior bisectors of A and B. As the quadrilateral $AKBK'$ is inscribed in a circle with the diameter KK', we obtain that the projections of K and K' to AB are symmetric with respect to the midpoint of AB. From this assertion and the one, proved above, it follows that the projections of

I and J to each of the sides of $ABCD$ are symmetric with respect to the midpoints of the corresponding sides, which is equivalent to the assertion of the problem.

3.10. See [6].

Список литературы

[1] http://faculty.evansville.edu/ck6/encyclopedia/ETC.html.

[2] Ф.Ивлев. Центры тяжести многоугольников. Доклад на ММКШ. 2008. https://www.mccme.ru/circles/oim/mmks/notes.htm

[3] A.Akopyan. Some remarks on the circumcenter of mass. https://arxiv.org/pdf/1512.08655.pdf

[4] И.Романов. Прямая Эйлера n-угольника. Доклад на ММКШ. 2017. https://www.mccme.ru/circles/oim/mmks/works2017/ignatov2.pdf

[5] А.Заславский. Диагонально-перпендикулярное отображение четырехугольников. Квант. 1998. №4.

[6] M.Rolnek, Le Anh Dung. The Miquel Points, Pseudocircumcenter, and Euler-Poncelet Point of a Complete Quadrilateral. Forum Geometricorum V.14 (2014). https://personal.us.es/rbarroso/trianguloscabri/sol/FG201413.pdf.

Вокруг теоремы Кэли

Задачу представляют Бурсиан О., Кохась Д., Кохась К.

Версия 0.99

Этот проект посвящен теореме Кэли о числе деревьев. Дерево — это связный граф без циклов. Теорема утверждает, что число помеченных деревьев с n вершинами равно n^{n-2}. Известно много доказательств этой теоремы, нашей целью будет познакомиться с некоторыми из них и изучить приложения различных подходов к этой теореме.

В каждом проекте есть довольно сложные задачи. По правилам конференции задачи можно решать, объединившись в команды; задачи разных проектов можно решать в составе разных команд. Мы советуем вам найти попутчиков, с которыми вам было бы интересно проводить исследования, описанные в этом проекте.

Задачи для первого знакомства

В олимпиадных задачах обычно используются графы с «обезличенными» вершинами — например, вершины — это какие-то города, а ребра — дороги между ними, или вершины — это люди (обычно безымянные), а ребра — это знакомства и т.п. В задачах о перечислении графов принята другая точка зрения — все вершины графа должны быть «индивидуальны». Чтобы не было диссонанса в терминологии, мы введем понятие «помеченный граф».

Пусть $[n] = \{1, 2, \ldots, n\}$. Дерево (или вообще произвольный граф) на n вершинах, вершины которого пронумерованы числами от 1 до n, называется *помеченным деревом* (соответственно *помеченным графом*). Чтобы построить помеченное дерево, можно взять дерево и расставить в его вершинах числа, или наоборот: мы можем считать, что множество $[n]$ — это множество вершин, и мы рисуем граф-дерево, соединяя эти вершины ребрами. Множество помеченных деревьев на n вершинах обозначим через $\mathcal{T}_n$.

Два (непомеченных) графа G_1 и G_2 с множеством вершин V_1 и V_2 называются *изоморфными* (или, попросту говоря, считаются одинаковыми), если существует такое взаимно однозначное отображение $f\colon V_1 \to V_2$, что вершины A, $B \in V_1$ соединены ребром в G_1 тогда и только тогда, когда $f(A)$ и $f(B)$ соединены ребром в G_2. Например, любое дерево с четырьмя вершинами изоморфно либо дереву «куриная лапа», либо дереву «путь длины три». В случае, когда G_1 и G_2 — помеченные графы, $V_1 = V_2 = [n]$ и в качестве f в этом определении берут тождественное отображение.

Мы предполагаем, что при решении задач разделе «Задачи для первого знакомства» теорема Кэли не должна использоваться. В формулировках задач через T_n обозначается количество помеченных деревьев на n вершинах, и вопрос о нахождении этой величины не ставится. Нумерация задач дана в соответствии с последующими разделами.

1.1. Граф называется *униццикли́ческим*, если он связный и содержит ровно один цикл. Докажите, что помеченных деревьев со 100 вершинами больше, чем помеченных униццикли́ческих графов с 98 вершинами.

1.2. Постройте взаимно однозначное соответствие между множеством, которое состоит из всевозможных отображений множества $[n]$ в себя, и множеством помеченных деревьев на n вершинах, в которых одна вершина снабжена красной меткой и одна — синей меткой (может оказаться, что обе метки поставлены возле одной и той же вершины).

1.3. Существует n^{n-1} различных отображений из множества $[n-1]$ в $[n]$. Докажите тождество

$$\sum_{j=1}^{n} C_{n-1}^{j-1}(n-j)^{n-j}T_j = n^{n-1},$$

разбив множество этих отображений на n частей так, чтобы j-е слагаемое оказалось равно количеству отображений в j-й части.

3.1. Дерево с n вершинами, ребра которого пронумерованы числами от 1 до $n-1$, называется *реберно помеченным*. Например, существует 4 различных реберно помеченных дерева на 4 вершинах — см. рис. 1. Докажите, что при $n \geqslant 3$ количество различных реберно помеченных деревьев на n вершинах равно $\frac{1}{n}T_n$.

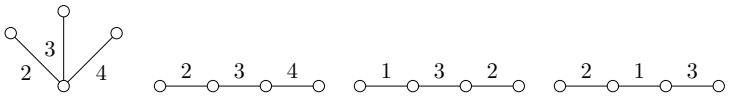


Рис. 1. Реберно помеченные курлапа и пути длины 3

Если мы выделили в дереве (помеченном или нет) одну из вершин, то будем называть такое дерево *корневым*, а саму отмеченную вершину будем называть *корнем*. Если же нам потребуется подчеркнуть, что ни одна из вершин нами не выделена, будем называть такое дерево *свободным*. *Листом* дерева называется вершина степени 1, за исключением случая, когда дерево корневое и корень имеет степень 1, в этом случае корень листом не считается. *Лес* — это граф, в котором каждая компонента связности является деревом.

Обозначим через $\mathcal{F}_n^k$ множество лесов на множестве вершин $[n]$, состоящих из k корневых деревьев с корнями 1, 2, …, k, причем таких, у которых вершина n находится в дереве с корнем 1 (рис. 2).

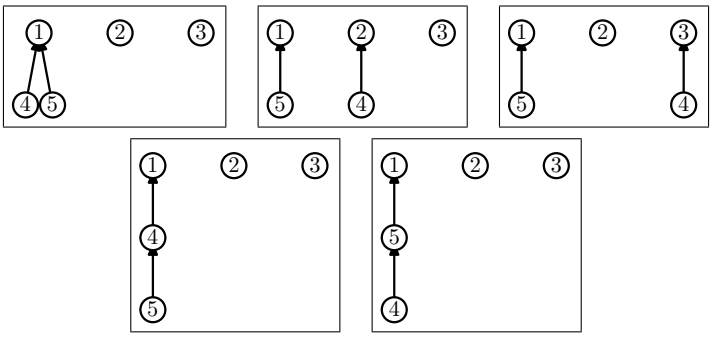


Рис. 2. Множество лесов $\mathcal{F}_5^3$. Мы ориентировали ребра «от периферии к корню»

Множества мы обозначаем «рукописными» буквами. Число элементов множества обозначается той же буквой в курсивном начертании. Так число в множестве $\mathcal{F}_n^k$ будем обозначать F_n^k.

1.4. Докажите, что при $2 \leqslant k \leqslant n-1$ выполняется рекуррентное соотношение

$$F_n^{k-1} = nF_n^k.$$

1.5. Пусть $V_1 = [r]$, $V_2 = \{r+1, \ldots, r+s\}$, $V = V_1 \cup V_2 = [r+s]$. Обозначим через $\mathcal{F}_{r,s}^k$ множество лесов, состоящих из k корневых деревьев с множеством вершин V с корнями 1, 2, …, k, у которых вершина $r+1$ находится в дереве с корнем 1, а у каждого ребра одна вершина из множества V_1, а другая — из множества V_2. Придумайте рекурсию (по k) для величины $F_{r,s}^k$

Вдоль улицы с односторонним движением расположено n мест для парковки автомобиля. На улицу въезжают последовательно n автомобилей с номерами от 1 до n в порядке возрастания. Каждый водитель едет к своему любимому месту парковки и, если оно не занято, припарковывается; в противном случае он едет дальше до первого свободного места и припарковывается там, если же все места дальше заняты, он уезжает (насовсем). Последовательностью предпочтений назовем список a_1, a_2, …, a_n любимых мест парковки первого, второго, …, n-го водителя.

4.1. Докажите, что существует $(n+1)^{n-1}$ последовательностей предпочтений, для которых все водители сумеют припарковаться.

4.2. Докажите, что успех или неуспех парковки на самом деле не зависит от порядка, в котором прибывают машины.

Следующая задача лежит в стороне от нашего сюжета. Но она позволяет понять, какие затруднения могут возникнуть, если мы станем перечислять непомеченные деревья.

3.2. Докажите, что количество различных (т. е. неизоморфных друг другу) непомеченных деревьев с n вершинами меньше 4^n.

1 Рекурсии, тождества, биекции

1.6. Докажите при помощи комбинаторных рассуждений (интерпретируя числа T_i как количества деревьев), что при $n > 1$ а) $T_n = \dfrac{n}{2}\displaystyle\sum_{k=0}^{n-2} C_{n-2}^k T_{k+1} T_{n-k-1}$;

b) Сведите эту формулу, а также формулы из задач 1.3 и 5.1 а) друг к другу алгебраически.

1.7. Обозначим через $\mathcal{T}(n,k)$ множество помеченных корневых деревьев с n вершинами, в которых корень — вершина 1 — имеет степень k. Докажите, что

$$(n-1)(k-1)T(n,k) = (n-k)T(n,k-1).$$

«Треугольным деревом» назовем граф, определеямый по индукции следующим образом. Самое маленькое треугольное дерево вопреки своему названию — это полный граф на двух вершинах. Если уже задано какое-нибудь треугольное дерево, мы можем взять любое ребро AB в нем, взять новую вершину C и добавить к дереву вершину C и ребра AC, BC. Помеченным треугольным деревом будем называть треугольное дерево, у которого вершины пронумерованы числами от 1 до n.

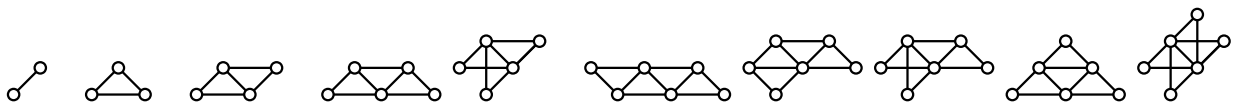


Рис. 3. Непомеченные треугольные деревья на 2, 3, 4, 5 и 6 вершинах.

Например, для $n = 5$ имеется 2 непомеченных треугольных дерева (рис. 3) и 70 помеченных.
Если некоторое ребро треугольного дерева выделено, то такое дерево будем называть «корневым».

1.8. Обозначим через $\Delta(n,k)$ число корневых помеченных треугольных деревьев на n вершинах, у которых корневое ребро принадлежит k треугольникам. Придумайте рекурсию (по k) для величины $\Delta(n,k)$.

2 Код Прюфера

Код Прюфера сопоставляет дереву с занумерованными вершинами последовательность его вершин следующим образом. Код Прюфера дерева с двумя вершинами — пустое слово. Если количество вершин дерева T больше двух, то обозначим через v лист с минимальным номером, а через u вершину, смежную с v. Тогда код Прюфера дерева T получается из кода Прюфера дерева $T - v$ приписыванием слева вершины u.

Проверьте, что Вы умеете решать задачу 2.1, и зарегистрируйте плюсик у жюри.

2.1. a) Найдите код Прюфера дерева с вершинами 1, 2, ..., 10 и рёбрами (8,9), (8,4), (4,10), (10,3), (3,5), (10,6), (10,1), (1,7), (1,2).

b) Восстановите дерево по коду Прюфера 1, 1, 2, 5, 4, 2, 7.

c) Докажите, что код Прюфера определяет взаимно однозначное соответствие между множеством деревьев с данными n вершинами и множеством слов длины $n-2$ из этих вершин.

d) Докажите, что в коде Прюфера вершина степени d встречается $d-1$ раз.

2.2. Чему равно количество корневых помеченных деревьев с n вершинами, у которых вершина n является листом (и тем самым она не корень)?

2.3. Чему равно количество свободных помеченных деревьев с $n > 10$ вершинами, у которых степень вершины 1 равна 10?

2.4. Найдите количество помеченных унициклических графов с n вершинами, имеющих цикл длины k.

2.5. Обозначим через $S(n,k)$ число Стирлинга второго рода, по определению оно равно количеству разбиений множества $[n]$ на k непустых частей. Докажите, что количество помеченных деревьев с n вершинами, ровно r из которых — листья, равно $\dfrac{n!}{r!}S(n-2,n-r)$.

2.6. Обозначим через $\tau(k_1,k_2,\ldots,k_n)$ число помеченных свободных деревьев с n вершинами, у которых степень i-й вершины равна k_i+1. Докажите, что $\tau(k_1,k_2,\ldots,k_n)=\dfrac{(n-2)!}{k_1!k_2!\ldots k_n!}$.

3 Результаты

В следующих задачах можно сдавать несколько решений, если они принципиально отличаются.

3.3. Выведите теорему Кэли из задач: a) 1.4, b) 1.6, c) 1.7, d) 2.6.

3.4. Докажите, что количество лесов, с вершинами в множестве $[n]$, состоящих из k корневых деревьев, равно $C_{n-1}^{k-1}n^{n-k}$.

3.5. Докажите, что количество лесов, с вершинами в множестве $[n]$, состоящих из двух некорневых деревьев, равно $\frac{1}{2}n^{n-4}(n-1)(n-6)$.

3.6. Докажите, что количество остовных деревьев в полном двудольном помеченном графе $K_{r,s}$ с долями $V_1=[r]$ и $V_2=\{r+1,\ldots,r+s\}$ равно $r^{s-1}s^{r-1}$.

3.7. Пусть Δ_n — число помеченных треугольных деревьев с n вершинами, Λ_n — число корневых помеченных треугольных деревьев с n вершинами и корневым ребром 1–2.

a) Докажите, что $\Lambda_n=(2n-3)^{n-3}$. b) Найдите Δ_n.

Пусть в ряд расположено n различных предметов. *Циклическая* перестановка — это перестановка, перемещающая предметы по некоторому циклу: один предмет ставится на место другого, этот другой — на место третьего, и т. д., последний ставится на место первого. *Транспозиция* (ij) — это перестановка, меняющая местами предметы на i-м и j-м месте. Если считать, что множество $[n]$ является множеством вершин некоторого графа, то транспозицию (ij) можно интерпретировать как ребро, соединяющее вершину i с вершиной j.

Результат последовательного выполнения перестановок s_1, s_2, …, s_{n-1} определяет перестановку, которая называется *произведением* этих перестановок и обозначается $s_1s_2\ldots s_{n-1}$. Произведения, отличающиеся порядком сомножителей, мы считаем различными. Например, если перестановка s — это транспозиция, меняющая местами предметы на первом и втором месте, а перестановка t — это транспозиция, меняющая местами предметы на третьем и четвертом месте, то произведения st и ts определяют одну и ту же перестановку предметов, и при этом считаются разными произведениями.

3.8. a) В ряд расположено n предметов. Докажите, что результат последовательного выполнения транспозиций s_1, s_2, …, s_{n-1} является циклической перестановкой в том и только том случае, когда граф, в котором множество вершин — это $[n]$, а множество ребер — это s_1, s_2, …, s_{n-1}, является деревом.

b) Докажите, что количество способов, которым циклическая перестановка множества $[n]$ может быть разложена в произведение $n-1$ транспозиций, равно T_n.

4 Парковочные функции

Вдоль улицы с односторонним движением расположено n мест для парковки автомобиля. На улицу въезжают последовательно n автомобилей с номерами от 1 до n в порядке возрастания. Каждый водитель едет к своему любимому месту парковки и, если оно не занято, припарковывается; в противном случае он едет дальше до первого свободного места и припарковывается там, если же все места дальше заняты, он уезжает (насовсем). Последовательность предпочтений, для которой все водители сумели припарковаться, называется *парковочной функцией*. Множество парковочных функций обозначим через $\mathcal{P}_n$.

4.3. Сколько существует парковочных функции $(a_1, a_2, \ldots, a_n)$, для которых соседние водители имеют разные предпочтения, т. е. $a_k \neq a_{k+1}$ при $k = 1, \ldots, n-1$?

4.4. Допустим, что на улицу, где расположено n мест для парковки, въезжают лишь $m < n$ машин. Сколько в этом случае существует последовательностей предпочтений, для которых все водители сумеют припарковаться?

4.5. Докажите, что число парковочных функций, для которых ровно k водителей $(1 \leqslant k \leqslant n)$ предпочитают парковаться на первом месте, равно $C_{n-1}^{k-1} n^{n-k}$.

4.6. Для каждой парковочной функции $a = (a_1, a_2, \ldots, a_n)$ определим разностную последовательность $c(a) = (c_1, c_2, \ldots, c_{n-1})$ по правилу

$$c_i = a_{i+1} - a_i \pmod{n+1}.$$

Сопоставим парковочной функции a помеченное дерево $t(a)$ с $n+1$ вершинами, которое задается кодом Прюфера $c(a)$.

Докажите, что описанное соответствие является биекцией между $\mathcal{P}_n$ и $\mathcal{T}_{n+1}$.

4.7. Докажите, что $(n+1)^{n-1} = \sum\limits_{\substack{0 \leqslant k_n \leqslant 1 \\ 0 \leqslant k_{n-1}+k_n \leqslant 2 \\ 0 \leqslant k_{n-2}+k_{n-1}+k_n \leqslant 3 \\ \ldots \\ 0 \leqslant k_2+k_3+\ldots+k_{n-1}+k_n \leqslant n-1}} \dfrac{n!}{(n-k_2-k_3-\ldots-k_n)!k_2!k_3!\ldots k_n!}$.

4.8. Будем называть парковочную функцию $a = (a_1, \ldots, a_n)$ *надежной*, если при всех j, $1 \leqslant j \leqslant n-1$, по крайней мере $j+1$ водителей предпочитают припарковаться на первых j местах. Докажите, что количество надежных парковочных функций для парковки длины n равно $(n-1)^{n-1}$.

4.9. Докажите рекуррентное соотношения с помощью комбинаторных рассуждений с парковочными функциями: $P_{n+1} = \sum\limits_{k=0}^{n} C_{n+1}^{k} P_k (n-k)^{n-k}$.

5 *Инверсии на деревьях и неудобства парковочных функций*

5.1. Докажите рекуррентные соотношения с помощью комбинаторных рассуждений:

a) $T_n = \sum_{k=0}^{n-2} C_{n-2}^k (k+1) T_{k+1} T_{n-k-1}$; b) $P_{n+1} = \sum_{k=0}^{n} C_n^k (k+1) P_k P_{n-k}$;

Возьмем помеченное дерево T с $n+1$ вершиной. Вершину $n+1$ назначим корнем и введем на ребрах дерева направление от периферии к корню. Мы «считаем правильным», когда метки вершин растут при приближении к корню. Будем говорить, что вершины i и j образуют *инверсию*, $1 \leqslant i < j \leqslant n$, если вершина i лежит на пути, ведущем от вершины j к корню. Переберем все пары вершин и обозначим через $\mathrm{inv}(T)$ суммарное количество инверсий в дереве T. Максимальное возможное значение величины $\mathrm{inv}(T)$ равно $\frac{n(n-1)}{2}$, оно достигается, когда T — это путь из n звеньев и нумерацией вершин $n+1$, 1, 2, …, n.

Пусть $a = (a_1, a_2, \ldots, a_n)$ — парковочная функция. Пусть в результате парковки первый водитель припарковался на p_1-м месте, второй — на p_2-м месте и т. д. Назовем величину

$$D(a) = \sum_{i=1}^{n} (p_i - a_i) = \frac{n(n+1)}{2} - \sum_{i=1}^{n} a_i.$$

неудобством парковочной функции a. Самое большое неудобство имеет функция $(1, 1, \ldots, 1)$, оно равно $\frac{n(n-1)}{2}$.

Теорема. Пусть n — произвольное натуральное число. Тогда при всех k, $0 \leqslant k \leqslant \frac{n(n-1)}{2}$, количество корневых помеченных деревьев на $n+1$ вершине с корнем $n+1$, имеющих k инверсий, равно количеству парковочных функций с неудобством k на улице с n парковочными местами.

Введем многочлены $F_n(x)$ и $H_n(x)$, «нумерующие» инверсии и неудобства:

$$F_0(x) = 1, \quad F_n(x) = \sum_{T \in \mathcal{T}_{n+1}} x^{\mathrm{inv}(T)}; \qquad H_0(x) = 1, \quad H_n(x) = \sum_{a \in \mathcal{P}_n} x^{D(a)},$$

Будем называть их *нумератор инверсий* и *нумератор неудобств*.

5.2. Пусть $\mathcal{T}^*$ — множество помеченных корневых деревьев на $n+3$ вершинах, у которых корень имеет степень 2 и помечен числом $n+3$, а два сына корневой вершины помечены числами $n+1$ и $n+2$. Выразите нумератор инверсий множества $\mathcal{T}^*$

$$F_n^*(x) = \sum_{T \in \mathcal{T}^*} x^{\mathrm{inv}(T)}$$

через многочлены $F_i(x)$.

5.3. Докажите, что многочлены $F_n(x)$ и $H_n(x)$ удовлетворяют при $n \geqslant 0$ одинаковым рекуррентным соотношениям

$$F_{n+1}(x) = \sum_{k=0}^{n} C_n^k (x^k + x^{k-1} + \ldots + 1) F_k(x) F_{n-k}(x). \tag{a}$$

$$H_{n+1}(x) = \sum_{k=0}^{n} C_n^k (x^k + x^{k-1} + \ldots + 1) H_k(x) H_{n-k}(x). \tag{b}$$

Теорема об инверсиях и неудобствах сразу следует из предыдущих двух задач. Но, возможно, вы сможете предложить биективное доказательство.

5.4. Докажите теорему об инверсиях и неудобствах, построив взаимно однозначное соответствие между множествами $\mathcal{T}_{n+1}$ и $\mathcal{P}_n$, при котором дереву с j инверсиями ставится в соответствие парковочная функция с неудобством j.

6 После промежуточного финиша

Помеченным плоским деревом будем называть корневое помеченное дерево, у которого сыновья любой вершины линейно упорядочены. Обозначим через $\mathcal{P}_n^k$ множество лесов, состоящих из k помеченных плоских деревьев на множестве $[n]$ с корнями 1, 2, ..., k, у которых вершина n находится в дереве с корнем 1.

1.9. Докажите, что при $2 \leqslant k \leqslant n-1$ выполняется рекуррентное соотношение

$$P_n^{k-1} = (2n-k)P_n^k.$$

3.9. Пусть n и k — натуральные числа, $2 \leqslant k \leqslant n$. Найдите количество помеченных деревьев на $[n]$, у которых первая и вторая вершины соединены путем длины $k-1$.

3.10. Докажите, что количество остовных лесов в полном двудольном помеченном графе $K_{r,s}$, состоящих из $k+\ell$ корневых деревьев с корнями 1, 2, ..., k и $r+1$, $r+2$, ..., $r+\ell$, равно $(r\ell+sk-k\ell)r^{s-\ell-1}s^{r-k-1}$.

3.11. Докажите, что количество остовных деревьев в полном трехдольном помеченном графе $K_{r,s,t}$ с долями $V_1 = [r]$, $V_2 = \{r+1, \ldots, r+s\}$ и $V_3 = \{r+s+1, \ldots, r+s+t\}$ равно $(r+s+t)(r+s)^{t-1}(s+t)^{r-1}(t+r)^{s-1}$.

3.12. Чему равно количество плоских помеченных корневых деревьев на $n+1$ вершине?

Тетраэдральное дерево определяется по индукции аналогично треугольному. Простейшее тетраэдральное дерево (вырожденное) — это треугольник (полный граф на трех вершинах), следующее по сложности — тетраэдр (полный граф на четырех вершинах). Если уже задано тетраэдральное дерево, мы можем добавить к нему новую вершину, взяв любую треугольную грань любого из тетраэдров и построив на этой грани как на основании тетраэдр с новой вершиной (рис. 4). Формально это значит, что мы добавили к графу одну новую вершину и три новых ребра (и, если хотите, три новые треугольные грани). Заметим, что в трехмерном пространстве тетраэдры могут пересекаться, подобно тому как в треугольных деревьях, изображаемых на плоскости, могли пересекаться треугольники.

3.13. Сколько существует помеченных тетраэдральных деревьев с n вершинами?

4.10. Докажите, что $(n-1)^{n-1} = \sum\limits_{\substack{0\leqslant k_{n-1}\leqslant 1\\ 0\leqslant k_{n-2}+k_{n-1}\leqslant 2\\ 0\leqslant k_{n-3}+k_{n-2}+k_{n-1}\leqslant 3\\ \ldots\\ 0\leqslant k_2+k_3+\ldots+k_{n-2}+k_{n-1}\leqslant n-2}} \dfrac{n!}{(n-k_2-k_3-\ldots-k_{n-1})!k_2!k_3!\ldots k_{n-1}!}.$

4.11. Докажите, что $n^n = \sum\limits_{\substack{0\leqslant k_1\leqslant 1\\ 0\leqslant k_1+k_2\leqslant 2\\ 0\leqslant k_1+k_2+k_3\leqslant 3\\ \ldots\\ 0\leqslant k_1+k_2+\ldots+k_{n-1}\leqslant n-1}} \dfrac{n!}{k_1!k_2!\ldots k_{n-1}!}.$

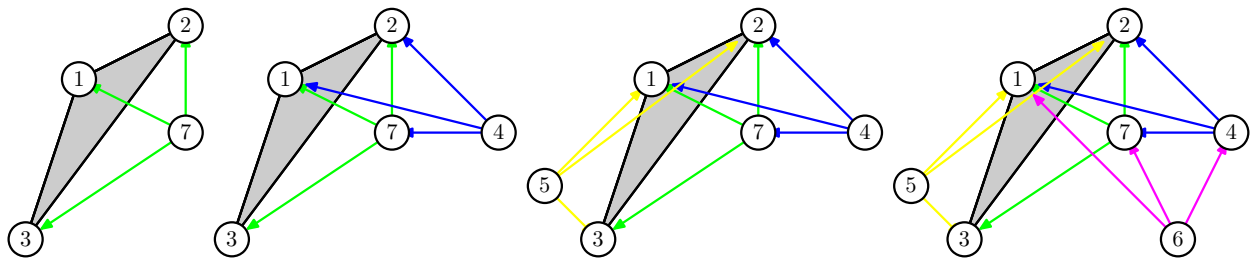


Рис. 4. Построение тетраэдрального дерева. К основному треугольнику (1, 2, 3) последовательно добавляются вершины 7, 4, 5, 6

Решения

1 Рекурсии, тождества, биекции

1.1. Мы взяли эту задачу в [3]. Отметим на цикле вершину A с наибольшей меткой и ту из двух соседних с ней по циклу вершин B, где метка крупнее. Уберем из дерева ребро AB, подвесим к A лист с меткой 99, и к B — лист с меткой 100. Мы построили инъективное отображение из множества унициклических графов в множество деревьев.

1.2. Решение 1. См. [6, задача 8.5] или [1] (глава 26, первое доказательство). Рассмотрим путь, ведущий из синей вершины в красную. Он задается некоторой последовательностью элементов множества $A \subset [n]$. На вершинах этого пути растут деревья. Саму последовательность можно представлять как перестановку элементов множества A. Зададим эту перестановку с помощью циклов (на элементах множества A). Мы получили набор циклов, причем на каждой вершине каждого цикла растет дерево.

С другой стороны, отображение множества $[n]$ в себя задается ориентированным графом: из вершины i рисуем стрелку в вершину $f(i)$ (разрешены петли). У этого графа все вершины имеют исходящую степень 1, поэтому он представляет собой объединение циклов, причем на каждой вершине цикла растет дерево (точнее, наоборот: дерево «вливается» в каждую вершину цикла).

Это и есть требуемая биекция.

Решение 2. Отображение из $[n]$ в $[n]$ задается последовательностью из n чисел. Возьмем дерево из условия задачи и выпишем его код Прюфера ($n-2$ числа), после чего выпишем номер красной, а затем номер синей вершины. Получилась последовательность из n чисел. Очевидно, что это биекция.

1.3. Мы взяли это утверждение в [17, п. 3.9]. Правая часть равенства подсчитывает всевозможные отображения из $[n-1]$ в $[n]$. Любое такое отображение может быть изображено в виде ориентированного графа на n вершинах: из каждой вершины выходит одно ребро, показывающее, куда отображается эта вершина. У вершины n могут быть только входящие ребра, и компонента связности вершины n — это дерево, в котором все стрелки «показывают в сторону n». Левая часть равенства перечисляет такие графы, классифицируя их по виду дерева, содержащего вершину n.

1.4. [14, Теорема 2.1]. На корневом дереве задано направление от корня к периферии. Построим отображение из множества $\mathcal{F}_n^{k-1}$ в $\mathcal{F}_n^k$. Для этого возьмем лес с $k-1$ деревом, найдем в нем вершину k, отломаем ее и все, что на ней растет, и посадим в качестве отдельного корневого дерева. Как правило получится дерево из $\mathcal{F}_n^k$ за исключением одного случая: если мы отломали ветку от первого дерева и вершина n находится на отломанной ветке. В этом случае сделаем коррекцию: поменяем метки 1 и k местами.

Посмотрим, сколько прообразов имеет при таком отображении произвольный лес из $\mathcal{F}_n^k$. Чтобы построить прообраз леса, нужно взять в нем k-е дерево и прицепить в качестве ветки к любой вершине первого, второго, ..., $(k-1)$-го дерева — это если мы подразумеваем, что не было коррекции. А для прообразов с коррекцией нужно первое дерево в качестве ветки прицепить к любой вершине k-го дерева и поменять метки 1 и k. Итого, каждая из n вершин имеющегося графа может быть использована для построения (уникального) прообраза. Таким образом, $F_n^{k-1} = nF_n^k$.

1.5. Ответ: $F_{r,s}^{k-1} = sF_{r,s}^k$ при $2 \leqslant k \leqslant r$. [14, Следствие 3.1]. Рекурсия строится так же, как в задаче 1.4. Поскольку вершина с номером k лежит в множестве V_1, при построении обратного отображения поддерево с корнем k может быть подвешено к s вершинам.

1.6. а) Это результат из [18]. Обозначим через E_n количество помеченных деревьев с вершинами на $[n]$, содержащих определенное ребро, например, ребро 1–2. Подсчитывая все ребра

во всех деревьях, приходим к тождеству

$$\frac{n(n-1)}{2}E_n = (n-1)T_n.$$

Таким образом, $T_n = \frac{1}{2}nE_n$. Теперь, чтобы найти E_n, достаточно выбрать, сколько вершин содержит дерево, висящее на вершине 1, а сколько на вершине 2, и какие именно это деревья. Получаем формулу $T_n = \frac{n}{2}\sum\limits_{k=0}^{n-2} C_{n-2}^k T_{k+1}T_{n-k-1}$.

b) Тождество из этой задачи выводится из тождества задачи 5.1 a) с помощью «хрестоматийного метода Гаусса»: нужно сложить два экземпляра суммы из задачи 5.1 a), поменять в одном из них индекс суммирования k на $n-2-k$ и сложить эти суммы почленно.

Выведем тождество задачи 1.3 из тождества 5.1 a), для этого запишем отдельно слагаемое для $j = n$, а в оставшейся сумме введем индекс суммирования k, где $j = k+1$:

$$n^{n-2} + \sum_{k=0}^{n-2} C_{n-1}^k (k+1)^{k+1}(n-k-1)^{n-k-1} = n^{n-1}.$$

Перенесем слагаемое n^{n-2} в правую часть, а в левой части преобразуем биномиальный коэффициент по формуле $C_{n-1}^k(n-k-1) = (n-1)C_{n-2}^k$:

$$\sum_{k=0}^{n-2}(n-1)C_{n-2}^k(n-k-1)(k+1)^{k+1}(n-k-1)^{n-k-3} = n^{n-2}(n-1).$$

Сократив на $(n-1)$, получаем формулу из задачи 5.1 a) с точностью до замены индекса суммирования.

1.7. [4] Пусть $A \in \mathcal{T}(n, k-1)$ — одно из деревьев, v — любая из его $n-k$ вершин, несмежных с вершиной 1. Заменим ребро, ведущее из вершины v к предку, на ребро, ведущее в корень. Полученное дерево обозначим B (очевидно $B \in \mathcal{T}(n,k)$), а пару деревьев (A, B) назовем *связкой*.

Подсчитаем двумя способами количество связок. С одной стороны, число связок равно $(n-k)T(n,k-1)$, поскольку связка однозначно определяется деревом A и вершиной v, дерево можно выбрать $T(n,k-1)$ способами, после чего вершина v выбирается $(n-k)$ способами. С другой стороны, связку можно получить, если мы выберем $T(n,k)$ способами дерево B, после чего удалим одно из ребер, выходящих из корня, и образовавшуюся «отломанную ветку» соединим с любой некорневой вершиной оставшегося дерева — всего получится

$$(n-1-n_1) + (n-1-n_2) + \ldots + (n-1-n_k) = (n-1)(k-1)$$

вариантов, здесь через n_i обозначено число вершин в «отломанной ветке», образовавшейся при удалении i-го ребра, выходящего из корня. Итого $(n-1)(k-1)T(n,k)$ вариантов. Значит, $(n-1)(k-1)T(n,k) = (n-k)T(n,k-1)$.

1.8. Ответ: $(n-k-2)\Delta(n,k) = k(2n-4)\Delta(n,k+1)$. Это утверждение из [9].

Отметим, что построение треугольного дерева, описанное в определении, можно начинать с любого ребра: возьмем любое ребро, добавим к нему треугольники, которые его содержат, потом добавим треугольники, примыкающие к уже построенным ребрам и т. д. Более того, пусть начальное ребро фиксировано, а при добавлении к дереву очередной вершины C, мы рисуем на ребрах CA, CB стрелки, выходящие из вершины C. Тогда ориентированный граф, изображающий треугольное дерево, не зависит от порядка, в котором добавлялись вершины!

Рассмотрим треугольное дерево G, у которого корневое ребро uv принадлежит k треугольникам, обозначим их uvw_1, uvw_2, …, uvw_k, и построим по нему дерево с $k+1$ треугольниками (рис. 5). Возьмем произвольную вершину w, не совпадающую ни с одной из вершин w_i, и рассмотрим минимальное треугольное поддерево, содержащее вершины u, v

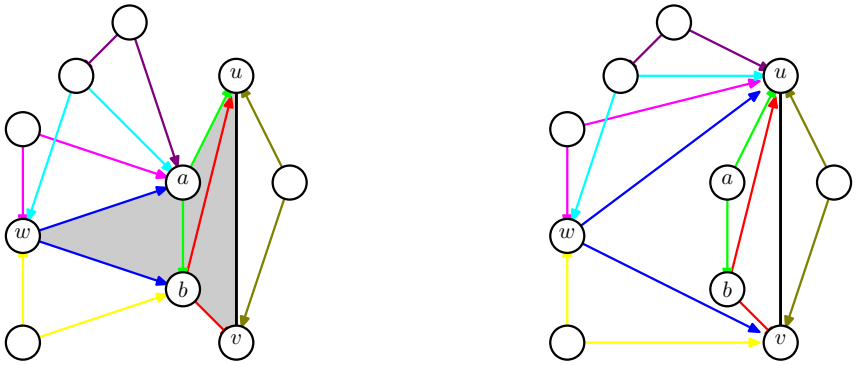


Рис. 5. Слева дерево с k треугольниками на корневом ребре uv, справа с $k+1$ треугольниками ($k=1$). Минимальное дерево, содержащее вершины w, u и v, закрашено серым цветом. От каждой вершины, кроме вершин u и v, ведут две стрелки к ребру, на которое был повешен треугольник, соответствующий этой вершине

и w. В силу минимальности из вершины w в этом поддереве выходят два ребра. Уберем эти ребра и вместо них проведем ребра wu и wv. В результате у корневого ребра появится еще один треугольник. Части дерева G, которые висели на убранных ребрах, перевесим на новые ребра wu и wv. (При выполнении этих действий могло случиться, что мы убрали ребро, соединяющее w с u или v, и тут же добавили его снова.) Выбрать вершину w можно $n-k-2$ способами, поэтому мы имеем $(n-k-2)\Delta(n,k)$ вариантов выполнения этой конструкции.

Теперь опишем обратную операцию: по дереву, у которого корневое ребро uv принадлежит $k+1$ треугольникам, построим дерево, у которого корневое ребро uv принадлежит k треугольникам. Для этого возьмем одну из $k+1$ вершин треугольников, связанных с корнем, пусть это будет вершина w, и «пересадим» треугольник uvw с ребра uv на какое-нибудь другое ребро ab. Это делается следующим образом: пусть G_1 и G_2 — треугольные поддеревья, растущие на ребрах wu и wv. Выберем произвольное ребро ab, не лежащее в $G_1 \cup G_2$ (и не совпадающее с uv), и заменим ребра wu и wv на ребра wa и wb. При этом поддеревья G_1 и G_2, висевшие на ребрах wu и wv, перевесим на ребра wa и wb соответственно.

Подсчитаем, сколькими способами может быть выполнена такая конструкция. В качестве ab может выбираться любое из $2n-4$ некорневых ребер, причем, если ребро ab принадлежит треугольному поддереву, висящему на корневом треугольнике uvw', то в качестве треугольника uvw, который мы перевешиваем на это ребро, можно взять любой из k корневых треугольников uvw, где $w \neq w'$. Итого $k(2n-4)\Delta(n,k+1)$ способов.

1.9. [14, Следствие 4.1]. Попробуем построить такую же рекурсию, как в задаче 1.4. На этот раз мест, куда можно подвесить поддерево с корнем k, больше. Для каждой вершины оно равно числу ее потомков плюс один. Суммарно по всем вершинам получается число всех ребер плюс число всех вершин. А число ребер в лесу из k деревьев равно $n-k$.

1.10. Ответ: $P^{r-1}_{n,p} = (p+1)P^r_{n+1,p+1}$. [14, Теорема 4.3]. Рекурсия почти как в задаче 1.4. В качестве r-го дерева берем поддерево с корнем в вершине r. На то место, где была вершина r, подвесим лист. Заметим, что если бы мы этого не сделали, то пронумерованный предок вершины r мог оказаться листом, если у него не было больше потомков. Число листьев и общее число вершин n увеличились на 1. Если теперь вершина $n-p$ оказалась в дереве с корнем r, переставим метки 1 и r. Обратно, убираем любой из $p+1$ листьев и вместо него подвешиваем дерево с корнем r если лист находится в другом дереве или подвешиваем дерево с корнем 1 и переставляем метки 1 и r, если лист находится в r-м дереве.

2 Код Прюфера

2.1. Эта задача 2.2.4 из книжки [3] — упражнение на понимание того, что представляет собой код Прюфера.

2.2. Ответ: $(n-1)^{n-1}$.

Код Прюфера некорневого дерева, у которого вершина n является листом, не содержит символа «n». Потому имеется $(n-1)^{n-2}$ таких кодов. Выбор корня увеличивает число вариантов в $(n-1)$ раз.

2.3. Ответ: $C_{n-2}^{9}(n-1)^{n-11}$. Потому что это число равно количеству заполнений n ячеек $n-2$ различными предметами, для которых первая ячейка содержит 9 предметов.

2.4. Ответ: $\frac{1}{2}(n-1)(n-2)\dots(n-k+1)n^{n-k}$.

Действительно, количество способов выбрать цикл равно $\frac{n(n-1)(n-2)\dots(n-k+1)}{2k}$ — выбираем последовательно первую, вторую и т. д. вершины цикла, после чего учтем, что нам не важно, которая вершина в цикле числится первой и каково направление цикла. Осталось подсчитать количество унициклических графов, содержащих цикл $(n, n-1, \dots, n-k+1)$. Уберем ребро, соединяющее n и $n-k+1$. Количество возможных кодов Прюфера для получившегося дерева равно kn^{n-1-k}.

Действительно, после $n-k$ шагов выписывания кода Прюфера нашего дерева от него останется как раз путь n, $n-1$, …, $n-k+1$. Первые $n-k-1$ элементов кода Прюфера произвольны, $(n-k)$-й элемент — это число от $n-k+1$ до n, а все остальные элементы детерминированы.

Мы взяли эту задачу в [3].

2.5. Мы взяли это утверждение в [5]. Если присмотреться, оно есть и в [7]. В свете кода Прюфера, кажется, это почти тавтология.

2.6. [7]. По алгоритму Прюфера каждому такому дереву взаимно однозначно соответствует код Прюфера — одночлен $x_{i_1}x_{i_2}\dots x_{i_{n-2}}$, который после «упрощения» приводится к виду $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ (где $k_1+k_2+\dots+k_n=n-2$). Таким образом количество разных кодов равно полиномиальному коэффициенту $\frac{(n-2)!}{k_1!k_2!\dots k_n!}$.

3 Результаты

3.1. Мы взяли это утверждение в [17]. Для каждого дерева с помеченными вершинами назначим вершину n корнем, тем самым мы зададим направление от корня и, как следствие, отношение «предок–потомок». Теперь каждому помеченному дереву с n вершинами поставим в соответствие реберно помеченное дерево с n вершинами. Для этого поставим на каждом ребре ij, где i потомок j, метку i.

Полученное реберно помеченное дерево позволяет восстановить исходную разметку вершин, если мы укажем, которая из вершин была корнем и присвоим ей метку n. Таким образом, каждое реберно помеченное дерево могло получиться при этом отображении из n различных вершинно помеченных деревьев.

3.2. Мы взяли эту задачу в [3]. Будем считать число корневых деревьев. Нарисуем дерево на плоскости, у каждого ребра зададим направление от корня. Теперь сопоставим дереву код: начиная от корня, будем обходить дерево, как будто это система стен на плоскости. Когда движемся по стрелке — пишем 1, а против — 0. Получим последовательность из $2n-2$ нулей и единиц. Нетрудно понять, что каждой последовательности соответствует не более одного дерева.

3.3. a) Теорема Кэли сразу следует из задачи 1.4 и равенства $F_n^{n-1} = 1$.

c) А также из задачи 1.7 и равенства $T(n,k) = C_{n-2}^{k-1}(n-1)^{n-k-1}$. Действительно, количество помеченных деревьев равно сумме

$$\sum_{k=1}^{n-1} T(n,k) = \sum_{k=1}^{n-1} C_{n-2}^{k-1}(n-1)^{n-k-1} = \sum_{k=0}^{n-2} C_{n-2}^{k}(n-1)^{n-2-k} = ((n-1)+1)^{n-2}.$$

b) Что касается задачи 1.6, теорема Кэли выводится из нее в [18] с помощью производящих функций и формулы обращения Лагранжа. Но, возможно, есть и элементарный метод.

d) Из задачи 2.6 теорема Кэли выводится с помощью суммирования в духе полиномиальной теоремы [7]:

$$\sum_{\substack{k_1+k_2+\ldots+k_n=n-2 \\ k_i \geqslant 0}} \frac{(n-2)!}{k_1!k_2!\ldots k_n!} = n^{n-2}.$$

3.4. [14, Следствие 2.3]. Существует всего один лес с $n-1$ деревьями. Применяя рекурсивное равенство $F_n^{k-1} = nF_n^k$ из задачи 1.4 несколько раз, получим, что $F_n^k = n^{n-k-1}$. Число лесов, в которых вершина с номером n содержится не в первом, а в любом другом фиксированном дереве, равно F_n^k. Следовательно, число лесов без условия на вершину n равно kn^{n-k-1}. Число способов выбрать корни для k деревьев равно C_n^k, отсюда искомое количество лесов равно $C_n^k kn^{n-k-1} = C_{n-1}^{k-1}n^{n-k}$.

3.5. Мы взяли это утверждение в [17, п. 4.3].

3.6. Решение 1. [14, Следствие 3.1]. Будем подсчитывать не только число деревьев, но и число лесов (у которых вершина $r+1$ находится в дереве с корнем 1). Воспользуемся рекурсивной формулой из задачи 1.5:

$$F_{r,s}^{k-1} = sF_{r,s}^k \quad \text{при} \quad 2 \leqslant k \leqslant r.$$

Пользуясь этой формулой, сведем впорос к подсчету числа лесов с r деревьями. Это число лесов равно $F_{r,s}^r = r^{s-1}$, так как число способов выбрать среди r корней предков для $s-1$ вершин равно r^{s-1}.

Решение 2 (код Прюфера). Код Прюфера такого такого дерева содержит $r-1$ предков одной доли и $s-1$ предков другой доли, так как в конце всегда остаются две вершины разных

долей. Каждый из $r-1$ предков может быть выбран s способами и аналогично, каждый из $s-1$ предков может быть выбран r способами.

3.7. а) Р е ш е н и е 1. Утверждение задачи взято в [9], где оно доказано пятью способами. Мы приводим третье доказательство из [9].

Воспользуемся рекурсией из решения 1.8 и тем, что $\Delta(n,k)=1$ при $k=n-2$. Получаем

$$\Delta(n,k)=(2n-4)\frac{k}{n-2-k}\Delta(n,k+1)=(2n-4)^2\frac{k(k+1)}{(n-2-k)(n-2-(k+1))}\Delta(n,k+2)=$$
$$=\ldots=(2n-4)^{n-2-k}\frac{k(k+1)\ldots(n-3)}{(n-2-k)(n-2-(k+1))\cdots 1}\Delta(n,n-2)=$$
$$=(2n-4)^{n-2-k}\frac{(n-3)!}{(k-1)!(n-3-(k-1))!}\Delta(n,n-2)=(2n-4)^{n-2-k}C_{n-3}^{k-1}.$$

Суммируя по всем возможным k и применяя формулу бинома Ньютона, вычисляем количество корневых треугольных деревьев: $\sum\limits_{k=1}^{n-2}C_{n-3}^{k-1}(2n-4)^{n-k-2}=(2n-3)^{n-3}$.

Р е ш е н и е 2 (код Прюфера). Закодируем помеченное корневое треугольное дерево кодом, аналогичным коду Прюфера.

Построение кода по дереву. Пусть дано треугольное помеченное корневое дерево с корневым ребром 1–2. Сначала по заданной разметке вершин дерева определим специальную разметку ребер. Для этого поставим на ребрах стрелки, как это описано в начале решения задачи 3.7. Тогда из каждой вершины, не принадлежащей корневому ребру, выходит две стрелки. Если вершина имеет метку x, то пометим выходящие из нее ребра xa и xb, где xa ведет в вершину с меньшей меткой, а xb — с большей. Корневое ребро будем обозначать 1–2. Таким образом, наше дерево содержит $2n-3$ ребра с «унифицированными» названиями:

$$12,\ 3a,\ 3b,\ 4a,\ 4b,\ \ldots,\ na,\ nb.$$

Запишем код, пользуясь новыми названиями ребер. Листьями треугольного дерева будем называть вершины степени 2. На каждом шаге смотрим на все вершины, являющиеся листьями текущего треугольного дерева, выбираем из них вершину с *наибольшим* номером, отрываем ее от дерева и записываем название ее ребра-предка. На последнем шаге отрываем вершину с оставшимся номером от корневого ребра 1–2, его можно не записывать.

Восстановление дерева по коду. Листьями дерева являются вершины с номером x, если оба ребра xa и xb не содержатся в коде, также листьями не могут быть вершины 1 и 2. Выпишем такие номера вершин. В этом списке вершина с наибольшим номером была оторвана первой, значит, первое ребро в коде — это ее ребро-предок. Записываем, какое ребро является предком для этой вершины, уберем ее из списка листьев, а ребро из кода. После удаления ребра из кода, могут появиться новые вершины, которые теперь следует считать листьями, добавим их в список листьев. Снова найдем в этом списке вершину с наибольшим номером и т. д.

В результате выполнения этого алгоритма, мы получим последовательность вершин с их ребрами-предками. В отличие от обычного дерева треугольное трудно восстановить, просматривая эту последовательность с начала, так как неизвестен один из номеров вершин ребра xa или xb. Зато, начиная с хвоста, это делается легко. Рисуем корневое ребро 1–2. Первой к нему была присоединена вершина, которой нет в последовательности. На следующем шаге присоединяется вершина y к ребру xa или xb, а эти ребра уже нарисованы, следовательно, известны обе их вершины.

Почему в списке всегда имеется хотя бы один лист? В текущем коде $n-3-k$ позиции, где k — число уже рассмотренных позиций. А число вершин, могущих оказаться листьями, равно $n-2-k$ (слагаемое 2 присутствует, так как вершины 1 и 2 не листья), то есть всегда на единицу больше. Даже если на всех позициях кода стоят ребра, соответствующие различным вершинам, в списке листьев есть один элемент.

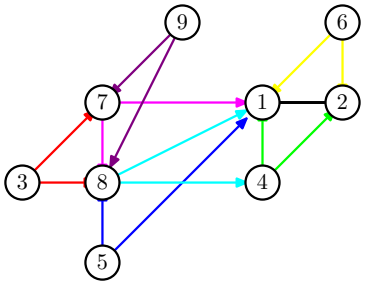


Рис. 6. Пример построения кода треугольного дерева (7b)(12)(8a)(7b)(8a)(4a).

Код содержит $n-3$ позиции. Всего ребер $2n-3$. На каждой позиции может быть любое ребро. Значит, число таких кодов равно $(2n-3)^{n-3}$. Поскольку каждому коду соответствует ровно одно дерево, а по каждому дереву строится код, корневых треугольных деревьев столько же.

Пример. Пусть имеется 8 вершин и код Прюфера (7b, 1–2, 8a, 7b, 8a, 4a).

Номер шага	Текущий код	Список листьев	Подвешенная вершина
1	(7b, 1–2, 8a, 7b, 8a, 4a)	3, 5, 6, 9	9
2	(1–2, 8a, 7b, 8a, 4a)	3, 5, 6	6
3	(8a, 7b, 8a, 4a)	3, 5	5
4	(7b, 8a, 4a)	3	3
5	(8a, 4a)	7	7
6	(4a)	8	8

Не перечислена вершина 4, значит, она была подвешена к ребру 1–2 первой. Нарисуем треугольник на вершинах 1, 2, 4. Далее были подвешены вершины 8, 7, 3, 5, 6, 9 к ребрам 4a, 8a, 7b, 8a, 1–2, 7b соответственно. Подвешиваем вершину 8 к ребру 4a (т. е. к ребру 2–4) и т. д. Получившееся треугольное дерево показано на рис. 6.

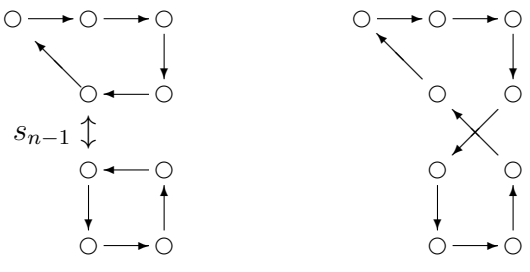
b) Так как выделенное ребро треугольного дерева может быть помечено любой парой меток, а не только 1–2, а любое из $2n-3$ ребер в треугольном дереве можно назначить корнем, выполняется соотношение

$$C_n^2 \Lambda_n = (2n-3)\Delta_n.$$

3.8. Этот результат J. Dénes мы приводим по книге [11] (лемма 3.15 и теорема 3.16).

a) Если граф, изображающий транспозиции, несвязен, то перестановка не сможет перенести предмет, отнесенный к одной из компонент, на место предмета из другой компоненты. Таким образом, граф связен и в нем $n-1$ ребро. Следовательно, это дерево.

Проверим теперь, что произведение транспозиций, построенное по произвольному помеченному дереву, является циклической перестановкой множества его вершин. Это утверждение легко доказывается индукцией по числу сомножителей. База $n=1$ тривиальна. Докажем переход. Зафиксируем произведение $s_1 s_2 \dots s_{n-1}$. При удалении ребра, соответствующего множителю s_{n-1}, дерево распадется на две компоненты. Оставшееся произведение $s_1 s_2 \dots s_{n-2}$ переставляет по циклу элементы в каждой из компонент. Добавление множителя s_{n-1} объединяет эти два цикла в один (см. рис).



b) Зафиксируем стандартное обозначение — будем задавать перестановку двустрочной диаграммой. Запись $\left(\begin{smallmatrix}1 & 2 & \dots & n\\ a_1 & a_2 & \dots & a_n\end{smallmatrix}\right)$ обозначает перестановку, которая переставляет первый предмет на место a_1, второй предмет — на место a_2 и т. д. Тогда, например, $C = \left(\begin{smallmatrix}1 & 2 & \dots & n-1 & n\\ 2 & 3 & \dots & n & 1\end{smallmatrix}\right)$ это одна из циклических перестановок. При необходимости столбцы диаграммы, задающей перестановку, можно переставлять. Тогда понятно, что обратная перестановка задается диаграммой, которая получатся из диаграммы исходной перестановки перестановкой строк.

Построим биекцию между множеством помеченных деревьев на n вершинах и и множеством разложений перестановки C в произведение $n-1$ транспозиций.

Возьмем произвольное помеченное дерево T. Сначала построим по этому дереву вспомогательное произведение транспозиций. Для этого назначим вершину 1 корнем и зафиксируем на ребрах направление к корню. Для каждой вершины i обозначим выходящее из нее ребро через s_i и тем же символом будем обозначать транспозицию чисел на концах ребра. Рассмотрим циклическую перестановку $S = s_2 \dots s_n$ (она циклическая по пункту a)) Запишем S в качестве диаграммы: $S = \left(\begin{smallmatrix}1 & a_2 & \dots & a_n\\ a_2 & a_3 & \dots & 1\end{smallmatrix}\right)$ и рассмотрим перестановку $F = \left(\begin{smallmatrix}1 & 2 & \dots & n\\ 1 & a_2 & \dots & a_n\end{smallmatrix}\right)$. Заметим, что

$$FSF^{-1} = C,$$

поскольку для всех k предмет, стоящий на k-м месте, перемещается под действием перестановки F на a_k-е место, потом S переставляет его на a_{k+1} место, и наконец, перестановка F^{-1} отправляет этот предмет на $(k+1)$-е место.

Рассмотрим набор транспозиций $u_i = Fs_iF^{-1}$ (в том, что перестановки u_i являются транспозициями, читатель может легко убедиться сам). Тогда

$$u_2 \dots u_n = Fs_2F^{-1}Fs_3F^{-1} \dots Fs_nF^{-1} = Fs_2s_3 \dots s_nF^{-1} = FSF^{-1} = C.$$

Таким образом, мы сопоставили произвольному дереву набор транспозиций u_i, произведение которых равно перестановке C:

Чтобы доказать, что данное сопоставление — биекция, покажем, как можно восстанавить дерево по произведению транспозиций u_i.

Пусть дано произведение $u_2 \dots u_n$, причем пусть этот набор транспозиций соответствует некоторому дереву $\widetilde{T}$, будем считать вершину 1 его корнем. Предположим на секундочку, что нам известна перестановка F. Тогда мы знаем, что $F^{-1}u_iF = s_i$ (и кстати, $F(1) = 1$, т. е. перестановка сохраняет метку корня). Таким образом, если транспозиция s_i меняет местами i и j, то транспозиция u_i меняет местами $F^{-1}(i)$ и $F^{-1}(j)$. Это значит, что если к меткам вершин дерева T применить перестановку F^{-1}, получится в точности дерево $\widetilde{T}$!

Поскольку дерево $\widetilde{T}$ нам известно, осталось восстановить перестановку F. По построению корень дерева $\widetilde{T}$ в 1. Зафиксировав направление к корню, мы для каждого i с легкостью найдем в дереве $\widetilde{T}$ ребро u_i, при этом соответствующее ребро в дереве T выходит из вершины i, следовательно, $F^{-1}(i)$ равно номеру вершины, из которой выходит ребро u_i.

3.9. Ответ: $kn^{n-k-1}(n-2)(n-3)\dots(n-k)$.

Аналогично 2.4. Существует $(n-2)(n-3)\dots(n-k)$ способов построить путь из первой вершины во вторую. Количество кодов Прюфера для дерева, содержащего такой путь, равно kn^{n-k-1}. Мы взяли это утверждение в [5, задача 5.93].

3.10. В [17, п. 3.5] это утверждение советуют доказывать с помощью рекурсии, мы воспользуемся рекурсией из задачи 1.5.

Как и в задаче 3.6, используя рекурсию из 1.5, находим, что

$$F^q_{a,b} = bF^{q+1}_{a,b} = \dots = b^{a-q}F^a_{a,b} = b^{a-q}a^{b-1},$$

где $F^q_{a,b}$ — число двудольных лесов с долями по a и b вершин, состоящих из q (где $q \leqslant a$) корневых деревьев с корнями 1, 2, …, q из первой доли, у которых вершина $a+1$ находится в дереве с корнем 1. Если мы умножим это значение на число корней q, то получим число лесов без условия на то, где находится вершина $a+1$.

Кроме этих соображений нам понадобятся биномиальные тождества

$$\sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} x^{\gamma} y^{r-k-\gamma} = (x+y)^{r-k} \quad \text{и} \quad \sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} \gamma x^{\gamma} y^{r-k-\gamma} = (r-k)x(x+y)^{r-k-1},$$

Приступим к решению задачи. Выберем в первой доле γ вершин, которые будут подвешены в качестве сыновей к ℓ корням второй доли. Подвесить γ вершин к ℓ корням можно γ^{ℓ} способами. После этого удалим ℓ корней второй доли, а выбранные вершины назначим корнями. У нас получится двудольный лес с долями по r и $s-\ell$ вершин, который состоит из $k+\gamma$ корневых деревьев с корнями, принадлежащими первой доле. Количество таких лесов равно $(k+\gamma)F_{r,s-\ell}^{k+\gamma}$. Следовательно, искомое значение равно

$$\sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} \ell^{\gamma}(\gamma+k)F_{r,s-\ell}^{k+\gamma} = \sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} \ell^{\gamma}(k+\gamma)(s-\ell)^{r-k-\gamma} r^{s-\ell-1} =$$

$$= kr^{s-\ell-1} \sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} \ell^{\gamma}(s-\ell)^{r-k-\gamma} + r^{s-\ell-1} \sum_{\gamma=0}^{r-k} C_{r-k}^{\gamma} \gamma \ell^{\gamma}(s-\ell)^{r-k-\gamma} =$$

$$= r^{s-\ell-1}(ks^{r-k} + (r-k)\ell s^{r-k-1}) = r^{s-\ell-1}s^{r-k-1}(ks + r\ell - k\ell).$$

3.11. [14, Следствие 3.3]. Пусть $V_1 = [r]$, $V_2 = \{r+1, \ldots, r+s\}$, $V_3 = \{r+s+1, \ldots, r+s+t\}$ и $V = V_1 \cup V_2 \cup V_3$. Обозначим через $F_{r,s,t}^{k}$ количество корневых трехдольных лесов на множестве вершин V, состоящих из k деревьев с корнями $1, 2, \ldots, k$, в которых вершина с номером $r+1$ является потомком вершины 1, и через $\bar{F}_{r,s,t}^{k}$ количество корневых трехдольных лесов на множестве вершин V с корнями $2, 3, \ldots, k+1$, в которых вершина с номером 1 является потомком вершины $r+1$. Нас интересует количество деревьев, т. е. $F_{r,s,t}^{1}$.

$$F_{r,s,t}^{1} \underset{(2)}{=} (s+t)^{r-1} F_{r,s,t}^{r} \underset{(3)}{=} (s+t)^{r-1} \bar{F}_{r,s,t}^{r} \underset{(4)}{=}$$

$$\underset{(4)}{=} (s+t)^{r-1}(r+t)^{s-1} \bar{F}_{r,s,t}^{r+s-1} \underset{(5)}{=} (s+t)^{r-1}(r+s+t)(r+s)^{t-1}.$$

(2) аналогично задаче 1.5 при $2 \leqslant k \leqslant r$ получаем рекурсивную формулу

$$F_{r,s,t}^{k-1} = (s+t)F_{r,s,t}^{k}$$

и, пользуясь этой формулой несколько раз, переходим к лесу с r деревьями;

(3) используем равенство $F_{r,s,t}^{r} = \bar{F}_{r,s,t}^{r}$ (леса в этих множествах отличаются только выбором корня для дерева, содержащего вершину 1);

(4) при $r+1 \leqslant k \leqslant r+s-1$ получаем рекурсивную формулу

$$\bar{F}_{r,s,t}^{k-1} = (r+t)\bar{F}_{r,s,t}^{k}$$

снова аналогично задаче 1.5 и переходим к лесу с $r+s-1$ деревьями; Переход от лесов с корнями $1, 2, \ldots, r$ к лесам с корнями $2, 3, \ldots, r+1$ обусловлен тем, что в этом рекурсивном равенстве вершина с номером k должна лежать во второй доле.

(5) число лесов с большим количеством деревьев легко считается:

$$\bar{F}_{r,s,t}^{r+s-1} = (r+s)^{t} + t(r+s)^{t-1},$$

в первом слагаемом вершина с номером 1 является сыном вершины с номером $r+1$, а оставшиеся t вершин третьей доле можно соединить с любыми $r+s$ вершин других долей, во втором слагаемом вершина с номером 1 является сыном некоторой вершины из третьей доли, а оставшиеся $t-1$ вершин аналогично распределяются по $r+s$ местам.

3.12. Ответ: $(2n)!/n!$. Тем самым количество плоских помеченных некорневых деревьев на $n+1$ вершине равно числу Каталана $\frac{1}{n+1}C_{2n}^{n}$. [14, Следствие 4.2].

3.13. Ответ: $C_n^3(3n-8)^{n-5}$ из [17] (решение там не приводится).

a) Число корневых тетраэдральных деревьев может быть посчитано с помощью кодирования, аналогично числу корневых треугольных деревьев.

Построение кода по дереву. Выберем корневой треугольник, например, треугольник $(1,2,3)$. Элементами кодовой последовательности будут треугольники — грани тетраэдров. Пусть вершина x была подвешена к грани с номерами вершин a, b и c, где $a<b<c$, будем называть эту грань предком вершины x. Обозначим грань (x,a,b) через $x\alpha$, (x,a,c) через $x\beta$, (x,b,c) через $x\gamma$. Таким образом, грани тетраэдра получили обозначения $x\alpha$, $x\beta$, $x\gamma$, где $x=4,\ldots,n$, а корневую крань мы обозначим $(1,2,3)$. Всего граней $3n-8$. Назовем листом тетраэдрального дерева вершину степени 3. На каждом шаге отрываем лист с наибольшим номером и записываем его грань-предка. Когда остается последний тетраэдр (4 вершины), мы останавливаемся.

Построение дерева по коду. Листьями являются вершины тетраэдального дерева с такими номерами $x\in\{4,\ldots,n\}$, для которых текущий код не содержит ни одной из граней $x\alpha$, $x\beta$, $x\gamma$.

Пример. Пусть имеется 7 вершин и код Прюфера $(4\beta,\ (1,2,3),\ 7\alpha)$.

Номер шага	Текущий код	Список листьев	Подвешенная вершина
1	$(4\beta,\ (1,2,3),\ 7\alpha)$	6, 5	6
2	$((1,2,3),\ 7\alpha)$	5, 4	5
3	(7α)	4	4
4	$()$	7	7

Читаем список подвешенных вершин в обратном порядке и получаем, что последовательно были подвешены вершины 7 к грани $(1,2,3)$, 4 к грани $7\alpha=(7,1,2)$, 5 к грани $(1,2,3)$, 6 к грани $4\beta=(4,1,7)$.

Получившееся тетраэдральное дерево показано на рис. 4.

Код содержит $n-4$ грани. Значит, всего возможных кодов $(3n-8)^{n-4}$.

b) Так как выделенное ребро тетраэдрального дерева может быть помечено любой тройкой меток, а не только 1, 2, 3, а любой из $5n-8$ треугольников в тетраэдральном дереве можно назначить корнем, выполняется соотношение

$$C_n^3\Lambda_n=(3n-8)\Delta_n.$$

4 Парковочные функции

4.1. Эта знаменитая задача поставлена в [15].

Увеличим стоянку, добавив $(n+1)$-е место для парковки, и замкнем улицу в цикл так, чтобы с $(n+1)$-го места она вела обратно к первому. Теперь имеется ровно $(n+1)^n$ последовательностей предпочтения (каждый из n водителей независимо от других может предпочитать одно из $n+1$ мест). Приезжая на круговую стоянку по описанному правилу, все n водителей смогут припарковаться при любых предпочтениях, причем одно место парковки останется свободным. Последовательность предпочтений удовлетворяет требованию исходной задачи тогда и только тогда, когда свободным остается $(n+1)$-е место. Действительно, то, что $(n+1)$-е место остается свободным, означает, что оно не является любимым ни для кого из водителей, и никто из водителей не проезжает мимо него в поисках парковки (иначе он припарковался бы там, а не проехал мимо). В таком случае можно закрыть $(n+1)$-е место парковки и прилегающий участок дороги (то есть вернуться к исходной задаче), не нарушая процесса поиска парковок.

Разобьем все последовательности предпочтений круговой стоянки на $(n+1)^{n-1}$ групп по $n+1$ последовательностей в каждой: в одну группу с последовательностью $(a_1, \ldots, a_n)$ отнесем те, которые получаются из нее циклическим сдвигом номеров мест парковки, т. е. $(a_1+1, \ldots, a_n+1)$, $(a_1+2, \ldots, a_n+2)$, $\ldots$, $(a_1+n, \ldots, a_n+n)$ (сложения по модулю $n+1$). В каждой группе имеется ровно одна последовательность предпочтений, удовлетворяющая требованию исходной задачи, а именно, та, в которой свободному месту соответствует номер $n+1$. Значит, искомое число последовательностей равно числу групп, т. е. $(n+1)^{n-1}$.

4.2. Более-менее ясно, что происходит, если поменять местами два соседних автомобиля.

4.3. Ответ: n^{n-1}.

Действуя как и в задаче 4.1, получаем, что на расширенной парковочной улице количество всевозможных последовательностей предпочтения равно $(n+1)n^{n-1}$, поскольку у первого водителя может быть $n+1$ любимое место, а у всех остальных — по n. При этом в каждой группе из $n+1$ последовательностей, отличающихся циклическим сдвигом, содержится ровно одна парковочная функция. Мы взяли эту задачу из книги [12].

4.4. Ответ: $(n+1-m)(n+1)^{m-1}$ последовательностей.

Решение 1. Рассмотрим расширенную парковочную улицу, как в задаче 4.1. Для m водителей существует $(n+1)^m$ всевозможных «расширенных» последовательностей предпочтений на этой улице. Разобьем их на группы по $(n+1)$ последовательностей, как в задаче 4.1, получится $(n+1)^{m-1}$ групп. Если в результате парковки $(n+1)$-е место оказалось свободно, то никто из водителей не любит $(n+1)$-е место и расширенная последовательность на самом деле является парковочной последовательностью для исходной улицы. Очевидно, каждая группа содержит в точности $n+1-m$ последовательностей, для которых $(n+1)$-е место оказывается свободным. Поэтому общее число парковочных последовательностей равно $(n+1-m)(n+1)^{m-1}$.

Решение 2 из книги [2, задача 96.54].

Для каждого целого m, $0 \leqslant m \leqslant n$, обозначим через $N(n,m)$ количество последовательностей предпочтения для m водителей, которые приводят к успешной парковке (в частности, $N(n,0) = 1$). Докажем индукцией по n, что $N(n,m) = (n+1-m)(n+1)^{m-1}$ при всех m. При $n = 1$ утверждение тривиально.

Переход от $n-1$ к n. Пусть k водителей любят места парковки, отличные от первого, а $m-k$ любят первое место ($0 \leqslant k \leqslant m$). Эти k водителей могут быть выбраны C_m^k способами. Нетрудно убедиться, что при заданных предпочтениях успех или неуспех парковки водителей не зависит от того, в каком порядке они приезжают. Поэтому можно считать, что $m-k$ водителей, которые любят первое место парковки, приезжают самыми последними. Эти $m-k$ водителей заведомо сумеют припарковаться — они займут первые $m-k$ свободных мест, оставшихся после первых k водителей. Значит, успех или неуспех парковки определяется только предпочтениями первых k водителей среди отведенных им $n-1$

мест. Значит, при заданном выборе этих k водителей имеется ровно $N(n-1,k)$ удачных последовательностей предпочтений. Таким образом,

$$N(n,k) = \sum_{k=0}^{m} C_m^k \cdot N(n-1,k)\,. \tag{1}$$

Подставим индукционное предположение и преобразуем:

$$N(n,k) = \sum_{k=0}^{m} C_m^k (n-k) n^{k-1} = \sum_{k=0}^{m} C_m^k n^k - \sum_{k=1}^{m} k \cdot C_m^k n^{k-1} = \sum_{k=0}^{m} C_m^k n^k - \sum_{k=1}^{m} m \cdot C_{m-1}^{k-1} n^{k-1} =$$
$$= \sum_{k=0}^{m} C_m^k n^k - m \cdot \sum_{k=0}^{m} C_{m-1}^k n^k = (n+1)^m - m \cdot (n+1)^{m-1} = (n+1-m) \cdot (n+1)^{m-1}\,,$$

что и требовалось. Здесь использовались тривиальная формула $k \cdot C_m^k = m \cdot C_{m-1}^{k-1}$ и бином Ньютона для разложения $(n+1)^m$ и $(n+1)^{m-1}$ по степеням n.

4.5. Пусть $b_1, b_2, \ldots, b_n$ — последовательность предпочтений, выписанная в порядке неубывания. Тогда $b_1 = b_2 = \ldots = b_k = 1$, $2 \leqslant b_{k+1} \leqslant b_{k+2} \leqslant \ldots$. Заметим, что последовательность предпочтений $b_{k+1}, b_{k+2}, \ldots, b_n$ позволяет $n-k$ водителям припарковаться на улице, где имеется $n-1$ парковочное место (это места со 2-го по n-е). Число таких последовательностей подсчитано в предыдущей задаче и равно $k \cdot n^{n-k-1}$. Количество способов выбрать среди n человек k желающих парковаться на первом месте равно C_n^k. Таким образом, общее число паковочных функций, для которых k человек хотели бы парковаться на первом месте, равно $C_n^k \cdot k \cdot n^{n-k-1} = C_{n-1}^{k-1} n^{n-k}$.

«Для проверки» просуммируем найденные выражения по k:

$$\sum_{k=1}^{n} C_{n-1}^{k-1} n^{n-k} = (n+1)^{n-1}$$

(формула бинома). Получилось число парковочных функций. Вот и хорошо.

Как видим, число парковочных функций в этой задаче такое же, как количество лесов на множестве $[n]$, состоящих из k корневых деревьев (задача 3.4).

Приведем биекцию из [13], дающую комбинаторное доказательство этого факта. Пусть дано дерево на $n+1$ вершине с корнем 0. Построим по нему очередь поиска в ширину. Сначала добавим в очередь корень дерева. Далее на каждом шаге вынимаем первую в очереди вершину и добавляем в конец очереди всех ее сыновей в порядке возрастания их номеров. И так далее, пока очередь не опустеет. Пусть A_i — это множество вершин, добавленных в очередь на i-том шаге (это все сыновья некоторой вершины), a_i — число элементов A_i. Если на шаге i ничего не добавили, то множество A_i пусто. Поскольку дерево является связным графом на $n+1$ вершине, то очередь поиска в глубину для него содержит хотя бы один элемент, пока не будет вынута $n+1$ вершина, и опустеет, когда вершины закончатся, то есть a_i удовлетворяют условиям:

$$\begin{cases} a_1 \geqslant 1 \\ a_1 + a_2 - 1 \geqslant 1 \\ \ldots \\ a_1 + a_2 + \ldots + a_k - k \geqslant 1 \\ a_1 + a_2 + \ldots + a_{n+1} = n \end{cases}$$

Определим парковочную функцию по следующему правилу: элементы множества A_i будут номерами машин, которые хотят припарковаться на месте i. Можно доказать, что построенное отображение является биекцией между парковочными функциями для n машин и деревьями на $n+1$ вершине.

4.6. Достаточно описать обратное отображение, т. е. правило, позволяющее по произвольной последовательности $c = (c_1, c_2, \ldots, c_{n-1})$, где все c_i суть остатки по модулю $n+1$, построить парковочную функцию $a = (a_1, \ldots, a_n)$, для которой c является разностной последовательностью. Это легко получается с помощью решения задачи 4.1.

Действительно, если фиксированы все разности $c_i = a_{i+1} - a_i \pmod{n+1}$, существует ровно $n+1$ последовательностей предпочтений для круговой стоянки с такими разностями. В решении 4.1 именно эти $(n+1)$ последовательностей объединены в одну группу и доказано, что в этой группе содержится ровно одна парковочная функция. Очевидно, она-то нам и нужна.

4.7. Приведенная сумма подсчитывает всевозможные парковочные функции. Действительно, чтобы задать парковочную функцию, сначала для каждого парковочного места i выберем число k_i, показывающее, сколько человек любит парковаться на этом месте. Неотрицательные числа k_i должны удовлетворять ограничениям:

$k_n \leqslant 1$, так как при наличии двух желающих парковаться на последнем месте парковка невозможна;

$k_{n-1} + k_n \leqslant 2$, так как при наличии трех желающих парковаться на двух последних местах парковка не состоится;

и т. д. до неравенства $k_2 + \ldots + k_{n-1} + k_n \leqslant n - 1$.

После того как числа k_2, k_3, …, k_n выбраны, положим $k_1 = n - k_2 - k_3 - \ldots - k_n$ и назначим последних k_1 человек желающими парковаться на первом месте.

Нетрудно понять, что построенный набор чисел реализуется как парковочная функция. Действительно, по задаче 4.2 порядок, в котором прибывают автомобили, нам неважен. Запуская на парковку, сначала тех, кто хочет парковаться на n-м месте, потом на $(n-1)$-м и т. д., мы прекрасненько всех припаркуем.

Осталось понять, что количество способов реализовать выбранные количества персонально равно стоящему в сумме полиномиальному коэффициенту.

4.8. Решение 1 (из книги [8, задача 5.49.f]). Пусть r_i — число элементов в последовательности a, равных i, в частности, $r_n = 0$. Определение надежной парковочной функции эквивалентно условиям:

1) все частичные суммы последовательности $r_1 - 1$, $r_2 - 1$, …, $r_{n-1} - 1$ положительны;

2) $\sum\limits_{i=1}^{n-1} (r_i - 1) = 1$.

Лемма. Для любой конечной целочисленной последовательности с суммой 1 существует единственная циклическая перестановка, у которой все частичные суммы положительны.

Очевидно, в надежной последовательности предпочтений все a_i — это числа от 1 до $n-1$. Если мы возьмем произвольный набор чисел из $[n-1]^n$, то определенные этим наборам чи́сла r_i удовлетворяют условию 2), но, вообще говоря, не удовлетворяют условию 1). Однако по лемме у этого набора чисел существует, и при том только одна, циклическая перестановка, удовлетворяющая первому условию!

Таким образом, количество надежных парковочных функций в $n-1$ раз меньше числа элементов в $[n-1]^n$.

Решение 2 (прямолинейный подсчет). Рассмотрим произвольную надежную парковочную функцию, пусть для нее k водителей хотят припарковаться на 1 месте ($2 \leqslant k \leqslant n$). Дадим одному из них красную кепку и удалим. Предпочтения оставшихся образуют обычную парковочную функцию на дороге с $n-1$ парковочным местом и $k-1$ желающим припарковаться на первом месте. Таким образом, чтобы получить парковочную функцию, где k водителей хотят припарковаться на 1 месте, нужно выбрать водителя в кепке (n способов) назначить предпочтения оставшимся (по задаче 4.5 это можно сделать $(n-1)^{n-k}C_{n-2}^{k-2}$ способами). Правда, получится не просто парковочная функция, а парковочная функция, наделяющая одого из k претендентов на первое место кепкой. Значит, количество искомых парковочных функций выражается суммой $\sum\limits_{k=2}^{n} \frac{n}{k} \cdot (n-1)^{n-k} C_{n-2}^{k-2}$. Нам остается проверить

тождество

$$\sum_{k=2}^{n} \frac{n}{k} \cdot (n-1)^{n-k} C_{n-2}^{k-2} = (n-1)^{n-1}.$$

Преобразуем левую часть: заменим индекс суммирования k на $i = n-k$, воспользуемся тем, что $\frac{n}{n-i} \cdot C_{n-2}^{i}(n-1) = (n-1-i)C_n^i$ после чего разобьем каждое слагаемое на две части:

$$\sum_{k=2}^{n} \frac{n}{k} \cdot (n-1)^{n-k} C_{n-2}^{k-2} = \sum_{i=0}^{n-2} \frac{n}{n-i} \cdot C_{n-2}^{i}(n-1)^i = \sum_{i=0}^{n-2} (n-1-i) \cdot C_n^i (n-1)^{i-1} =$$
$$= \sum_{i=0}^{n-2} C_n^i (n-1)^i - \sum_{i=0}^{n-2} C_n^i \cdot i(n-1)^{i-1}.$$

В последнем выражении первая сумма по формуле бинома равна

$$n^n - C_n^n (n-1)^n - C_n^{n-1}(n-1)^{n-1}. \tag{2}$$

Для второй суммы отбросим нулевое слагаемое, сделаем преобразование $C_n^i \cdot i = nC_{n-1}^{i-1}$, и тогда она тоже считается с помощью бинома:

$$\sum_{i=0}^{n-2} C_n^i \cdot i(n-1)^{i-1} = n \sum_{i=1}^{n-2} C_{n-1}^{i-1}(n-1)^{i-1} = n\big(n^{n-1} - C_{n-1}^{n-1}(n-1)^{n-1} - C_{n-1}^{n-2}(n-1)^{n-2}\big). \tag{3}$$

Осталось заметить, что разность выражений (2) и (3) равна $(n-1)^{n-1}$.

4.9. Пусть b_1, b_2, …, b_{n+1} — последовательность номеров любимых мест, выписанная в порядке возрастания. Тот факт, что все сумеют припарковаться, означает выполнение неравенств $b_1 \leqslant 1$ (следовательно, $b_1 = 1$), $b_2 \leqslant 2$, …, $b_{n+1} \leqslant n+1$.

Выберем наибольшее k, $0 \leqslant k \leqslant n$, для которого $b_{k+1} = k+1$. Тогда последовательность предпочтений b_1, …, b_k является парковочной функцией для улицы с k парковками, а последовательность $b_{k+1} - k$, $b_{k+2} - k$, …, $b_{n+1} - k$ — надежная парковочная функция для улицы с $n+1-k$ парковками. (Надежность следует из максимальности k.) Верно и обратное: выбор парковочной последовательности b_1, …, b_k и надежной парковочной последовательности $b_{k+1} - k$, $b_{k+2} - k$, …, $b_{n+1} - k$ позволяет задать парковочную функцию для все улицы.

Таким образом, чтобы построить произвольную парковочную функцию на улице с $n+1$ парковкой, нужно выбрать любое k, выбрать C_{n+1}^k произвольных k водителей, назначить для их предпочтений одну из P_k парковочных функций, а для остальных $n+1-k$ водителей в качестве препочтений назначить одну из $(n-k)^{n-k}$ надежных парковочных функций. Это и есть комбинаторное истолкование рассматриваемой формулы.

4.10. Аналогично задаче 4.7 формула подсчитывает количество надежных парковочных функций на парковке длины n.

4.11. В [10] эта формула доказана с помощью непростой биекции с помеченными деревьями. Мы докажем ее, пользуясь сходством с предыдущими задачами.

Назовем модернизированной парковочной функцией любую парковочную последовательность $(a_1, \ldots, a_n)$, в которой дополнительно пронумерованы все элементы, равные 1. Например, $(\underset{1}{1}, 2, \underset{2}{1}, 3, 3)$ и $(\underset{2}{1}, 2, \underset{1}{1}, 3, 3)$ — две различные модернизированные парковочные функции (для $n = 5$). Количество модернизированных парковочных функций на парковке длины n обозначим $N^*(n)$.

Рассуждая как в задаче 4.7, мы получаем, что сумма подсчитывает количество модернизированных парковочных функций. Осталось проверить, что $N^*(n) = n^n$.

Рассмотрим модернизированные парковочные последовательности, в которых k человек любят НЕ первое место, а $n-k$ предпочитают парковаться на первом месте. Пользуясь

обозначениями и рассуждениями задачи 4.4, заключаем, что число таких последовательностей равно $\frac{n!}{k!}N(n-1,k)$. И тогда суммарное количество модернизированных парковочных функций задается формулой, аналогичной формуле (1):

$$N^*(n) = \sum_{k=0}^{n} \frac{n!}{k!} \cdot N(n-1,k) = \sum_{k=0}^{n} \frac{n!}{k!} \cdot (n-k)n^{k-1}.$$

Это телескопическая сумма, она равна n^n.

5 *Инверсии на деревьях и неудобства парковочных функций*

5.1. Оба утверждения навеяны [16].

a) Возьмем произвольное помеченное дерево на n вершинах. Пусть n–u — это первое ребро на пути из вершины n в вершину 1 (возможно, $u = 1$). Удалим это ребро, дерево распадется на два дерева A_n и A_1. При этом в дереве A_1 естественным образом выделена вершина u, т. е. можно считать, что это дерево корневое. Пусть дерево A_1 имеет $k+1$ вершину, $0 \leqslant k \leqslant n-2$. Тогда дерево A_n имеет $n-k-1$ вершин. Очевидно, помеченный лес (A_n, A_1) однозначно задается исходным помеченным деревом на n вершинах.

Покажем, как устроено обратное отображение. Для каждого k, $0 \leqslant k \leqslant n-2$, выберем вершины для дерева A_1. Поскольку вершина 1 должна находиться в дереве A_1, а вершина n — в дереве A_n, для этого нужно выбрать k вершин среди всех элементов множества $[n]$, кроме 1 и n; это можно сделать C_{n-2}^k способами. Остальные $n-k-1$ вершин будут принадлежать дереву A_n. Далее построим сами деревья A_1 и A_n — это можно сделать соответственно $(k+1)T_{k+1}$ и T_{n-k-1} способами. Наконец, нам нужно «скрепить» деревья, для этого нужно провести ребро, соединяющее вершину n с любой корнем дерева A_1. Мы получили комбинаторное истолкование k-го слагаемого из суммы в правой части доказываемого тождества: оно равно количеству остовных лесов на множестве $[n]$, состоящих ровно из двух деревьев, таких что одно дерево содержит вершину n и кроме нее еще k других вершин, а другое дерево — корневое и содержит вершину 1.

b) Рассмотрим произвольную парковочную функцию $a = (a_1, a_2, \ldots, a_{n+1})$ для улицы с $n+1$ парковочным местом. Пусть водители въехали на улицу в порядке возрастания номеров и последнему из них досталось место k. Зафиксируем предпочтения первых n водителей и попытаемся увеличить предпочтение последнего водителя, насколько это возможно, т. е. подберем максимальное a_{n+1}, для которого последовательность $(a_1, a_2, \ldots, a_{n+1})$ остается парковочной функцией. Очевидно, этим максимальным значением является $a_{n+1} = k$, причем никто из остальных водителей не претендовал на k-е место, а также никто из тех, кто не смог припарковаться на любимом месте, не проезжал мимо k-го места. Отсюда следует, что ровно $k-1$ человек предпочитали парковаться на местах с 1-го $(k-1)$-е и ровно $n+1-k$ человек предпочитали парковаться на местах с $(k+1)$–го по $(n+1)$-е. Положим, $\widetilde{a} = (a_1, a_2, \ldots, a_n, k)$ и будем называть эту последовательность укрупнением последовательности a.

Ясно, что при любом $\ell \leqslant k$ последовательность $(a_1, a_2, \ldots, a_n, \ell)$ является парковочной функцией, и из каждой из этих k парковочных функций (и только из них) при укрупнении получается фунция $\widetilde{a}$.

Как же нам задать последовательность $\widetilde{a}$? Последний водитель выделен изначально. Нужно выбрать $k-1$ водителя, которые будут парковаться на первых $k-1$ местах (C_n^{k-1} вариантов) и назначить им парковочную функцию (P_{k-1} вариантов). Далее нужно задать парковочную функцию для тех, кто паркуется на местах после k-го ($P_{n-(k-1)}$ вариантов). Итак, для выбора последовательности $\widetilde{a}$ имеется $C_n^{k-1}P_{k-1}P_{n-(k-1)}$ вариантов. Вспоминая, что последовательность $\widetilde{a}$ является укрупнением k различных парковочных функций, заключаем, что число парковочных функций P_{n+1} вычисляется по формуле

$$P_{n+1} = \sum_{k=1}^{n+1} C_n^{k-1} k P_{k-1} P_{n-(k-1)}$$

5.2. Ответ: $F_n^*(x) = \sum\limits_{k=0}^{n} C_n^k F_k(x) F_{n-k}(x)$.

5.3. Оба утверждения взяты из [16]. Эти рекурсии уточняют рекурсии из задачи 5.1.

a) Заметим, что в определении величины $\mathrm{inv}(T)$ можно считать, что метки вершин — это любые вещественные числа. Кроме того, зафиксируем правило, что корень не используется при подсчете числа инверсий дерева, и тогда совершенно неважно, какой меткой он помечен.

Дадим полезное определение. Пусть дано помеченное корневое дерево T на множестве $[\ell]$ и фиксировано множество чисел $S = \{s_1, s_2, \ldots, s_\ell\}$. Определим семейство, состоящее из ℓ корневых деревьев T_1, T_2, $\ldots$, T_ℓ, вершины которых помечены элементами множества S. Дерево T_i получается из дерева T с помощью замены его меток на метки из множества S следующим образом. В корень дерева T вместо имеющейся там метки ставится метка s_i. Остальные элементы множества S упорядочиваются по возрастанию и расставляются в некорневых вершинах дерева T так, «как это сделано в дереве T»: самая маленькая метка ставится в вершину 1, следующая по величине метка ставится в вершину 2 и т. д. Очевидно, количество инверсий у всех деревьев этого семейства одинаково. Будем называть множество деревьев из этого семейства *равноинверсными* друг другу.

Вернемся к решению задачи. Дополним рассуждения решения 5.1 a) подсчетом инверсий. Чтобы не менять обозначений, докажем требуемое соотношение, взяв вместо параметра n значение $n-2$ (напомним, что многочлен F_n строится по множеству деревьев с $n+1$ вершинами):

$$F_{n-1}(x) = \sum_{k=0}^{n-2} C_{n-2}^k (x^k + x^{k-1} + \ldots + 1) F_k(x) F_{n-k-2}(x).$$

Итак, в решении 5.1 a) всевозможные помеченные деревья находятся во взаимно однозначном соответствии с лесами (A_n, A_1). Чтобы задать лес (A_n, A_1), нужно выбрать k вершин для дерева A_1 среди всех элементов множества $[n]$, кроме 1 и n, (получается C_{n-2}^k вариантов, остальные $n-k-1$ вершин автоматически попадут в дерево A_n) и построить сами деревья A_1 и A_n, при этом дерево A_1 корневое. Далее мы «скрепляем» деревья, проводя ребро, соединяющее вершину n с корнем дерева A_1.

Чтобы подсчитывать инверсии, зафиксируем деревья A_n и A_1 и сгруппируем в один кластер $k+1$ лесов вида (A_n, A), где A пробегает множество корневых деревьев, равноинверсных дереву A_1. Число инверсий в образовавшемся дереве $T \in \mathcal{T}_n$ равно $\mathrm{inv}(A_n) + \mathrm{inv}(A) + \delta_A$, где поправка δ_A равна числу инверсий, которые образует в дереве T корневая вершина дерева A с другими вершинами дерева A (будучи корнем дерева A, она не участвовала в подсчете величины $\mathrm{inv}(A)$, а после скрепления деревьев участвует). Как мы отмечали, $\mathrm{inv}(A) = \mathrm{inv}(A_1)$ для всех деревьев A, равноинверсных дереву A_1. Что же касается поправки δ_A, нетрудно понять, что она по одному разу принимает значения 0, 1, 2, $\ldots$, k, когда A пробегает множество всех деревьев, равноинверсных дереву A_1.

Каждый лес (A_n, A) из нашего кластера определяет слагаемые $x^{\mathrm{inv}(A_n)}$, $x^{\mathrm{inv}(A)}$ в нумераторах $F_{n-k-2}(x)$, $F_k(x)$. Показатель их произведения $x^{\mathrm{inv}(A_n)+\mathrm{inv}(A)}$ равен числу инверсий в образовавшемся графе без учета поправки. Перебирая все деревья, равноинверсные A_1, получаем произведение $(x^k + x^{k-1} + \ldots + 1)x^{\mathrm{inv}(A_n)+\mathrm{inv}(A)}$, которое дает сумму одночленов, с точностью до перестановки равную слагаемым нумератора $F_{n-1}(x)$ для деревьев, порожденным нашим кластером. Суммируя по всем кластерам, получем требуемую формулу.

b) Дополним рассуждения решения 5.1 b) подсчетом неудобств. В этом решении множество парковочных функций разбито на кластеры. В один кластер с парковочной функцией $a = (a_1, a_2, \ldots, a_{n+1})$ входят парковочные функции $(a_1, a_2, \ldots, a_n, i)$, где $1 \leqslant i \leqslant k$, а через k обозначено максимальное возможное предпочтение $(n+1)$-го водителя, при котором последовательность $(a_1, a_2, \ldots, a_n, k)$ все еще остается парковочной функцией.

Для перечисления всевозможных парковочных функций с заданным параметром k мы перебираем всевозможные функции a' для тех, кто паркуется на первых $k-1$ местах, и всевозможные функции a'' для тех, кто паркуется на последних $n-(k-1)$ местах. Позволяя некоторую вольность речи, скажем, что неудобство этих парковочных выриантов равно $D(a')$ и $D(a'')$, а на языке нумераторов — $x^{D(a')}$ и $x^{D(a'')}$. Что же касается $(n+1)$-го человека, который по нашему плану паркуется на k-м месте, то его вклад в общее неудобство принимает для функций из нашего кластера по одному разу значения 0, 1, $\ldots$, $k-1$. Таким образом, суммарное неудобство парковочных функций из одного кластера записывается выражением $(x^{k-1} + x^{k-2} + \ldots + 1)x^{D(a')}x^{D(a'')}$. Суммируя по всем кластерам, получаем требуемую формулу.

5.4. Требуемая биекция коротко описана в [19]. Следующую конструкцию, которая привносит в эти рассуждения дополнительные подробности, нам любезно сообщил И. Богданов.

Рассмотрим произвольное помеченное дерево T с $n+1$ вершиной без инверсий. Как обычно, мы считаем вершину $n+1$ корнем, вводя тем самым отношение «предок–потомок». Припишем к каждой вершине, кроме корня, целое неотрицательное число, не превосходящее числа её потомков (исключая её саму); это число будем называть *плохостью* вершины. Полученный объект (помеченное дерево с приписанными плохостями) назовём *оснащённым деревом* (или кратко *о-деревом*), а множество всех оснащённых деревьев с $n+1$ вершиной обозначим через $\mathcal{E}_{n+1}$. Сумму всех плохостей вершин о-дерева E назовём *плохостью* о-дерева и обозначим $\mathrm{bad}(E)$.

Требуемая биекция является композицией двух биекций, описанных ниже.

(i): Биекция между $\mathcal{E}_{n+1}$ и $\mathcal{T}_{n+1}$. **Только** в рамках построения этой биекции мы будем **различать** *вершину* дерева и *число*, которым она помечена (т.е. *пометку* вершины). Это полезно, ибо в процессе построения биекции пометки будут переставляться.

Назовём *инверсностью* вершины помеченного дерева количество её потомков, числа в которых больше, чем число в самой вершине. Ясно, что количество инверсий в дереве равно сумме инверсностей его вершин.

Мы устроим биекцию следующим образом. По о-дереву $E \in \mathcal{E}_{n+1}$ мы построим дерево $T \in \mathcal{T}_{n+1}$ такое, что

(a) T и E соответствуют одному и тому же *непомеченному* дереву, и их корни совпадают;

(b) плохость любой *вершины* в E равна её инверсности в T.

Как следствие, $\mathrm{bad}(E) = \mathrm{inv}(T)$.

Для этого в о-дереве E надо переставить пометки вершин. Мы будем делать это «сверху вниз», обработав сначала всех сыновей корня, затем всех их сыновей и т. д. Пусть v — очередная вершина, которую надо обработать, i — её плохость в о-дереве, а $a_1 > a_2 > \ldots > a_k$ — текущие пометки её и всех её потомков в убывающем порядке (тогда a_1 — пометка в v, и $k > i$). Переставим метки $a_1, \ldots, a_{i+1}$ так: поставим a_{i+1} в v, а a_{j+1} заменим на a_j при всех $j = 1, 2, \ldots, i$. Нетрудно понять, что инверсность v стала равна i, никакие два потомка v инверсии не образуют, и инверсности остальных вершин не поменялись (ибо не поменялись множества их потомков). Значит, обработав таким образом все вершины, мы получим дерево T с требуемыми свойствами.

На рисунке ниже показан пример действия этого алгоритма (индексы указывают плохости вершин).

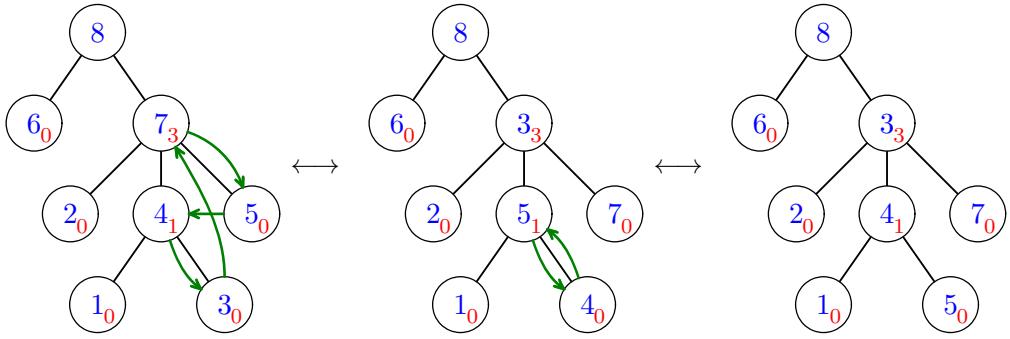


Рис. 7. Построение T по E (и наоборот)

Чтобы построить обратное отображение из $\mathcal{T}_{n+1}$ в $\mathcal{E}_{n+1}$, заметим, что плохости вершин в E расставляются автоматически, исходя из условия (b). Перестановка же пометок строится похожим образом снизу вверх. Когда обрабатывается вершина v, никакие два её потомка не образуют инверсии. Пусть $a_1 > \ldots > a_k$ — пометки её и её потомков, причём в v стоит a_{i+1}. Тогда достаточно переставить метки по циклу $a_1 \to a_{i+1} \to a_i \to \ldots \to a_1$. В результате этого процесса получится требуемое о-дерево.

Легко видеть, что построенные отображения взаимно обратны.

(ii): Биекция между $\mathcal{P}_n$ и $\mathcal{E}_{n+1}$. Пусть $a = (a_1, \ldots, a_n)$ — парковочная функция, а $p_1, \ldots, p_n$ — номера мест, на которых припарковались соответствующие водители; тогда $p = (p_1, \ldots, p_n)$ — перестановка чисел $1, 2, \ldots, n$. Назовём *неудобством* i-го водителя величину $p_i - a_i$; суммарное неудобство всех водителей есть неудобство функции a.

Мы устроим биекцию следующим образом. По функции a мы построим о-дерево $E \in \mathcal{E}_{n+1}$ такое, что

(c) плохость вершины с пометкой k равна неудобству водителя k.

Как следствие, $\mathrm{bad}(E) = D(a)$, а значит, композиция двух наших биекций — требуемая.

Осталось, собственно, предъявить вторую биекцию. Мы начнём с более простой биекции — между перестановками $p = (p_1, \ldots, p_n)$ и помеченными деревьями $T \in \mathcal{T}_{n+1}$ без инверсий. Затем мы продолжим эту биекцию на парковочные функции и оснащённые деревья.

Шаг 1. Сопоставление перестановок деревьям без инверсий. Положим $p_{n+1} = n + 1$ и рассмотрим числа 1, 2, …, $n+1$ как вершины строящегося дерева; назовём число p_i *местом* вершины i. Для каждой вершины $i \leqslant n$ найдём наименьшее из мест p_j при $j > i$, которое больше p_i, и соединим i с j. Мы получим связный граф (все вершины соединены путём с $n + 1$) с n рёбрами, т. е. дерево T. (Процесс получения этого дерева удобно представлять себе «справа налево»: мы по очереди рассматриваем вершины $n, n-1, \ldots, 1$ и подсоединяем их к получающемуся справа дереву согласно правилу.)

Исследуем полученное дерево. Ясно, что в описанной выше ситуации i — сын j. Выберем произвольную вершину $j \leqslant n$. Для любого потомка k вершины j выполнены неравенства $k < j$ и $p_k < p_j$ (в частности, в дереве нет инверсий). Пусть $s > j$ — вершина, для которой $p_s < p_j$, и p_s максимальное возможное (если такого нет, положим $p_s = 0$). Тогда, рассмотрев процесс получения дерева справа налево, нетрудно видеть, что выполнено следующее свойство:

(d) места всех потомков вершины j больше p_s и меньше p_j,

и наоборот — все вершины с такими местами являются потомками j (ибо они присоединяются либо к j, либо к её потомкам).

Свойства (c) и (d) позволяют по дереву T восстановить перестановку p, действуя опять же справа налево. Начнём с вершины n; согласно (d), места её и её потомков в точности составляют число от 1 до p_n; поэтому p_n есть число её потомков. Далее действуем аналогично: рассматривая очередную вершину j, являющуюся сыном некоторой вершины k, мы знаем, что p_j должно лежать между p_s и p_k, где p_s — наибольшее уже определённое место, меньшее p_k. Значит, если у j ровно d потомков, то они будут иметь места $p_s + 1, \ldots, p_s + d$, а само p_j равно $p_s + d + 1$. Таким образом, перестановка (p_i) восстановлена.

На рисунке ниже показана работа обоих алгоритмов. Около вершин дерева справа указаны восстанавливаемые значения p_i, а также определяемый диапазон мест их потомков.

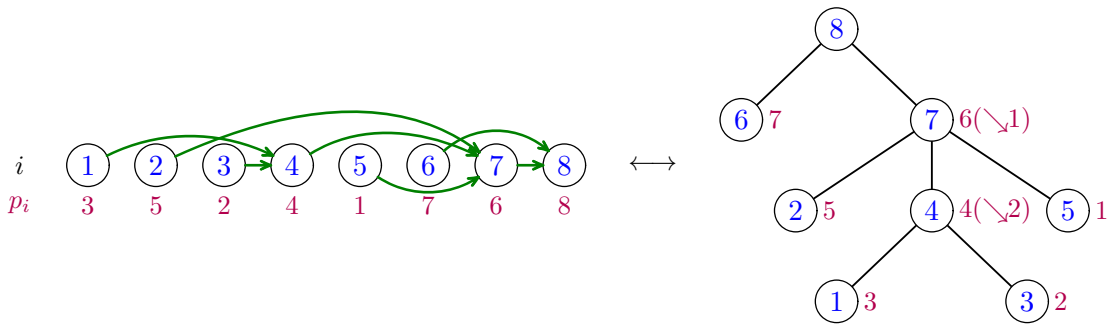


Рис. 8. Построение T по p (и наоборот)

Теперь нетрудно видеть, что построенные отображения действительно взаимно обратны. Действительно, отображение $T \mapsto p$ строилось так, чтобы восстановить исходную перестановку, если T было по ней построено. Наоборот, пусть мы построили p по T. Выберем любое $i \leqslant n$, являющееся сыном k в дереве T. Пусть $j > i$ — та вершина, к которой i подсоединится в обратной процедуре. Тогда $p_i < p_j \leqslant p_k$, то есть j — потомок k или сама k. С другой стороны, по построению p, все потомки k, лежащие между i и k, получали места, меньшие p_i. Значит, $j = k$, и по перестановке p восстанавливается именно T.

Шаг 2: Оснащение. Теперь можно построить требуемую биекцию. Пусть a — парковочная функция, а p — соответствующая ей перестановка. Тогда по p можно построить помеченное дерево T и оснастить его согласно (c), сопоставив вершине j плохость $p_j - a_j$. Согласно (d), число потомков j равно $p_j - p_s - 1$. С другой стороны, когда машина j попала на место p_j, место p_s было свободным; значит, $a_j > p_s$, так что $p_j - a_j \leqslant p_j - p_s - 1$, т. е. плохость вершины j не превосходит числа её потомков. Итого, мы получили о-дерево E. Наоборот, по о-дереву E (точнее, по подлежащему помеченному дереву T) можно восстановить перестановку p, а по ней — функцию a, опять же согласно (c). Ясно, что если по a псстроить E, то по E восстановится именно функция a. Осталось понять, что, наоборот, если по произвольному $E \in \mathcal{E}_{n+1}$ построить функцию a, то по ней обратно построится дерево E.

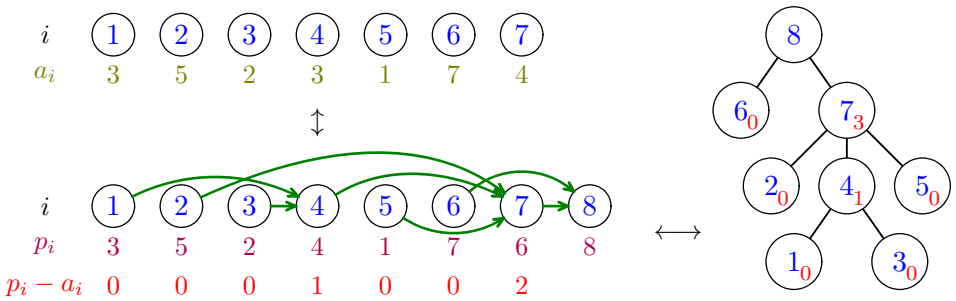


Рис. 9. Оснащение дерева

Для начала покажем, что полученная функция a — парковочная. Поскольку $a_i \leqslant p_i$, а (p_i) — перестановка, для этого достаточно показать, что $a_i > 0$. Это просто: если у вершины i есть d потомков, все они имеют номера, меньшие p_i; значит, p_i больше, чем d — и, как следствие, чем плохость вершины j. Отсюда и следует требуемое.

Осталось показать, что, если по о-дереву E получены перестановка $p = (p_i)$ и парковочная функция a, то, действуя по этой парковочной функции, водители образуют ровно перестановку p. Для начала вспомним, что согласно (d) места p_j всех потомков j вершины i и её самой образуют множество $A_j = \{p_i - d, \ldots, p_j - 1, p_j\}$, где d — число потомков j. Значит, $a_j \in A_j$.

Теперь нетрудно показать, что водитель i попадёт на место p_i, индукцией по i. При $i = 1$ это верно, ибо 1 — лист нашего дерева, то есть $p_1 = a_1$. Пусть все водители $j < i$ попали на предписанные места. В частности, попали на свои места все потомки i; значит, все места $p_i - d, \ldots, p_i - 1$ уже заняты, а p_i — свободно. Так как $a_i \in A_i$, отсюда и следует, что водитель i припаркуется на p_i. Доказательство окончено.

Литература

[1] *Айгнер М., Циглер Г.* Доказательства из Книги. М.:Мир, 2006.

[2] *Берлов С. Л., Иванов С. В., Кохась К. П.* Петербургские математические олимпиады. СПб.: «Лань», 2000.

[3] *Глибичук А. А., Дайняк А. Б., Ильинский Д. Г., Купавский А. Б., Райгородский А. М., Скопенков А. Б., Чернов А. А.* Элементы дискретной математики в задачах. М.:МЦНМО, 2016.

[4] *Иванов О. А.* Элементарная математика для школьников, студентов и преподавателей. М.:МЦНМО, 2009.

[5] Комбинаторный анализ. Задачи и упражнения. / Под. ред. К. А. Рыбникова. М.: Наука, 1982.

[6] *Ландо С. К.* Введение в дискретную математику. М.: МЦНМО, 2012.

[7] *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004.

[8] *Стэнли Р.* Перечислительная комбинаторика. Т. 2. М.: Мир, 2005.

[9] *Beineke L. W., Moon J. W.* Several proofs of the number of labelled 2-dimensional trees. In «Proof Techniques in Graph Theory» (F. Harary, editor). New York: Academic Press, 1969. P. 11-20.

[10] *Benjamin A. T., Juhnke F.* Another way of counting N^N. // SIAM J. Disc. Math. 1992. V. 5. No. 3. P. 377–379.

[11] *Bóna M.* Combinatorics of permutations. Chapman & Hall/CRC, 2004.

[12] *Bóna M.* A walk through combinatorics. 3rd ed. World Scientific Publ. Co., 2011.

[13] *Chassaing P. , Marckert J.-F.* Parking functions, empirical processes, and the width of rooted labeled trees // Electron. J. Combin. 2001. V. 8. № 1. Research Paper 14.

[14] *Guo S., Guo V.* A recursive algorithm for trees and forests // `http://arxiv.org/pdf/math/1702.01744v1.pdf`

[15] *Konheim A. G., Weiss B.* An occupancy discipline and applications. // SIAM J. Appl. Math. 1966. Vol. 14. № 6. P. 1266–1274.

[16] *Kreweras G.* Une famille de polynômes ayant plusieurs propriétés énumeratives // Period. Math. Hungar. V. 11. 1980. № 4. P. 309–320.

[17] *Moon J. W.* Counting labelled trees. William Clowes and Sons, 1970.

[18] *Shukla A.* A short proof of Cayley's tree formula // `https://arxiv.org/pdf/0908.2324.pdf`

[19] *Yan C. H.* Parking functions// in Handbook of Enumerative Combinatorics. M. Bóna, ed.

Around Cayley's theorem

Bursian O., Kokhas D., Kokhas K.

This project is related with Cayley's theorem about tree counting. Tree is a connected graph without cycles. The theorem states that the number of labelled trees with n vertices is equal to n^{n-2}. There exist many proofs of this theorem, our goal is to introduce some of them and to investigate applications of different approaches to the theorem.

There are rather difficult problems in each project. By the rules of the Summer conference it is allowed to come together in teams for problems solving; you may join in different teams for different projects. We recommend you to find companions, and make cooperative investigations of this project.

First acquaintance with labelled trees

In olympiad problems usually graphs with "unnamed" vertices are used. For example, vertices are some towns and edges are roads between them, or vertices are persons (without names) and edges are acquaintances etc. Another point of view is taken in problems about graph counting: all graph vertices should be "individual". To exclude terminology issues we define a "labelled graph".

Let $[n] = \{1, 2, \ldots, n\}$. A tree (or an arbitrary graph as well) with n vertices which are enumerated by numbers from 1 to n, is called a *labelled tree* (accordingly, a *labelled graph*). To construct a labelled tree we can take a tree and number its vertices, or contrariwise: we can consider the set $[n]$ as a set of vertices and draw a tree by connecting these vertices by edges. The set of all labelled trees with n vertices is denoted by $\mathcal{T}_n$.

Two (unlabelled) graphs G_1 and G_2 with vertex sets V_1 and V_2 are called *isomorphic* (or, speaking plainly, are the same) if there exists a one-to-one mapping $f\colon V_1 \to V_2$ such that vertices A, $B \in V_1$ are connected by an edge in G_1 if and only if $f(A)$ and $f(B)$ are connected by an edge in G_2. For example, any tree with four vertices is isomorphic to either the tree "Chicken's feet" or the tree "Path of length three". In case when G_1 and G_2 both are labelled trees, $V_1 = V_2 = [n]$, the identity plays the role of f.

We assume that Cayley's theorem should not be used in solutions of problems from section "First acquaintance with labelled trees". The symbol T_n in problem statements denotes the number of labelled trees with n vertices, and the question of finding this value is not stated. Problem numbering is given according to the topics of the next sections.

1.1. A graph is called *unicyclic* if it is connected and contains exactly one cycle. Prove that the number of labelled trees with 100 vertices is greater than the number of labelled unicyclic graphs with 98 vertices.

1.2. Construct a bijection between the set of all mappings from $[n]$ to itself and the set of labelled trees with n vertices containing one vertex marked with red stamp and one vertex marked with blue stamp (it may happens that both stamps mark the same vertex).

1.3. There exist n^{n-1} different mappings from the set $[n-1]$ to $[n]$. Prove the identity

$$\sum_{j=1}^{n} \binom{n-1}{j-1} (n-j)^{n-j} T_j = n^{n-1},$$

by partitioning the set of these mappings into n parts in such a way that j-th term in the sum be equal to the number of mappings in j-th part.

3.1. A tree with n vertices and edges enumerated by numbers from 1 to $n-1$, is called an *edge labelled* tree. For example, there exist 4 different edge labelled trees with 4 vertices — see fig. 1. Prove that for $n \geq 3$ the number of different edge labelled trees with n vertices is equal to $\frac{1}{n} T_n$.

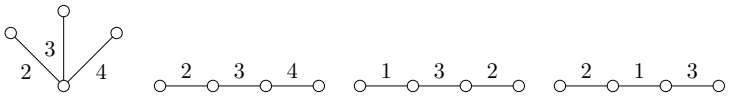


Figure 1. Edge labelled chicken's feet and paths of length 3

If we singled out one of the vertices in a tree (labelled or not) then we call such a tree *rooted* and the vertex that has been singled out is called a *root*. If we need to emphasize that none of the vertices is singled out then we call such a tree *free*. A *leaf* of a tree is a vertex of degree 1, except for the case when the tree is rooted and the root has degree 1, in this case the root is not considered as a leaf. A *forest* is a graph in which each connected component is a tree.

The set of forests on vertex set $[n]$ consisting of k rooted trees with roots $1, 2, \ldots, k$, such that vertex n is in the tree with root 1 is denoted by $\mathcal{F}_n^k$ (fig. 2).

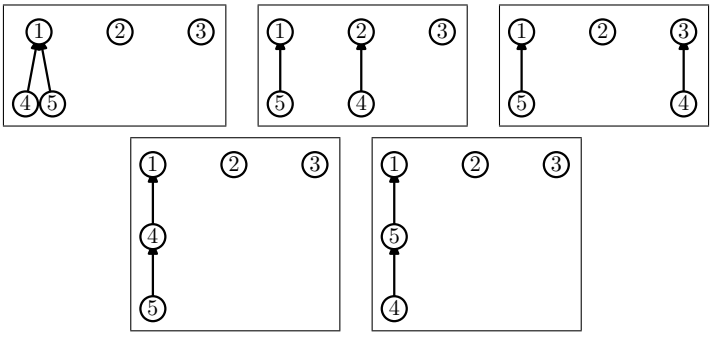


Figure 2. Set of forests $\mathcal{F}_5^3$. We orient each edge towards the root.

We denote sets by "handwritten" letters. Number of set elements is denoted by the same letter in italic font. For example, the number of elements of set $\mathcal{F}_n^k$ we denote by F_n^k.

1.4. Prove the recurrent relation for $2 \le k \le n-1$:

$$F_n^{k-1} = nF_n^k.$$

1.5. Let $V_1 = [r]$, $V_2 = \{r+1, \ldots, r+s\}$, $V = V_1 \cup V_2 = [r+s]$. Denote by $\mathcal{F}_{r,s}^k$ the set of forests consisting of k rooted trees on vertex set V with roots $1, 2, \ldots, k$, such that vertex $r+1$ is in the tree with root 1, and each edge connects vertex from V_1 with vertex from V_2. Find the recurrence relation (by k) for the numbers $F_{r,s}^k$.

There are n parking spaces available along a one-way street and each of n drivers numbered from 1 to n has a preferred parking space. The drivers arrive consecutively in increasing order of their numbers. Each driver goes to his preferred parking place and parks on that place if it's not occupied; otherwise he goes farther to first free space and parks there, if all the spaces are occupied he goes away forever. By a preference sequence we call a list $a_1, a_2, \ldots, a_n$ of preferred parking places of the first, second, $\ldots$, n-th driver.

4.1. Prove that the number of preference sequences in which everyone will find a parking space is $(n+1)^{n-1}$.

4.2. Prove that success or unsuccess of the parking process does not depend on the order in which the cars arrive.

The next problem is out of the mainstream of our project. But it gives a possibility to understand what troubles arise in counting of unlabelled trees.

3.2. Prove that the number of different (that is nonisomorphic to each other) unlabelled trees with n vertices is less than 4^n.

1 Recursions, identities, bijections

1.6. Prove by combinatorial reasoning (interpreting numbers T_i as numbers of trees), that for $n > 1$

a) $T_n = \frac{n}{2} \sum_{k=0}^{n-2} \binom{n-2}{k} T_{k+1} T_{n-k-1}$;

b) Reduce this formula and also the formulas from problems 1.3 and 5.1 a) to each other algebraically.

1.7. Denote by $\mathcal{T}(n,k)$ the set of labelled rooted trees with n vertices in which the root is labelled by 1 and has degree k. Prove that

$$(n-1)(k-1)T(n,k) = (n-k)T(n,k-1).$$

A "triangle tree" is a graph defined by induction in the following way. The smallest triangle tree is a complete graph with two vertices (in contrast with its name). If some triangle tree is already given we can take its arbitrary edge AB, take new vertex C and add vertex C and edges AC, BC to the tree. By a labelled triangle tree we call a triangle tree with vertices numbered from 1 to n.

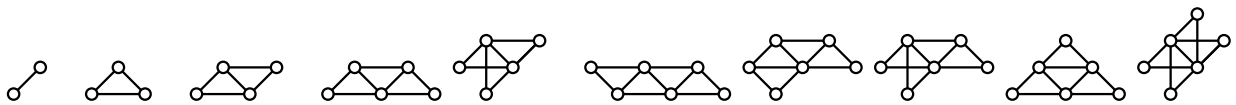


Figure 3. Unlabelled triangle trees on 2, 3, 4, 5 and 6 vertices

For example, for $n = 5$ there exist 2 unlabelled and 70 labelled triangle trees (fig. 3).
If some edge of a triangle tree is singled out then we call such tree "rooted".

1.8. Denote by $\Delta(n,k)$ the number of rooted labelled triangle trees with n vertices such that its rooted edge belongs to k triangles. Find recursion (by k) for the numbers $\Delta(n,k)$.

2 Prüfer code

Prüfer code corresponds a tree with numbered vertices to the sequence of its vertices in the following way. Prüfer code of a tree with two vertices is an empty word. If the number of vertices of a tree T is more than 2 then denote by v a leaf with smallest number, and by u the vertex adjacent to v. Then Prüfer code of tree T is obtained from Prüfer code of tree $T - v$ by appending the vertex u (to the left).

Check that you know how to solve problem 2.1 and come to jury to register your plus.

2.1. a) Find Prüfer code of tree with vertices 1, 2, ..., 10 and edges (8,9), (8,4), (4,10), (10,3), (3,5), (10,6), (10,1), (1,7), (1,2).

b) Reconstruct tree by the Prüfer code 1, 1, 2, 5, 4, 2, 7.

c) Prove that Prüfer code defines one-to-one correspondence between the set of trees on the given set of n vertices and the set of words of length $n-2$ with "letters" from this set.

d) Prove that a vertex of degree d occurs $d-1$ times in the Prüfer code.

2.2. What is the number of rooted labelled trees with n vertices in which vertex n is a leaf (and hence it is not root)?

2.3. What is the number of free labelled trees with $n > 10$ vertices in which the degree of vertex 1 is equal to 10?

2.4. Find the number of labelled unicyclic graphs with n vertices having a cycle of length k.

2.5. Denote by $S(n,k)$ Stirling number of the second kind, by definition it is equal to the number of ways to partition set $[n]$ into k nonempty parts. Prove that the number of labelled trees on n vertices with exactly r leafs is equal to $\frac{n!}{r!} S(n-2, n-r)$.

2.6. Denote by $\tau(k_1, k_2, \ldots, k_n)$ the number of free labelled trees with n vertices such that the degree of i-th vertex is $k_i + 1$. Prove that $\tau(k_1, k_2, \ldots, k_n) = \dfrac{(n-2)!}{k_1!k_2!\ldots k_n!}$.

3 Results

You can submit several solutions of the next problems if they are quite different.

3.3. Deduce Cayley's theorem from problems: a) 1.4, b) 1.6, c) 1.7, d) 2.6.

3.4. Prove that the number of forests with vertices from set $[n]$ consisting of k rooted trees is equal to $\binom{n-1}{k-1}n^{n-k}$.

3.5. Prove that the number of forests with vertices from set $[n]$ consisting of two free trees is equal to $\frac{1}{2}n^{n-4}(n-1)(n-6)$.

3.6. Prove that the number of spanning trees of complete bipartite labelled graph $K_{r,s}$ with parts $V_1 = [r]$ and $V_2 = \{r+1, \ldots, r+s\}$ is equal to $r^{s-1}s^{r-1}$.

3.7. Let Δ_n be the number of labelled triangle trees with n vertices, Λ_n be the number of rooted labelled triangle trees with n vertices and rooted edge 1–2.

a) Prove that $\Lambda_n = (2n-3)^{n-3}$.

b) Find Δ_n.

Let n different objects are arranged in the row. A *cyclic* permutation is a permutation that moves all the objects along some cycle: it puts the first object on the place of the second one, puts the second one on the place of the third one and so on, the last object is put on the place of the first one. A *transposition* (ij) is a permutation that changes objects on the i-th и j-th place. If we consider $[n]$ as set of vertices of some graph then the transposition (ij) can be interpreted as an edge connecting vertex i with vertex j.

The result of consecutive applying of permutations s_1, s_2, …, s_{n-1} is a permutation that is called a *product* of these permutations and is denoted by $s_1 s_2 \ldots s_{n-1}$. We consider the products that differ by the order of factors as different. For example, if permutation s is a transposition changing objects on the first and second places, permutation t is a transposition changing objects on the third and fourth places, then the products st and ts determine the same permutations but we consider them as different products.

3.8. a) n objects are arranged in the row. Prove that the result of consecutive applying of transpositions s_1, s_2, …, s_{n-1} is a cyclic permutation if and only if the graph with vertex set $[n]$ and edge set s_1, s_2, …, s_{n-1} is a tree.

b) Prove that the number of ways in which a cyclic permutation of set $[n]$ can be represented as a product of $n-1$ transpositions is T_n.

4 *Parking functions*

There are n parking spaces available along a one-way street and each of n drivers numbered from 1 to n has a preferred parking space. The drivers arrive consecutively in increasing order of their numbers. Each driver goes to his preferred parking place and parks on that place if it's not occupied; otherwise he goes farther to first free space and parks there, if all the spaces are occupied he goes away forever. A preference sequence for which everyone finds a parking space is called a *parking function*. The set of parking functions is denoted by $\mathcal{P}_n$.

4.3. Find the number of parking functions $(a_1, a_2, \ldots, a_n)$ such that any two consecutive drivers have different preferences that is $a_k \neq a_{k+1}$ for $k = 1, \ldots, n-1$?

4.4. Let only $m < n$ cars enter the street with n parking spaces. How many preference sequences exist such that all the drivers find a parking space?

4.5. Prove that the number of parking functions such that exactly k drivers $(1 \leq k \leq n)$ prefer to park in the first place is equal to $\binom{n-1}{k-1} n^{n-k}$.

4.6. For each parking function $a = (a_1, a_2, \ldots, a_n)$ define the sequence of differences $c(a) = (c_1, c_2, \ldots, c_{n-1})$ by the rule

$$c_i = a_{i+1} - a_i \pmod{n+1}.$$

Let the parking function a correspond to the labelled tree $t(a)$ with $n+1$ vertices that is given by Prüfer code $c(a)$.

Prove that this correspondence is a bijection between $\mathcal{P}_n$ and $\mathcal{T}_{n+1}$.

4.7. Prove that $(n+1)^{n-1} = \sum_{\substack{0 \leq k_n \leq 1 \\ 0 \leq k_{n-1}+k_n \leq 2 \\ 0 \leq k_{n-2}+k_{n-1}+k_n \leq 3 \\ \cdots \\ 0 \leq k_2+k_3+\ldots+k_{n-1}+k_n \leq n-1}} \frac{n!}{(n-k_2-k_3-\ldots-k_n)!k_2!k_3!\ldots k_n!}$.

4.8. We call a parking function $a = (a_1, \ldots, a_n)$ *sure* if at least $j+1$ drivers prefer park in the first j places for all j, $1 \leq j \leq n-1$. Prove that the number of sure parking functions in the street with n parking spaces is equal to $(n-1)^{n-1}$.

4.9. Prove by combinatorial arguments the recurrent relation: $P_{n+1} = \sum_{k=0}^{n} \binom{n+1}{k} P_k (n-k)^{n-k}$.

5 *Inversions on trees and deficiencies of parking functions*

5.1. Prove the recurrent relation by combinatorial arguments:

a) $T_n = \sum_{k=0}^{n-2} \binom{n-2}{k} (k+1) T_{k+1} T_{n-k-1}$; b) $P_{n+1} = \sum_{k=0}^{n} \binom{n}{k} (k+1) P_k P_{n-k}$;

Consider a labelled tree T with $n+1$ vertices. Assign vertex $n+1$ to be a root and define directions on the tree edges towards the root. We "accept as correct" that the vertex labels increase when we move towards the root. We say that vertices i and j form *inversion*, $1 \le i < j \le n$, if vertex i lies on the path from vertex j to the root. Check all pairs of vertices and denote by $\mathrm{inv}(T)$ the total number of inversions in tree T. A maximum value of $\mathrm{inv}(T)$ is equal to $\frac{n(n-1)}{2}$, it is achieved when T is a path of n edges whose vertices are labelled as $n+1$, $1, 2, \ldots, n$.

Let $a = (a_1, a_2, \ldots, a_n)$ be a parking function. Let first driver parked in p_1-th place, the second driver parked in p_2-th place etc. We call the value

$$D(a) = \sum_{i=1}^{n} (p_i - a_i) = \frac{n(n-1)}{2} - \sum_{i=1}^{n} a_i.$$

the *deficiency* of parking function a. Function $(1, 1, \ldots, 1)$ has the largest possible deficiency, it is equal to $\frac{n(n-1)}{2}$.

Theorem. Let n be arbitrary natural number. Then for all k, $0 \le k \le \frac{n(n-1)}{2}$, the number of rooted labelled trees on $n+1$ vertices with root $n+1$ having k inversions is equal to the number of parking functions with deficiency k in the street with n parking spaces.

Introduce polynomials $F_n(x)$ and $H_n(x)$ that "number" inversions and deficiencies:

$$F_0(x) = 1, \quad F_n(x) = \sum_{T \in \mathcal{T}_{n+1}} x^{\mathrm{inv}(T)}; \qquad H_0(x) = 1, \quad H_n(x) = \sum_{a \in \mathcal{P}_n} x^{D(a)},$$

We call them *inversion enumerator* и *deficiency enumerator*.

5.2. Let $\mathcal{T}^*$ be the set of labelled rooted trees with $n+3$ vertices such that its root has degree 2 and is labelled by $n+3$, and two sons of the root are labelled by $n+1$ and $n+2$. Express the inversion enumerator of the set $\mathcal{T}^*$

$$F_n^*(x) = \sum_{T \in \mathcal{T}^*} x^{\mathrm{inv}(T)}$$

in terms of the polynomials $F_i(x)$.

5.3. Prove that polynomials $F_n(x)$ and $H_n(x)$ satisfy the same recurrent relations for $n \ge 0$

$$F_{n+1}(x) = \sum_{k=0}^{n} \binom{n}{k} (x^k + x^{k-1} + \ldots + 1) F_k(x) F_{n-k}(x). \tag{a}$$

$$H_{n+1}(x) = \sum_{k=0}^{n} \binom{n}{k} (x^k + x^{k-1} + \ldots + 1) H_k(x) H_{n-k}(x). \tag{b}$$

The eheorem about inversions and deficiencies immediately follows from two previous problems. Though you might suggest a bijective proof.

5.4. Prove the theorem about inversions and dificiencies by constructing one-to-one correspondence between the sets $\mathcal{T}_{n+1}$ and $\mathcal{P}_n$ such that a parking function with dificiency j corresponds to the tree with j inversions.

6 *Additional tasks*

By a *labelled plane tree* we call a rooted labelled tree such that the sons of any of its vertex are lineary ordered. Denote by $\mathcal{P}_n^k$ the set of forests consisting of k labelled plane trees on the set $[n]$ with roots 1, 2, ..., k such that vertex number n is in the tree with root 1.

1.9. Prove that the recurrent relation holds for $2 \le k \le n-1$

$$P_n^{k-1} = (2n-k)P_n^k.$$

3.9. Prove that the number of spanning trees in the complete bipartite labelled graph $K_{r,s}$ containing $k+\ell$ trees rooted in vertices 1, 2, ..., k and $r+1, r+2, \ldots, r+\ell$ is equal to

$$(r\ell + sk - k\ell)r^{s-\ell-1}s^{r-k-1}.$$

3.10. Prove that the number of spanning trees in complete tripartite labelled graph $K_{r,s,t}$ with parts $V_1 = [r]$, $V_2 = \{r+1, \ldots, r+s\}$ and $V_3 = \{r+s+1, \ldots, r+s+t\}$ is equal to

$$(r+s+t)(r+s)^{t-1}(s+t)^{r-1}(t+r)^{s-1}.$$

3.11. What is the number of plane labelled rooted trees with $n+1$ vertices?

A tetrahedral tree is defined by induction similarly as a triangle one. The simplest tetrahedral tree (degenerate) is a triangle (complete graph with three vertices), the next simplest is a tetrahedron (complete graph with four vertices). If some tetrahedral tree is already given then we may add a new vertex by taking any triangle face in any of tetrahedrons and constructing a new tetrahedron with the new vertex using the chosen face as a base. Formally it means that we add to the graph one new vertex and three new edges (and three new triangle faces, if you wish). Note that the tetrahedrons may intersect in the three-dimensional space as well as triangles of a triangle tree may intersect in the plane.

3.12. How many labelled tetrahedral trees with n vertices exist?

4.10. Prove that $(n-1)^{n-1} = \sum_{\substack{0\le k_{n-1}\le 1\\ 0\le k_{n-2}+k_{n-1}\le 2\\ 0\le k_{n-3}+k_{n-2}+k_{n-1}\le 3\\ \ldots\\ 0\le k_2+k_3+\ldots+k_{n-2}+k_{n-1}\le n-2}} \frac{n!}{(n-k_2-k_3-\ldots-k_{n-1})!k_2!k_3!\ldots k_{n-1}!}.$

4.11. Prove that $n^n = \sum_{\substack{0\le k_1\le 1\\ 0\le k_1+k_2\le 2\\ 0\le k_1+k_2+k_3\le 3\\ \ldots\\ 0\le k_1+k_2+\ldots+k_{n-1}\le n-1}} \frac{n!}{k_1!k_2!\ldots k_{n-1}!}.$

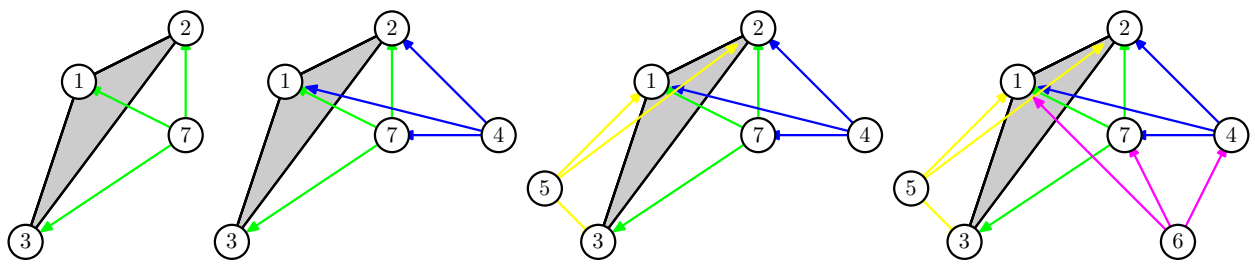


Figure 4. Construction of a tetrahedral tree. We add cosequently vertices 7, 4, 5, 6 to the initital triangle (1, 2, 3)

Solutions

1 Recursions, identities, bijections

1.1. We took this problem from [3]. Let A be a vertex with the largest label on the cycle, and B be one of the two adjacent vertices that has larger label. Remove edge AB from the tree, hang a leaf with label 99 to vertex A and a leaf with label 100 to vertex B. We constructed injective mapping from the set of unicyclic graphs to the set of trees.

1.2. See [6, problem 8.5] or the first proof in [1, chapter 26]. Consider the path from the blue vertex to the red one. Let $A \subset [n]$ be the set of labels of this path. Our tree consists of this path and several trees that grow on the vertices of this path. The sequence of labels along the path can be interpreted as a permutation of elements of set A. Draw this permutation as a set of cycles (with vertices on the elements of set A). We obtain a set of cycles, and several trees that grow on its vertices.

From the other hand, mapping from set $[n]$ to itself is given by the directed graph: for each i draw an arrow from vertex i to vertex $f(i)$ (loops are allowed). Since all the vertices of this graph have outgoing degree 1, the graph is a union of several cycles and several trees that grow on the vertices of these cycles (speaking more carefully the trees "pour in" the vertices of the cycles).

This is the required bijection.

1.3. We took this statement from [17, p. 3.9]. The rigth hand side of the equality counts all possible mappings from $[n-1]$ to $[n]$. Any such mapping f can be drawn as a directed graph with n vertices: each vertex i is a starting point of an arrow that goes to $f(i)$. Vertex n can have ingoing edges only, and the connected component of vertex n is a tree in which all the arrows directed "towards n". The left hand side of the equality counts such graphs classifying them by the trees containing vertex n.

1.4. [14, theorem 2.1]. The root of a tree determines a direction from the root to the periphery. Construct a mapping from set $\mathcal{F}_n^{k-1}$ to $\mathcal{F}_n^k$. For this we take an arbitrary forest with $k-1$ trees, find vertex k in it, cut off this vertex together with the branch that grows on it, and put it as a separate rooted tree. Ususally the result is a tree from $\mathcal{F}_n^k$ except the case when we cut off the branch from first tree and this branch contains vertex n. In this case we do a correction: exchange labels 1 and k.

Now count how many preimages for this mapping has an arbitrary forest from $\mathcal{F}_n^k$. In order to construct a preimage of a forest, we have to take its k-th tree and attach it as a branch to an arbitrary vertex of the first, second, ..., $(k-1)$-th tree of the forest. This construction imply that there was no correction. And for preimages with correction, we have to attach the first tree as a branch to an arbitrary vertex of k-th tree and then exchange labels 1 and k. Thus, each of n vertices of the graph can be used for construction of a unique preimage. Hence, $F_n^{k-1} = nF_n^k$.

1.5. Answer: $F_{r,s}^{k-1} = sF_{r,s}^k$ for $2 \le k \le r$. [14, Corollary 3.1]. Recursion can be constructed as in problem 1.4. Since the vertex k must belong to set V_1, in inverese mapping the subtree with root k can be attached to any of s vertices of set V_2.

1.6. a) This result is from [18]. Denote by E_n the number of labelled trees with vertices on $[n]$ containing one specified edge, for example, edge 1–2. Counting all the edges in all the trees we obtain an identity

$$\frac{n(n-1)}{2} E_n = (n-1)T_n.$$

Thus, $T_n = \frac{1}{2} n E_n$. Now to find E_n we have to choose how many vertices do the tree hanging on vertex 1 and the tree hanging on vertex 2 contain, and choose trees with these numbers of vertices. We obtain formula $T_n = \frac{n}{2} \sum\limits_{k=0}^{n-2} \binom{n-2}{k} T_{k+1} T_{n-k-1}$.

b) The equality in this problem can be derived from the equality of problem 5.1 a) by a "Gauss method": sum up two copies of the sum in the problem 5.1 a), change index of the summation k with $n-2-k$ and sum up these sums term by term.

Now derive the identity of problem 1.3 from the identity 5.1 a). For this write separately the summand for $j=n$, and change the summation index in the remaining sum by the rule $j=k+1$:

$$n^{n-2}+\sum_{k=0}^{n-2}\binom{n-1}{k}(k+1)^{k+1}(n-k-1)^{n-k-1}=n^{n-1}.$$

Subtract n^{n-2} from both sides and apply the formula $\binom{n-1}{k}(n-k-1)=(n-1)\binom{n-2}{k}$ in the left hand side:

$$\sum_{k=0}^{n-2}(n-1)\binom{n-2}{k}(n-k-1)(k+1)^{k+1}(n-k-1)^{n-k-3}=n^{n-2}(n-1).$$

By cancelling $(n-1)$ we obtain the formula from the problem 5.1 a) up to a change of the summation index.

1.7. [4] Let $A\in\mathcal{T}(n,k-1)$ be one of the trees, v be any of its $n-k$ vertices adjacent to vertex 1. Replace the edge connecting vertex v to its ancestor with the edge connecting this vertex and the root. Denote the obtained tree by B (obviously $B\in\mathcal{T}(n,k)$), we will call a pair of trees (A,B) a *bundle*.

Count the number of bundles by two different ways. From the one hand, the number of bundles is equal to $(n-k)T(n,k-1)$, because the bundle is uniquely determined by the tree A with vertex v. The tree can be chosen in $T(n,k-1)$ ways, then the vertex v can be choosen in $(n-k)$ ways. From the other hand, the bundle may be obtained in the following way: choose a tree B in $T(n,k)$ ways, remove one edge outgoing from the root, and connect the "broken branch" obtained with any of non root vertices of the remaining tree. In total we obtain

$$(n-1-n_1)+(n-1-n_2)+\ldots+(n-1-n_k)=(n-1)(k-1)$$

ways where n_i is the number of vertices in the "broken branch" formed after removal of the i-th edge outgoing from the root. So we have $(n-1)(k-1)T(n,k)$ cases. Thus, $(n-1)(k-1)T(n,k)=(n-k)T(n,k-1)$.

1.8. Answer: $(n-k-2)\Delta(n,k)=k(2n-4)\Delta(n,k+1)$. This statement is from [9].

Note that the construction in the definition of a triangle tree can start from any edge: take any edge, add the triangles that contain this edge, then add triangles that contain any of the already constructed edges and so on. Furthermore, let the first edge be fixed, and during the appending to the tree the next vertex C, we draw arrows on the edges CA, CB outgoing from vertex C. Then the directed graph that represents the triangle tree does not depend on the order in which the vertices had been added!

Consider a triangle tree G in which the rooted edge uv belongs to k triangles, denote them by uvw_1, uvw_2, …, uvw_k, and construct a tree with $k+1$ triangles by the following construction (fig. 5). Take an arbitrary vertex w, coinsiding with no one of the vertices w_i, and consider a minimal triangle subtree containing vertices u, v and w. Vertex w has two outgoing edges in this subtree since it is minimal one. Remove these edges and draw edges wu and wv instead of them. As a result of this operation we obtain a rooted tree that has one more triangle. The parts of tree G that were hunging on the removed edges, hang now on the new edges wu and wv. (It may happens that during these actions we remove the edge connecting w with u or v, and immediately restroe it.) Vertex w may be chosen in $n-k-2$ ways, so we have $(n-k-2)\Delta(n,k)$ ways of implementing this construction.

Now describe the inverse operation: given a tree in which the rooted edge uv belongs to $k+1$ triangles, construct a tree in which the rooted edge uv belongs to k triangles. Take one of the $k+1$ triangle vertices connected to the root, let it be vertex w, and "displant" (move) triangle

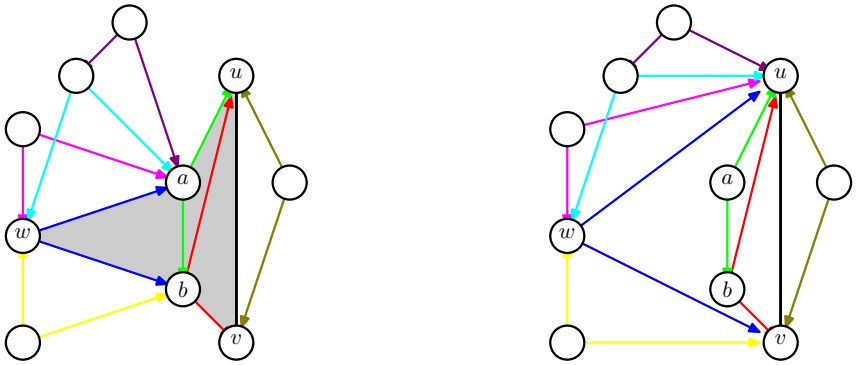


Figure 5. A tree with k triangles on the rooted edge uv (left figure) and a tree with $k+1$ triangles ($k=1$) (right figure). The minimal tree containing vertices w, u and v is colored gray. Two arrows go from each vertex except u and v to the endpoints of the edge on which the triangle corresponding to the vertex had been hunged

uvw from the edge uv to another edge, say, ab. It can be done in the following way: let G_1 and G_2 be triangle trees growing on the edges wu and wv. Choose an arbitrary edge ab, not belonging to $G_1 \cup G_2$ (and not coinsiding with uv), and replace edges wu and wv with edges wa and wb. The subtrees G_1 and G_2, hanging on edges wu and wv, we displant on the edges wa and wb correspondingly.

Count in how many ways this construction can be implemented. Any of $2n-4$ non root edges can be assigned as ab. If edge ab belongs to the triangle subtree, hanging on the rooted triangle uvw', then we can take any of k rooted triangles uvw, where $w \neq w'$, as triangle uvw, which we hang on this edge. In total, $k(2n-4)\Delta(n,k+1)$ ways.

1.9. [14, corollary 4.1]. Try to construct a recursion similar to that of in problem 1.4. In this problem we have more places where the subtree with root k may be hanged. For each vertex the number of places is equal to the number of its descendants plus one. In total for all vertices we obtain the number of all edges plus the number of all vertices. And the number of edges in forest with k trees is equal to $n-k$.

2 *Prüfer code*

2.1. This is problem 2.2.4 from [3], it is just an exercise for understanding what is a Prüfer code.

2.2. Answer: $(n-1)^{n-1}$.

Prüfer code of unrooted tree in which vertex n is a leaf does not contain symbol "n". Hence there are $(n-1)^{n-2}$ such codes. The choise of the root increases the number of cases in $(n-1)$ times.

2.3. Answer: $\binom{n-2}{9}(n-1)^{n-11}$. Since this number is equal to the number of fillings of n cells by $n-2$ different objects for which the first cell contains 9 objects.

2.4. Answer: $\frac{1}{2}(n-1)(n-2)\dots(n-k+1)n^{n-k}$.

The number of ways to choose a cycle is equal to $\frac{n(n-1)(n-2)\dots(n-k+1)}{2k}$: we choose the first vertex of cycle, the second one and so on consequently, after that we take into account that it is not important which vertex of the cycle is the first and what is the cycle direction. It remains to count the number of unicyclic graphs containing cycle $(n, n-1, \dots, n-k+1)$. Remove the edge connecting n and $n-k+1$. The number of possible Prüfer codes for obtained tree is equal to kn^{n-1-k}. Indeed, after $n-k$ steps of Prüfer encoding the remaining part of the tree is exactly the path n, $n-1$, …, $n-k+1$. Then the first $n-k-1$ elements of Prüfer code can be assigned arbitrarily, $(n-k)$-th element is the number from $n-k+1$ to n, and all other elements are determined.

We took this problem from [3].

2.5. We took this problem from [5]. Attentive reader can also find it in [7]. Due to Prüfer code, it seems to be almost a tavtology.

2.6. [7]. Prüfer's algorithm maps labeled trees to monomials $x_{i_1}x_{i_2}\dots x_{i_{n-2}}$, which can be "reduced" to the form $x_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ (where $k_1+k_2+\dots+k_n=n-2$). Thus the number of different codes is equal to the polynomial coefficient $\frac{(n-2)!}{k_1!k_2!\dots k_n!}$.

3 Results

3.1. We took this statement in [17]. For each labeled tree assign vertex n to be a root, then the direction to the root is defined on each edge and the relation "ancestor–descendant' ' is given. Now to each labeled tree with n vertices we put into correspondence an edge-labeled tree with n vertices. For this we put the label i on each edge ij , where i is a descendant of j.

The obtained edge labeled tree allows us to recover the initial vertex labelling if we indicate which vertex was a root and label it by n. Hence each edge labeled tree could be obtained in our mapping from n different labeled trees.

3.2. We took this problem in [3]. Let us count the number of rooted trees. Draw a tree on the plane and draw an arrow on each edge towards the periphery. Now put a code into correspondence to the tree: starting from the root move along the tree as if it is a system of walls on the plane. If we move along the arrow write 1, if against write 0. We obtain a sequence of $2n-2$ zeroes and ones. It is clear that each sequence determines at most one tree.

3.3. a) Cayleys theorem follows from problem 1.4 and the equality $F_n^{n-1} = 1$.

c) Cayley's theorem follows from problem 1.7 and the equality $T(n,k) = \binom{n-2}{k-1}(n-1)^{n-k-1}$. Indeed, the number of labeled trees is equal to the sum

$$\sum_{k=1}^{n-1} T(n,k) = \sum_{k=1}^{n-1} \binom{n-2}{k-1}(n-1)^{n-k-1} = \sum_{k=0}^{n-2} \binom{n-2}{k}(n-1)^{n-2-k} = ((n-1)+1)^{n-2}.$$

b) In [18] Cayley's theorem is drived from problem 1.6 by means of generation functions and Lagrange inverse formula, but may be elementary method exist.

d) Cayley's theorem is drived from problem 2.6 by the summation like in the polynomial theorem

$$\sum_{\substack{k_1+k_2+\ldots+k_n=n-2 \\ k_i \geq 0}} \frac{(n-2)!}{k_1!k_2!\ldots k_n!} = n^{n-2}.$$

3.4. See [14, corollary 2.3].

3.5. We took this problem in [17, п. 4.3].

3.6. See [14, corollary 3.1]. We can prove the statement by means of Prüfer code. At the end of the Prüfer encoding we obtain two vertices from different parts of the graph. Therefore the code contains $r-1$ labels from the first part and $s-1$ labels from the second part and the total numbers of codes equals $r^{s-1}s^{r-1}$.

3.7. a) Solution 1. The statement is taken from [9] where it is proven by five different ways. We present the third proof in [9].

Applying the recursion from solution 1.8 and the "initial condition" $\Delta(n,k) = 1$ for $k = n-2$, we obtain

$$\Delta(n,k) = (2n-4)\frac{k}{n-2-k}\Delta(n,k+1) = (2n-4)^2\frac{k(k+1)}{(n-2-k)(n-2-(k+1))}\Delta(n,k+2) =$$
$$= \ldots = (2n-4)^{n-2-k}\frac{k(k+1)\ldots(n-3)}{(n-2-k)(n-2-(k+1))\cdots 1}\Delta(n,n-2) =$$
$$= (2n-4)^{n-2-k}\frac{(n-3)!}{(k-1)!(n-3-(k-1))!}\Delta(n,n-2) = (2n-4)^{n-2-k}\binom{n-3}{k-1}.$$

By summing over all possible k and applying the binomial expansion we compute the number of rooted triangle trees: $\sum\limits_{k=1}^{n-2}\binom{n-3}{k-1}(2n-4)^{n-k-2} = (2n-3)^{n-3}$.

Solution 2 (Prüfer code). We encode a labelled rooted triangle tree by a code similar to Prüfer code.

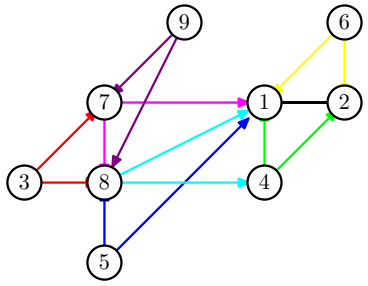


Figure 6. Example of the construction of code for the triangle tree (7b)(12)(8a)(7b)(8a)(4a).

Construction of the code by a tree. Let a triangle labelled rooted tree with rooted edge 1–2 be given. At first, given labelling of the vertices, define a special labelling of edges. Draw arrows on the edges by the same way as in solution of problem 3.7. Then each vertex has two outgoing arrows (except the vertices of the root edge). If a vertex has label x, then label its outgoing edges as xa and xb, where the endpoint of the edge xa has smaller label than the endpoint of the edge xb. Denote the root edge by 1–2. Thus, our tree contains $2n-3$ edges with "unified" names:

$$12,\ 3a,\ 3b,\ 4a,\ 4b,\ \ldots,\ na,\ nb.$$

We write the code using new names of edges. Vertices of degree 2 we call leaves. In each step we choose the leaf of the current triangle tree with maximal label, remove the chosen vertex and write the name of its ancestor edge. In the last step the last vertex is connected with endpoints of root edge 1–2, and we skip writing.

Recovering the tree by a code.

All the vertices x for which both edges xa and xb do not belong to the code are leaves. (The vertices 1 and 2 are not the leaves by definition.) So looking at the code we can write the List of leaves. In this list the vertex z with the largest label has been removed the first. Therefore the first symbol in the code is the name of the edge-ancestor of z. Write the vertex z and its edge-ancestor to the second list, call it the "List of triangles", remove the first symbol from the code, remove z from the List of leaves. Look at the (shortened) code once again, seek a new vertices that become leaves and update the List of leaves. Now take the vertex with the largest label and the first symbol in the code and so on.

At the end of this algorithm we obtain the List of triangles containing the sequence of vertices with their edge-ancestors. Unlike the usual trees it is not easy to recover the triangle tree by reading List of triangles from the beginning because the unified name of an edge (xa or xb) "hides" the labels of its endpoints. But if we start to read the List of triangles from the tail, it can be done easily. Draw the root edge 1–2. And start the construction of the tree like in its defintion. Vertex which is not contained in List of triangles should be appended to the tree the first. In the next step the vertex y has the edge-ancestor with the name of the form xa or xb, and since this edge has been already drawn, we know the labels of both its endpoints.

Why does the list always contain at least one leaf? The current code has $n-3-k$ positions where k is the number of already considered positions. And the number of vertices that could be a leaves is equal to $n-2-k$ (we subtract 2 because the vertices 1 and 2 are not leaves), that is greater by 1.

The code contains $n-3$ positions, the tree contains $2n-3$ edges. Each edge can be written in any position, so the number of codes is equal to $(2n-3)^{n-3}$. Since eaxctly one tree corresponds to each code, and any tree determines a code, the number of rooted triangle trees coinsides with the number of codes.

Example. Let $n=8$ and the code is (7b, 1–2, 8a, 7b, 8a, 4a).

Number of step	Current code	List of leaves	List of triangles
1	(7b, 1–2, 8a, 7b, 8a, 4a)	3, 5, 6, 9	9, 7a
2	(1–2, 8a, 7b, 8a, 4a)	3, 5, 6	6, 1–2
3	(8a, 7b, 8a, 4a)	3, 5	5, 8a
4	(7b, 8a, 4a)	3	3, 7b
5	(8a, 4a)	7	7, 8a
6	(4a)	8	8, 4a

List of triangles does not contain vertex 4, it implies that this vertex has been hung to the edge 1–2 at the first step. So we draw the triangle with vertices 1, 2, 4. Then vertices 8, 7, 3, 5, 6, 9 have been hung to the edges 4a, 8a, 7b, 8a, 1–2, 7b correspondingly. Hang vertex 8 to the edge 4a (i. e. to the edge 2–4) and so on. The obtained triangle tree is depicted in fig. 6.

b) Since the root edge of a triangle tree may be labelled by any pair of labels, not only 1–2, and any of $2n-3$ edges in triangle tree may be chosen as the root, the relation holds

$$\binom{n}{2}\Lambda_n = (2n-3)\Delta_n.$$

3.8. This statement of J. Dénes is proven in [11] (lemma 3.15 and theorem 3.16).

3.9. Answer: $kn^{n-k-1}(n-2)(n-3)\dots(n-k)$.

Similarly to problem 2.4. We can choose a path from the first vertex to the second in $(n-2)(n-3)\dots(n-k)$ ways. The number of Prfer codes for trees that contain this path equals kn^{n-k-1}. We took this problem in [5, problem 5.93].

3.10. We took this problem in [17, p. 3.5].

3.11. [14, Corollary 3.3]. Let $V_1=[r]$, $V_2=\{r+1,\dots,r+s\}$, $V_3=\{r+s+1,\dots,r+s+t\}$ and $V=V_1\cup V_2\cup V_3$. Denote by $F^k_{r,s,t}$ the number of rooted tripartite forests on the vertex set V consisting of k trees with roots 1, 2, …, k in which the vertex number $r+1$ is a descendant of vertex 1, and by $\bar F^k_{r,s,t}$ the number of rooted tripartite forests on the vertex set V with roots 2, 3, …, $k+1$ in whcih the vertex number 1 is a descendant of vertex $r+1$. We are interested in the number of trees, i. e. $F^1_{r,s,t}$.

$$F^1_{r,s,t} \underset{(2)}{=} (s+t)^{r-1}F^r_{r,s,t} \underset{(3)}{=} (s+t)^{r-1}\bar F^r_{r,s,t} \underset{(4)}{=}$$
$$\underset{(4)}{=} (s+t)^{r-1}(r+t)^{s-1}\bar F^{r+s-1}_{r,s,t} \underset{(5)}{=} (s+t)^{r-1}(r+s+t)(r+s)^{t-1}.$$

(2) similarly to problem 1.5 for $2\le k\le r$ we obtain the recurrent formula

$$F^{k-1}_{r,s,t} = (s+t)F^k_{r,s,t}$$

and applying this formula several times we turn to the forest with r trees;

(3) apply the equality $F^r_{r,s,t}=\bar F^r_{r,s,t}$ (forests in these sets differ only by the choise of the root for the tree containing vertex 1);

(4) for $r+1\le k\le r+s-1$ we obtain the recurrent formula

$$\bar F^{k-1}_{r,s,t} = (r+t)\bar F^k_{r,s,t}$$

and again similarly to problem 1.5 turn to the forest with $r+s-1$ trees; The transition from forests with roots 1, 2, ..., r to forests with roots 2, 3, ..., $r+1$ is caused by the condition that in this recurrent equality the vertex number k has to belong to second part.

(5) the number of forests with large number of trees can be easily computed:

$$\bar{F}^{r+s-1}_{r,s,t} = (r+s)^t + t(r+s)^{t-1},$$

in the first summand the vertex 1 is a son of vertex $r+1$, and the remaining t vertices of the third part can be connected with any of $r+s$ vertices of the two other parts; in the second summand the vertex 1 is a son of some vertex from the third part, and the remaining $t-1$ vertices similarly connected with any of $r+s$ vertices.

3.12. Answer: $(2n)!/n!$. Thus the number of plane labelled unrooted trees with $n+1$ vertices is equal to $\frac{1}{n+1}\binom{2n}{n}$. [14, Corollary 4.2].

3.13. Answer: $\binom{n}{3}(3n-8)^{n-5}$ из [17].

a) The number of rooted tetrahedral trees may be counted by encoding similarly to the number of rooted triangle trees.

Construction of the code by a tree. Choose the rooted triangle of the tree, for example, triangle $(1,2,3)$. The elements of code sequence are triangles (faces of tetrahedrons). Let vertex x be hanged to the face with vertex labels a, b and c, where $a<b<c$, we call this face ancestor of vertex x. Denote the face (x,a,b) by $x\alpha$, (x,a,c) by $x\beta$, (x,b,c) by $x\gamma$. Therefore, the faces of all tetrahedrons are denoted $x\alpha$, $x\beta$, $x\gamma$, where $x=4,\ldots,n$, and the root face we denote by $(1,2,3)$. The tree has $3n-8$ faces. Any vertex of degree 3 we call a leaf of a tetrahedral tree. In each step we remove the leaf with the largest labelr and write its face-ancestor. When the last tetrahedron remains (4 vertices), we stop.

Construction of the tree by a code. Leaves are vertices of the tetrahedral tree with those labels $x\in\{4,\ldots,n\}$, for which the current code does not contain no one of the faces $x\alpha$, $x\beta$, $x\gamma$.

Example. Let $n=7$ and the code is $(4\beta,\ (1,2,3),\ 7\alpha)$.

Number of step	Current code	List of leaves	Hanged vertex
1	$(4\beta,\ (1,2,3),\ 7\alpha)$	6, 5	6
2	$((1,2,3),\ 7\alpha)$	5, 4	5
3	(7α)	4	4
4	$()$	7	7

We read the list of hanged vertices in the reverse order and obtain that vertex 7 had been hung to the face $(1,2,3)$, vertex 4 had been hung to the face $7\alpha=(7,1,2)$, vertex 5 to the face $(1,2,3)$, vertex 6 to the face $4\beta=(4,1,7)$ consequently.

The obtained tetrahedral tree is depicted in fig. 4.

Since the code contains $n-4$ faces, we have in total $(3n-8)^{n-4}$ possible codes.

b) Since the root tringle of a tetrahedral tree can be labelled by any triple of labels, not only 1, 2, 3, and each of $3n-8$ triangles in a tetrahedral tree can be assigned as the root, the relation holds:

$$\binom{n}{3}\Lambda_n = (3n-8)\Delta_n.$$

4 *Parking functions*

4.1. This famous problem has been posed in [15].

Enlarge the parking lot by appending the $(n+1)$-th parking place, and enclose the street in a cycle so that it leads from the $(n+1)$-th place to the first one. For the enlarged street we have exactly $(n+1)^n$ preference sequences (each of the n drivers independently prefers one of the $n+1$ places). Now, for any preferences all the n drivers park successfully, and one parking place remains free. The preference sequence satisfies the requirements of the initial problem if and only if the $(n+1)$-th place is remained free. Indeed, the fact that the $(n+1)$-th place remains free means that no one prefers it and no one drives by it seeking the free place for parking (in the opposite case he had to park there and not to drive by). Therefore, in this case we can remove the $(n+1)$-th parking place with the adjacent part of the road (i. e. return to initial problem), without breaking the process of parking.

Partition all preference sequences for the cyclic parking lot into $(n+1)^{n-1}$ groups consisting of $n+1$ sequences each: along with sequence $(a_1, \ldots, a_n)$ we group all its cyclic shifts, i. e. $(a_1+1, \ldots, a_n+1)$, $(a_1+2, \ldots, a_n+2)$, $\ldots$, $(a_1+n, \ldots, a_n+n)$ (sums are taken modulo $n+1$). Observe that each group contains exactly one preference sequence satisfying the requirement of the initial problem, namely the sequence for which the $(n+1)$-th parking lot remains free.

Thus, the number of preferennce sequences is equal to the number of groups, i. e. $(n+1)^{n-1}$.

4.2. It is more or less evident what happens when two consequitive cars change their order.

4.3. Answer: n^{n-1}.

Similarly to the problem 4.1, we obtain that for the extended parking street the number of all possible preference sequences is equal to $(n+1)n^{n-1}$, because the first driver can have $n+1$ favourite places, and each next driver can have n favourite places. As in problem 4.1, each group of $n+1$ sequences that differ by a cyclic shift, contains one parking function only. We took this problem from book [12].

4.4. Answer: $(n+1-m)(n+1)^{m-1}$ sequences.

Solution from book [2, problem 96.54].

For every integer m, $0 \le m \le n$, denote by $N(n,m)$ the number of preference sequences for m drivers which lead to successful parking (in particular, $N(n,0) = 1$). We prove by induction on n that $N(n,m) = (n+1-m)(n+1)^{m-1}$ for all m. For $n = 1$ the statement is trivial.

Induction step $(n-1) \to n$. Let k drivers like parking places greater than 1 and $m-k$ drivers like the first place $(0 \le k \le m)$. Those k drivers may be chosen in C_m^k ways. It is easily seen that, given the preferences, success or unsuccess of parking does not depend on the order the drivers arrive. So we can assume that the $m-k$ drivers that like the first place arrive the latest. Those $m-k$ drivers can park for sure — they occupy the first $m-k$ free places remainig after parking of the first k drivers. Thus, success or unsuccess of the parking process depends only on the preferences of the first k drivers (on $n-1$ places). Therefore, after we have chosen those k drivers there exist exactly $N(n-1,k)$ successful preference sequences. Thus,

$$N(n,k) = \sum_{k=0}^{m} \binom{m}{k} \cdot N(n-1,k)\,. \tag{1}$$

Apply the hypothesis of induction and transform:

$$N(n,k) = \sum_{k=0}^{m} \binom{m}{k}(n-k)n^{k-1} = \sum_{k=0}^{m} \binom{m}{k} n^k - \sum_{k=1}^{m} k\binom{m}{k} n^{k-1} = \sum_{k=0}^{m} \binom{m}{k} n^k - \sum_{k=1}^{m} m\binom{m-1}{k-1} n^{k-1} =$$

$$= \sum_{k=0}^{m} \binom{m}{k} n^k - m \cdot \sum_{k=0}^{m-1} \binom{m-1}{k} n^k = (n+1)^m - m \cdot (n+1)^{m-1} = (n+1-m) \cdot (n+1)^{m-1}\,,$$

as desired. We use here the trivial formula $k \cdot \binom{m}{k} = m \cdot \binom{m-1}{k-1}$ and the binomial formulan for expansions of $(n+1)^m$ and $(n+1)^{m-1}$ in powers of n.

4.5. Let b_1, b_2, ..., b_n be the preference sequence written in nondecreasing order. Then $b_1 = b_2 = \ldots = b_k = 1$, $2 \le b_{k+1} \le b_{k+2} \le \ldots$. Note that preference sequence b_{k+1}, b_{k+2}, ..., b_n allows $n-k$ drivers park in the street with $n-1$ parking places (from 2-nd to n-th). The number of such sequences is computed in the previous problem and is equal to $k \cdot n^{n-k-1}$. The number of ways to choose k drivers that prefer to park at the first place is equal to $\binom{n}{k}$. Therefore, the total number of parking functions for which k drivers want to park in the first place is equal to $\binom{n}{k} \cdot k \cdot n^{n-k-1} = \binom{n-1}{k-1} n^{n-k}$.

"In order to check" this result, sum up the obtained expressions over k:

$$\sum_{k=1}^{n} \binom{n-1}{k-1} n^{n-k} = (n+1)^{n-1}$$

(binomial expansion). We obtain the number of parking functions. That's good.

We see that the number of parking functions in this problem is the same as the number of forests on set $[n]$ consisting of k rooted trees (problem 3.4).

We present the bijection from [13] that gives the combinatorial proof of this fact. Let a tree with n+1 vertices be given. Construct a queue of the breadth first search by this tree. At first we add the root to the queue. Then in each step we remove the first vertex in the queue and add its sons to the queue in increasing order of their numbers. And so on while queue is not empty. Let A_i be the set of vertices added in i-th step (all these vertices are sons of some vertex), a_i be the number of elements of A_i. If in step i none of vertices had been added then A_i is empty. Since the tree is a connected graph with $n+1$ vertices, the queue of the breadth first search for it contains at least one element, while vertex $n+1$ is not removed, and the queue will be empty when we will remove all $n+1$ vertices, that means that a_i comply with restrictions:

$$\begin{cases} a_1 \ge 1 \\ a_1 + a_2 - 1 \ge 1 \\ \ldots \\ a_1 + a_2 + \ldots + a_k - k \ge 1 \\ a_1 + a_2 + \ldots + a_{n+1} = n \end{cases}$$

We define a parking function in the following way: elements of A_i be the numbers of cars that prefer to park at i-th place. It can be proved that the described mapping is a bijection between parking functions for n cars and trees with $n+1$ vertices.

4.6. It is sufficient to describe the inverse mapping, i. e. the rule that allows, given an arbitrary sequence $c = (c_1, c_2, \ldots, c_{n-1})$ where all c_i are remainders modulo $n+1$, to construct a parking function $A = (a_1, \ldots, a_n)$ for which c is a sequence of differences. It can be easily obtained from the solution of problem 4.1.

Ideed, if all the differences $c_i = a_{i+1} - a_i \pmod{n+1}$ are fixed, then there exist exactly $n+1$ preference sequences with those differences for a cyclic parking street. In solution 4.1 those $(n+1)$ sequences are united in one group and it is proved that exactly one parking function belongs to this group. Obviously, that is what we wanted.

4.7. The sum counts all possible parking functions. In fact, to determine a parking function one may start with choosing, for each parking place i, the number k_i which shows how many drivers like that place. Non negative integer numbers k_i should comply with the following restrictions:

$k_n \le 1$ since in the opposite case there exist two drivers who wish park in the last place, so the parking will fail;

$k_{n-1} + k_n \le 2$ since in the opposite case there exist three drivers who wish to park in two last places, so the parking will fail;

and so on till the inequality $k_2 + \ldots + k_{n-1} + k_n \le n-1$.

After numbers k_2, k_3, ..., k_n had been chosen, let $k_1 = n - k_2 - k_3 - \ldots - k_n$ and assign the last k_1 drivers to prefer the first place.

It is easy to understand that the numbers k_1, k_2, ..., k_n satisfying the above restrictions produce a parking function. Indeed, by problem 4.2 the success of the parking process does not depend on the order in which cars enter. Let those who want to park in n-th place go first, then those who want to park in $(n-1)$-th place go after them, and so on. They will perfectly park all cars.

It remains to observe that the number of ways to realize the set k_1, k_2, ..., k_n as a parking functions is equal to the term under the summation sign.

4.8. Solution 1 (from book [8, problem 5.49.f]). Let k_i be the number of elements of sequence a that are equal to i, in particular, $k_n = 0$. The condition on a preference sequence to be a sure parking function is equivalent to the following restrictions:

1) all partial sums of the sequence $k_1 - 1$, $k_2 - 1$, ..., $k_{n-1} - 1$ are positive;
2) $\sum\limits_{i=1}^{n-1}(k_i - 1) = 1$.

Lemma. For any finite integer sequence with sum 1 there exists a unique cyclic permutation such that all its partial sums are positive.

The proof of the lemma is left to the reader.

Obviously, in the sure preference sequence all a_i are numbers from 1 to $n-1$. If we take an arbitrary sequence of n numbers from $[n-1]$, then then numbers k_i defined by this sequence satisfy the condition 2), but, generally speaking, do not satisfy the condition 1). But by the lemma this sequence has a cyclic permutation (exactly one) satisfying the first condition!

Therefore, the number of sure parking functions is $n-1$ times less then the number of elements of $[n-1]^n$.

Solution 2 (direct computation). Consider an arbitrary sure parking function, let k drivers want to park at the first place for this function ($2 \le k \le n$). We give a red hat to one of them and remove him. The preferences of the remaining drivers form a usual (not necessarily sure) parking function in the street with $n-1$ parking places and $k-1$ drivers that prefer to park in the first place. So, to obtain a parking function for which k drivers want to park in first place, we have to choose one driver in hat (n ways) and assign prefernces to others (by problem 4.5 it can be done by $(n-1)^k\binom{n-2}{k-2}$ ways). As a result we obtain not just a parking function, but a parking function such that one of k drivers pretending on the first parking place wears a red hat. Thus, the total number of parking functions is expressed by the sum $\sum\limits_{k=2}^{n}\frac{n}{k}\cdot(n-1)^{n-k}\binom{n-2}{k-2}$. It remains to check the identity

$$\sum_{k=2}^{n}\frac{n}{k}\cdot(n-1)^{n-k}\binom{n-2}{k-2} = (n-1)^{n-1}.$$

Transform the left hand side of the expression: replace the summation index k by $i = n-k$, apply the equality $\frac{n}{n-i}\cdot\binom{n-2}{i}(n-1) = (n-1-i)\binom{n}{i}$ and after that split each summand as a difference of two terms:

$$\sum_{k=2}^{n}\frac{n}{k}\cdot(n-1)^{n-k}\binom{n-2}{k-2} = \sum_{i=0}^{n-2}\frac{n}{n-i}\cdot\binom{n-2}{i}(n-1)^i = \sum_{i=0}^{n-2}(n-1-i)\cdot\binom{n}{i}(n-1)^{i-1} =$$
$$= \sum_{i=0}^{n-2}\binom{n}{i}(n-1)^i - \sum_{i=0}^{n-2}\binom{n}{i}\cdot i(n-1)^{i-1}.$$

By the binomial formula the first sum is equal to

$$n^n - \binom{n}{n}(n-1)^n - \binom{n}{n-1}(n-1)^{n-1}. \qquad (2)$$

For the second sum observe that the 0-th summand vanishes, apply formula $\binom{n}{i}\cdot i = n\binom{n-1}{i-1}$, and after that apply the binomial formula:

$$\sum_{i=0}^{n-2}\binom{n}{i}\cdot i(n-1)^{i-1} = n\sum_{i=1}^{n-2}\binom{n-1}{i-1}(n-1)^{i-1} = n\Big(n^{n-1}-\binom{n-1}{n-1}(n-1)^{n-1}-\binom{n-1}{n-2}(n-1)^{n-2}\Big). \tag{3}$$

It remains to note that the difference of expressions (2) and (3) is equal to $(n-1)^{n-1}$.

4.9. Take an arbitrary parking function. Let b_1, b_2, ..., b_{n+1} be a sequence of numbers of preferred places, written in increasing order. The success of the parking process means that the following inequalities hold: $b_1 \le 1$ (and hence $b_1 = 1$), $b_2 \le 2$, ..., $b_{n+1} \le n+1$.

Choose the largest k, $0 \le k \le n$, such that $b_{k+1} = k+1$. Then the preference sequence b_1, ..., b_k is a parking function for the street with k parking places, and the sequence $b_{k+1}-k$, $b_{k+2}-k$, ..., $b_{n+1}-k$ is a sure parking function for the street with $n+1-k$ parking places. (It is a sure function due to maximality of k.)

Thus, in order to construct an arbitrary parking function in the street with $n+1$ parking places, one may choose an arbitrary k, choose arbitrary k drivers (in $\binom{n+1}{k}$ ways), assign one of the P_k parking functions for their preferences, and assign one of the $(n-k)^{n-k}$ sure parking functions to determine the preferences of the other $n+1-k$ drivers. Thus, we obtain a combinatorial interpretation of the formula under consideration.

4.10. Similarly to problem 4.7, the formula counts the number of sure parking functions for the parking lot of length n.

4.11. In [10] this formula is proved by a complicated bijection with the set of labelled trees. We prove it similarly to the previous problem.

Say that an *enchanced* parking function is a parking sequence $(a_1, \dots, a_n)$ in which all the elements which equal 1 are numbered. For example, $(\underset{1}{1}, 2, \underset{2}{1}, 3, 3)$ and $(\underset{2}{1}, 2, \underset{1}{1}, 3, 3)$ are two different enchanced parking functions (for $n=5$). We denote by $N^*(n)$ the number of enchanced parking functions for the parking lot of length n.

By arguments as in problem 4.7 we obtain that the sum counts the number of enchanced parking functions. It remains to check that $N^*(n) = n^n$.

Consider an enchanced parking sequences in which k drivers like NOT the first place, and $n-k$ drivers prefer to park in the first place. Similarly to problem 4.5we conclude that the number of such sequences equals $\frac{n!}{k!}N(n-1,k)$. Then the total number of enchanced parking functions is given by the formula similar to formula (1):

$$N^*(n) = \sum_{k=0}^{n}\frac{n!}{k!}\cdot N(n-1,k) = \sum_{k=0}^{n}\frac{n!}{k!}\cdot(n-k)n^{k-1}.$$

That is a telescoping series, it is equal to n^n.

5 Inversions on trees and deficiencies of parking functions

5.1. Both statements are inspired by [16].

a) Consider an arbitrary labelled tree with n vertices. Let n–u be the first edge on the path from vertex n to vertex 1 (the case $u=1$ is possible). Remove this edge, the tree breaks up into the two trees A_n and A_1. Vertex u is singled out in tree A_1 in a natural way, i. e. we consider this tree as rooted. Let tree A_1 have $k+1$ vertex, $0 \le k \le n-2$. Then tree A_n has $n-k-1$ vertices. Obviously, the labelled forest (A_n, A_1) is uniquely defined by the initial labelled tree with n vertices.

Now we demonstrate how the inverse mapping is constructed. For all k, $0 \le k \le n-2$, choose vertices for tree A_1. Since vertex 1 has to be in tree A_1, and vertex n has to be in tree

A_n, we need to choose k vertices from the elements of set $[n]$, except 1 and n. This can be done in $\binom{n-2}{k}$ ways; the other $n-k-1$ vertices belong to tree A_n. Then construct trees A_1 and A_n themselves, it can be done in $(k+1)T_{k+1}$ and T_{n-k-1} ways, respectively. Finally, we need "to fasten" the trees, so we need to draw an edge connecting vertex n with the root of tree A_1. We obtain a combinatorial interpretation of the k-th summand on the right hand side of the identity: it is equal to the number of spanning trees on set $[n]$ consisting of exactly two trees such that one tree contains $k+1$ vertices (including vertex n), and the other tree is rooted and contains vertex 1.

b) Consider an arbitrary parking function $a = (a_1, a_2, \ldots, a_{n+1})$ for a street with $n+1$ parking places. Let drivers enter the street in increasing order of their numbers, and assume that the last of them parks on place k. Fix the preferences of the first n drivers and try to increase the preference of the last driver as much as posiible, i. e. find a maximum value of a_{n+1} for which the sequence $(a_1, a_2, \ldots, a_{n+1})$ is a parking function. It is clear that:

— this maximum value is $a_{n+1} = k$,

— none of the other drivers prefers the k-th place, and

— no one of those who found his favourite place occupied drives by the k-th place.

It follows that exactly $k-1$ drivers prefer the places from 1-st to the $(k-1)$-th, and exactly $n+1-k$ drivers prefer the places from the $(k+1)$-th to the $(n+1)$-th. Let $\widetilde{a} = (a_1, a_2, \ldots, a_n, k)$, call this sequence the *enlargement* of the sequence a.

Obviously, for any $\ell \le k$ the sequence $(a_1, a_2, \ldots, a_n, \ell)$ is a parking function, and all k such parking functions (and only them) have the same enlargement function $\widetilde{a}$.

How to construct a sequence $\widetilde{a}$? The last driver is singled out from the beginning. We need to choose $k-1$ drivers who will park in the first $k-1$ places ($\binom{n}{k-1}$ ways) and assign them a parking function (P_{k-1} ways). Then we need to assign a parking function for those who park in the places after the k-th ($P_{n-(k-1)}$ ways). So, there are $\binom{n}{k-1}P_{k-1}P_{n-(k-1)}$ ways to choose a sequence $\widetilde{a}$. Remembering that $\widetilde{a}$ is the enlargement sequence for k different parking functions, we conclude that the number of parking functions P_{n+1} is computed by the formula

$$P_{n+1} = \sum_{k=1}^{n+1} \binom{n}{k-1} k P_{k-1} P_{n-(k-1)}.$$

5.2. Answer: $F_n^*(x) = \sum\limits_{k=0}^{n} \binom{n}{k} F_k(x) F_{n-k}(x)$.

5.3. Both statements are from [16]. These recursions are detailed versions of the recursions from problem 5.1.

a) Note that in the definition of $\mathrm{inv}(T)$ the labels of vertices can be considered as arbitrary real numbers. Besides that, let us demand that the root has no contribution to the number $\mathrm{inv}(T)$, therefore the number $\mathrm{inv}(T)$ does not depend on the root label.

We give a useful definition. Consider a labelled rooted tree T on set $[\ell]$ and fix a set of numbers $S = \{s_1, s_2, \ldots, s_\ell\}$. Define a collection consisting of ℓ rooted trees T_1, T_2, …, T_ℓ, such that the vertices of each of them are labelled by the elements of set S. Tree T_i is obtained from tree T by replacing its labels by labels from set S in the following way. The root of tree T has some label, replace it by label s_i. Arrange the other elements of the set S in increasing order and place them in unrooted vertices of tree T in the same way "as it has been done in tree T": the smallest label is put at vertex 1, the next label is put at vertex 2, etc. Is is evident that the numbers of inversions in all trees in this collection coincide. Call the set of trees of this collection *equally-inversional* to each other.

Now return to the solution. Append the inversion counting to the reasonings of solution 5.1 a). In order not to change notations, we will prove the required relation with n replaced with $n-2$ (recall that polynomial F_n is generated by the set of forests with $n+1$ vertices):

$$F_{n-1}(x) = \sum_{k=0}^{n-2} \binom{n-2}{k} (x^k + x^{k-1} + \ldots + 1) F_k(x) F_{n-k-2}(x).$$

So in solution 5.1 a) all possible labelled trees are in one to one correspondence with forests (A_n, A_1). To define forest (A_n, A_1), we need to choose k vertices for tree A_1 from all elements of set $[n]$ except 1 and n, (we have $\binom{n-2}{k}$ ways, the other $n-k-1$ vertices automatically belong to tree A_n) and construct trees A_1 and A_n themselves (the tree A_1 is rooted). Then we "fasten" trees by drawing an edge that connects vertex n with the root of tree A_1.

To count the inversions, fix trees A_n and A_1 and group in one cluster the $k+1$ forests of the form (A_n, A), where A ranges over the set of rooted trees which are equally-inversional to tree A_1. The number of inversions in each tree $T \in \mathcal{T}_n$ obtained in this way is equal to $\mathrm{inv}(A_n)+\mathrm{inv}(A)+\delta_A$, where the correction term δ_A equals the number of inversions of the root vertex of A with other vertices of A (being the root of tree A, it does not participate in the counting of the value $\mathrm{inv}(A)$, but after fastening the trees it participates). As we noted, $\mathrm{inv}(A) = \mathrm{inv}(A_1)$ for all trees A that are equally-inversional to tree A_1. As for the term δ_A, it is clear that it takes each of the values 0, 1, 2, ..., k exactly once, as A runs over the set of all trees that are equally-inversional to tree A_1.

Each forest (A_n, A) of our cluster determines summands $x^{\mathrm{inv}(A_n)}$, $x^{\mathrm{inv}(A)}$ in the enumerators $F_{n-k-2}(x)$, $F_k(x)$. The exponent of their product $x^{\mathrm{inv}(A_n)+\mathrm{inv}(A)}$ equals the number of inversions of the obtained graph without taking into account the correction term. Summing the contributions of the trees that are equally-inversional to tree A_1 we obtain the expression

$$(x^k + x^{k-1} + \ldots + 1)x^{\mathrm{inv}(A_n)+\mathrm{inv}(A)},$$

which equals the sum of monomials of the enumerator $F_{n-1}(x)$ for the trees generated by our cluster. Summing over all clusters we obtain the required formula.

b) We append the deficiency counting to the reasonings of solution 5.1 b). In that solution the set of parking functions is partitioned into clusters. A cluster generated by a parking function $a = (a_1, a_2, \ldots, a_{n+1})$ consists of all parking functions $(a_1, a_2, \ldots, a_n, i)$ where $1 \le i \le k$, and k is the maximal possible preference of $(n+1)$-th driver for which the sequence $(a_1, a_2, \ldots, a_n, k)$ is a parking function.

For counting all possible parking functions with given parameter k we consider all possible functions a' for those drivers who park in the first $k-1$ places, and all possible functions a'' for those who park in the last $n-(k-1)$ places. Roughly speaking, the deficiency of these parking cases is equal to $D(a')$ and $D(a'')$, and in the language of enumerators it equals $x^{D(a')}$ and $x^{D(a'')}$. As for the $(n+1)$-th driver who parks in the k-th place for all functions of our cluster, his contribution to the whole deficiency for functions of our cluster takes each of the values 0, 1, 2, ..., k exactly once. Thus, the total deficiency of parking functions from one cluster is expressed by $(x^{k-1}+x^{k-2}+\ldots+1)x^{D(a')}x^{D(a'')}$. Summing over all clusters we obtain the required formula.

5.4. See [19].

References

[1] *Айгнер М., Циглер Г.* Доказательства из Книги. М.:Мир, 2006.

[2] *Берлов С. Л., Иванов С. В., Кохась К. П.* Петербургские математические олимпиады. СПб.: "Лань", 2000.

[3] *Глибичук А. А., Дайняк А. Б., Ильинский Д. Г., Купавский А. Б., Райгородский А. М., Скопенков А. Б., Чернов А. А.* Элементы дискретной математики в задачах. М.:МЦНМО, 2016.

[4] *Иванов О. А.* Элементарная математика для школьников, студентов и преподавателей. М.:МЦНМО, 2009.

[5] Комбинаторный анализ. Задачи и упражнения. / Под. ред. К. А. Рыбникова. М.: Наука, 1982.

[6] *Ландо С. К.* Введение в дискретную математику. М.: МЦНМО, 2012.

[7] *Сачков В. Н.* Введение в комбинаторные методы дискретной математики. М.: МЦНМО, 2004.

[8] *Стэнли Р.* Перечислительная комбинаторика. Т. 2. М.: Мир, 2005.

[9] *Beineke L. W., Moon J. W.* Several proofs of the number of labelled 2-dimensional trees. In "Proof Techniques in Graph Theory" (F. Harary, editor). New York: Academic Press, 1969. P. 11-20.

[10] *Benjamin A. T., Juhnke F.* Another way of counting N^N. // SIAM J. Disc. Math. 1992. V. 5. No. 3. P. 377–379.

[11] *Bóna M.* Combinatorics of permutations. Chapman & Hall/CRC, 2004.

[12] *Bóna M.* A walk through combinatorics. 3rd ed. World Scientific Publ. Co., 2011.

[13] *Chassaing P. , Marckert J.-F.* Parking functions, empirical processes, and the width of rooted labelled trees // Electron. J. Combin. 2001. V. 8. № 1. Research Paper 14.

[14] *Guo S., Guo V.* A recursive algorithm for trees and forests // `http://arxiv.org/pdf/math/1702.01744v1.pdf`

[15] *Konheim A. G., Weiss B.* An occupancy discipline and applications. // SIAM J. Appl. Math. 1966. Vol. 14. № 6. P. 1266–1274.

[16] *Kreweras G.* Une famille de polynômes ayant plusieurs propriétés énumeratives // Period. Math. Hungar. V. 11. 1980. № 4. P. 309–320.

[17] *Moon J. W.* Counting labelled trees. William Clowes and Sons, 1970.

[18] *Shukla A.* A short proof of Cayley's tree formula // `https://arxiv.org/pdf/0908.2324.pdf`

[19] *Yan C. H.* Parking functions// in Handbook of Enumerative Combinatorics. M. Bóna, ed.

Замощения: подстановки и декорации.

Алексей Белов-Канель, Пьер Гийон, Илья Иванов-Погодаев, Иван Митрофанов

Этот проект посвящен замощениям на плоскости. Обычно, когда плитками нескольких типов удается замостить плоскость, речь идет о замощении, структура которого периодически повторяется. Более строго: замощение называется *периодическим* если оно переходит в себя при сдвиге на ненулевой вектор. Китайский математик Хао Ванг в 1961 году поставил следующую задачу:

Рассмотрим единичные квадраты, стороны которых раскрашены в конечное множество цветов, каждая в один цвет. Пусть выбрано несколько типов таких квадратов. Разрешается прикладывать квадраты друг к другу сторонами, покрашенными в один цвет. Допустим, можно использовать неограниченное количество квадратов выбранных типов. Верно ли, что если можно замостить плоскость, то это можно сделать периодическим способом?

Изначально Ванг предполагал, что ответ положительный, то есть, если какое-нибудь замощение существует, то есть и периодическое. Но в 1966 году Роберт Бергер (ученик Ванга) построил набор, состоящий из 20426 квадратов, которым можно замостить плоскость только непериодически. Позднее Бергер сократил число плиток до 104, а в 1971 году Рафаэль Робинсон значительно упростил конструкцию, представив набор из 6 многоугольников, которыми можно замостить плоскость только непериодически.

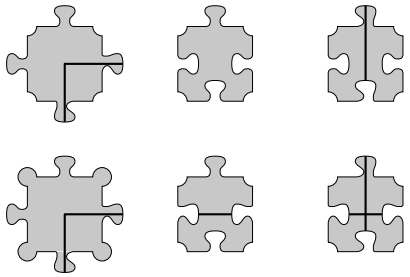


Рис. 1. Набор плиток Робинсона.

Эта задача имеет философскую подоплеку. Речь идет о том, можно ли добиться некоторого глобального свойства (непериодичности) обладая локальными средствами (цветовыми правилами примыкания). Вообще подобные постановки возникают часто: например, как организовать работу вычислительной сети, чтобы локальный сбой не нарушал глобальной работы. Или как локальное взаимодействие молекул приводит к формированию кристаллов.

В рамках этого проекта мы будем постепенно осваивать методы, чтобы решать такие задачи, в разных постановках. Основной задачей первой части проекта будет построение набора многоугольников, которыми можно замостить плоскость только непериодическим способом (B10). По сути, эта задача сводится к построению системы локальных правил (граничных условий, определяющих, когда можно ставить квадратные плитки рядом, а когда нельзя). Построение такого набора использует несколько приемов, которым посвящены предварительные задачи.

A. Одномерный случай

Рассмотрим бесконечную в обе стороны ленту, состоящую из клеток – одинаковых квадратов. Будем расставлять буквы из конечного алфавита, по одной в каждую клетку. Клетку с буквой внутри будем называть *плиткой*.

Замощением будем называть расстановку букв алфавита во всех клетки ленты. *Периодическими* будем называть такие замощения, которые переходят в себя при сдвиге на целое ненулевое расстояние p. При этом, как легко видеть, его можно описать как периодическое повторение какой-то комбинации из p плиток. Комбинация из p плиток – это период замощения, а число p – это длина периода.

Запретом или *запрещенным словом* или *локальным правилом* будем называть комбинацию из нескольких соседних плиток. Мы будем интересоваться замощениями, внутри которых не встречается ни один из запретов. В записи удобно плитки записывать буквами конечного алфавита, а запреты – словами. Замощения, в которых не встречается ни один из запретов, называются *разрешенными*. В дальнейшем мы всегда будем предполагать, что локальных правил конечное число.

Замощения, переходящие друг в друга при сдвиге, будем считать *эквивалентными* или одинаковыми. В дальнейшем мы не будем различать такие замощения.

A1 Рассмотрим алфавит $\{0, 1\}$, причем слово 01 запрещено. сколько существует неэквивалентных разрешённых замощений?

A2 Покажите, что даже для двух букв существует замощение, не являющееся периодическим.

A3 Придумайте конечную систему запретов в алфавите $\{a, b, c\}$, чтобы разрешенным было только периодическое замощение с периодом abc.

A4 Существует ли система запретов в алфавите $\{0, 1\}$ такая, что разрешенных неэквивалентных замощений ровно сто?

A5 Пусть A некоторое конечное слово. Докажите, что существует конечная система запретов, такая что единственным разрешенным замощением будет периодическое с периодом A.

A6 Пусть A некоторое непериодическое замощение. Докажите, что не существует конечной системы запретов, для которой единственными разрешенными замощениями будут A и эквивалентные ему.

A7 Пусть имеется n букв. Пусть каждый запрещенное слово имеет длину 2, и всего их k, причем разрешенных замощений не существует. Для какого минимального k это возможно?

B. Плоский случай: локальные правила и подстановки

Выводы из одномерного случая. Запрет в одномерном случае играет роль локального условия. Комбинируя локальные условия мы хотим добиться глобального свойства. Но в одномерном случае конечное число запретов не дает возможности получить только непериодические замощения.

Перейдем к двумерному случаю. Сначала еще раз зафиксируем основные понятия и определения.

Рассмотрим клеточную плоскость и будем записывать в каждую клетку одну из букв конечного алфавита L, будем называть его *алфавитом плиток*. Пусть в каждой клетке записана одна из букв алфавита. Тогда задана расстановка букв в клетках. Такую расстановку будем называть *замощением*.

По аналогии с одномерным случаем, замощение называется периодическим, если оно переходит в себя при сдвиге на ненулевой целочисленный вектор (a, b).

Эквивалентность замощений. Определение. Рассмотрим два замощения бесконечной плоскости S_1 и S_2. Допустим, одно из них можно сдвинуть на целочисленный вектор и получить другое. В этом случае будем считать, что S_1 и S_2 *эквивалентны. Замечание.* Все замощения конечной фигуры считаются неэквивалентными.

Локальные правила. Определение. Пусть n – натуральное число, не меньшее 2. Рассмотрим множество всех квадратов $n \times n$, состоящих из наших букв-плиток. Иначе говоря, это множество – L^{n^2} (множество конечных наборов из n^2 букв в алфавите L). Рассмотрим в этом множестве некоторое **конечное** подмножество M. То есть, M – это несколько квадратов $n \times n$, составленных из букв алфавита L. Эти квадраты будем называть *запрещенными* или *локальными правилами*, число n – размер локального правила. Замощение называется *разрешенным*, если в нем не встречается запрещенных квадратов.

Задавая различные локальные правила, мы можем в какой-то степени управлять разрешёнными замощениями. Рассмотрим несколько примеров.

B1 Пусть алфавит плиток состоит из двух букв. Постройте локальные правила, чтобы разрешенным замощением была только шахматная раскраска.

B2 Пусть в алфавите две буквы 0 и 1, восемь квадратов 2×2 запрещены (см. рисунок ниже). Сколько существует разрешенных замощений прямоугольника $m \times n$?

1	1
0	1

1	1
1	0

1	0
1	1

0	1
1	1

1	0
0	0

0	1
0	0

0	0
0	1

0	0
1	0

B3 Пусть в алфавите $\{0, 1\}$ запрещены те же квадраты 2×2, что и в предыдущей задаче, а кроме того запрещён один квадрат с единицами на главной диагонали. Опишите все неэквивалентные разрешенные замощения плоскости.

1	1
0	1

1	1
1	0

1	0
1	1

0	1
1	1

1	0
0	0

0	1
0	0

0	0
0	1

0	0
1	0

1	0
0	1

B4 Пусть в алфавите четыре буквы, и разрешенными квадратами 2×2 являются квадраты с четырьмя разными буквами. Остальные квадраты запрещенные. Сколько существует разрешенных замощений прямоугольника $m \times n$?

B5 Пусть алфавит плиток состоит из двух букв. Пусть задано k запрещенных блоков 2×2 так, что нет ни одного разрешенного замощения. Какое минимальное k может быть?

B6 Пусть в плиточном алфавите $\{0, 1\}$ задано некоторое множество локальных правил, причем картинка на рисунке является разрешенной (остальные клетки, кроме девяти, заполнены нулями.) Докажите, что существует еще бесконечное множество неэквивалентных между собой разрешенных замощений.

0	1	0
1	0	1
1	1	1

Эта задача показывает, что не всегда [1] получается с помощью локальных правил задать одно конкретное замощение. Но если нельзя задать одно, может быть можно задать некоторое множество в чем то похожих друг на друга замощений? Будем говорить, что множество замощений *задается некоторыми локальными правилами*, если разрешенными замощениями при таких правилах будут только замощения из этого множества.

B7 *Рамкой* назовём фигуру, состоящую для некоторых $m, n > 1$ из $2(m + n) - 4$ граничных клеток прямоугольника $m \times n$. Назовём раскраску *красивой*, если единицы стоят на объединении какого-то (конечного или бесконечного) множества рамок, а в остальных клетках стоят нули. Пусть задано конечное множество локальных правил, и все красивые раскраски клетчатой плоскости являются разрешёнными. Докажите, что есть бесконечно много неэквивалентных разрешённых раскрасок, не являющихся красивыми.

B8 Пусть заданы некоторые локальные правила и, в соответствии с этими правилами, для любого положительного r плитками можно замостить область, включающую круг радиуса r. Докажите, что тогда можно замостить и всю плоскость.

С помощью локальных правил можно получать довольно сложные замощения. Например, с помощью них можно добиться того, чтобы все разрешенные замощения были непериодичны. Сразу это задачу будет решить сложно, мы рекомендуем вернуться к ней в цикле C, после освоения дополнительных методов.

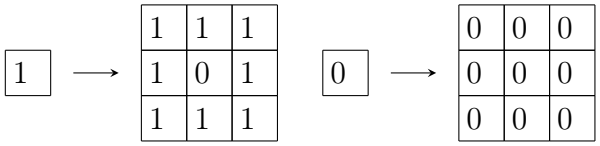
B9* Придумайте локальные правила такие, чтобы все разрешенные замощения были непериодичны.

B10* Постройте конечный набор многоугольников, которыми можно замостить плоскость только непериодически. Многоугольники друг к другу можно прикладывать как угодно, можно поворачивать и переворачивать, но они не должны перекрываться.

Определение. Пусть каждому символу алфавита сопоставлен квадрат $k \times k$ из символов того же алфавита. Такое соответствие будем называть *подстановкой*.

Если есть подстановка σ и замощение A какой-то области (конечной или бесконечной), то можно получить новое замощение $\sigma(A)$. Для этого каждую плитку мы заменяем на соответствующий квадрат $k \times k$. Если начать с одной плитки и применять подстановку несколько раз, мы получим большой квадрат.

Определение. Пусть задана некоторая $k \times k$ подстановка σ. Пусть также замощение плоскости можно разбить вертикальными и горизонтальными прямыми на квадраты $k \times k$ так, что каждый квадрат $k \times k$ лежит в образе σ (то есть каждый квадрат является $\sigma(A)$ для некоторой буквы A). Запишем вместо каждого квадрата $\sigma(A)$ букву A. Полученное замощение будем обозначать как $\sigma^{-1}(S)$. Если $\sigma^{-1}(S)$ определено однозначно, будем говорить, что в замощении S возможен переход к прообразу $\sigma^{-1}(S)$. Замощение будем называть *бесконечно декодируемым* относительно подстановки σ, если переход к прообразу можно провести любое число раз.



B11 Рассмотрим подстановку как на рисунке. Бесконечно декодируемое замощение для неё называется *ковром Серпинского*.

a) Докажите, что есть бесконечно много попарно неэквивалентных ковров Серпинского.

b) Докажите, что все ковры Серпинского кроме одного являются непериодичными замощениями.

c) Задаётся ли множество ковров Серпинского локальными правилами?

Если мы хотим задать с помощью локальных правил бесконечно декодируемые замощения, логично потребовать, чтобы подстановка переводила разрешённые замощения в разрешённые.

Определение. Будем говорить, что подстановка *согласована с локальными правилами* размера k, если
1) для любой буквы A, квадрат $\sigma(A)$ является разрешенным;
2) если X – разрешенный квадрат 2×2, то квадрат $\sigma(X)$ содержит только разрешенные квадраты $k \times k$.

B12 Пусть заданы локальные правила R, причем $k = 2$, то есть все запрещенные квадраты размера 2×2. Пусть некоторый квадрат A размера $N \times N$ является разрешенным, то есть не содержит запрещенных квадратов 2×2. Пусть подстановка σ согласована с R. Докажите, что квадрат $\sigma(A)$ также разрешенный.

[1] на самом деле, для непериодических замощений – *никогда*, и позже мы это докажем

B13 Пусть подстановка σ согласована с локальными правилами размера 2. Докажите, что существует разрешенное замощение.

B14 Рассмотрим подстановку σ. Верно ли, что существует замощение S, для которого верно $\sigma(S)$ эквивалентно S? Придумайте достаточные условия на σ, чтобы такое замощение существовало.

C. Примеры непериодичности

Итоги после циклов A и B. Мы хотим найти такое множество замощений, которое с одной стороны задаётся локальными правилами, а с другой стороны – содержит только непериодичные замощения. В одномерном случае такого множества не бывает (почему?). Самые простые известные нам двумерные примеры – это бесконечно декодируемые относительно подстановки замощения.

Подходит не любая подстановка.

C1 a) Приведите пример такой подстановки, что все бесконечно декодируемые замощения непериодичны, но множество бесконечно декодируемых замощений не задаётся локальными правилами.

b) Приведите пример такой подстановки, что все бесконечно декодируемые замощения периодичны.

Искать подходящие подстановки проще не «с нуля», а в некотором смысле улучшая не подходящие.

Переход к другому алфавиту. Декорации. Пусть задан алфавит плиток $a, b, c \dots$. Мы можем ввести конечное число дубликатов (оттенков) для каждой буквы и рассмотреть расширенный алфавит плиток $a_1, \dots a_k, b_1, \dots b_k, c_1, \dots c_k, \dots$. Будем теперь вводить локальные правила для расширенного алфавита. После этого можно рассмотреть разрешенные замощения и игнорировать введенные оттенки. Такой прием называется *введение декораций*.

Определение. Пусть задана подстановка σ_1 в алфавите A_2 и σ_2 в алфавите A_2. Подстановку σ_2 будем считать *декорацией для* σ_1, если выполнены следующие условия:

1) существует функция f, определенная на A_2, со значениями в A_1;

2) если $\sigma_2(a) = M$ – квадрат, составленный из букв алфавита A_2, то $\sigma_1(f(a)) = f(M)$.

Функцию f можно понимать как забывание оттенка у цвета, а $f(M)$ – это квадрат того же размера, что и M, но из основных цветов без оттенков.

Основной нашей задачей будет доказательство того, что заданную подстановку можно декорировать так, чтобы множество бесконечно декодируемых замощений задавалось локальными правилами.

Для начала мы разберем некоторые полезные частные случаи. Пусть задана подстановка σ. Если A – буква алфавита, то $\sigma(A)$ - квадрат 2×2 из четырех букв алфавита (куда отображается A). Будем считать, что разные символы отображаются в разные квадраты 2×2.

Разделение образов. Определение. Определим отображение σ_{UL}, сопоставляющее символу A левый верхний угол квадрата $\sigma(A)$. Аналогично определим отображения σ_{DL}, σ_{UR}, σ_{DR}. Будем считать, что подстановка обладает свойством разделения образов, если каждый символ алфавита присутствует в образе ровно одного из этих четырех отображений.

C2 Приведите пример подстановки с разделением образов.

Свойство разделения образов помогает нам при конструировании локальных правил. Сначала постараемся добиться цели для частного случая – какой нибудь подстановки. После этого, попробуем разобраться с подстановками с разделением образов. И уже потом перейдем к общему случаю.

Идея построения. Для начала попробуйте раскрашивать ребра квадратов в различные цвета и формулировать локальные правила в терминах сочетаний этих цветов. Основная цель – добиться того, чтобы любое разрешенное замощение позволяло себя декодировать, то есть переходить к предыдущему уровню иерархии. Такой переход к предыдущему уровню и осуществляет подстановка.

C3 Придумайте какую нибудь подстановку σ и локальные правила, такие, что любое разрешенное замощение S допускает переход к прообразу $\sigma^{-1}(S)$ и замощение $\sigma^{-1}(S)$ также является разрешенным. Докажите, что всякое разрешенное замощение является непериодичным.

C4 Пусть задана 2×2 подстановка σ с разделением образов. Пусть также заданы локальные правила, что любое разрешенное замощение S допускает переход к прообразу $\sigma^{-1}(S)$ и замощение $\sigma^{-1}(S)$ также является разрешенным. Докажите, что всякое разрешенное данными локальными правилами замощение является непериодичным.

C5 Пусть задана 2×2 подстановка σ с разделением образов. Докажите, что для некоторой декорации подстановки множество бесконечно декодируемых замощений определяется локальными правилами.

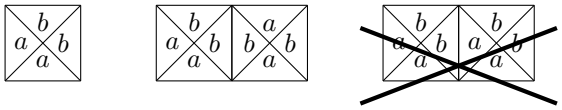
C6 Пусть задана 3×3 подстановка σ с разделением образов. Докажите, что для некоторой декорации подстановки множество бесконечно декодируемых замощений определяется локальными правилами.

C7 Пусть задана 2×2 подстановка σ, не обязательно с разделением образов. Докажите, что для некоторой декорации подстановки множество бесконечно декодируемых замощений определяется локальными правилами.

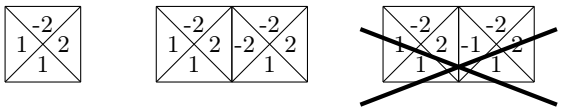
D. Различные формализмы и перевод непериодичности на другие языки.

Задачи о замощения можно формулировать на разных языках (формализмах). Иногда бывает полезно, получив продвижение в какой-то одной постановке, перевести ее на другую.

Формализм Ванга. Каждая плитка – единичный квадрат. Каждая сторона квадрата раскрашена в один из конечного множества цветов. Квадраты можно прикладывать друг к другу, совмещая стороны одного цвета.



Формализм дополняющих цветов. Каждая плитка – единичный квадрат. На сторонах каждого квадрата написаны ненулевые целые числа из конечного набора, которые можно назвать цветами. Квадраты можно прикладывать друг к другу, совмещая стороны, на которых написаны противоположные числа.



Иногда считают, что вместе с плиткой в наборе есть и повернутая на 90 градусов плитка. В этом случае говорят, что плитки можно поворачивать.

Рассмотрим плитку A с цветами (a_1, a_2, a_3, a_4) по часовой стрелке. Перевернутой плиткой будем называть плитку с цветами $(-a_3, -a_2, -a_1, -a_4)$ *против часовой стрелки*. Если для каждой плитки в наборе есть и ее перевернутая плитка то говорят, что плитки можно переворачивать.

Определение. Будем называть набор *апериодическим* (в каком-либо формализме), если с его помощью можно замостить плоскость только непериодически.

D1 Докажите, что формализмы Ванга и дополняющих цветов эквивалентны, то есть если есть непериодический набор в одном формализме, то есть соответствующий ему непериодический набор в другом.

D2 Назовем многоугольник *квадратно-составленным*, если он представляет собой фигуру полимино, составленную из единичных квадратов (связную и без дыр внутри). Постройте апериодический набор из квадратно-составленных многоугольников, которые можно поворачивать и переворачивать.

D3 Рассмотрим формализм дополняющих цветов, причем плитки можно поворачивать и переворачивать.

a) Может ли набор быть апериодичным?

b) Пусть теперь по-прежнему плитки разрешается прикладывать по правилам дополняющих цветов, но перевернутые плитки не могут иметь общую сторону. Докажите, что существует апериодический набор.

Замощения: подстановки и декорации. Решения.

A. Одномерный случай

A1 *Ответ: 3.* Понятно, что замощения из всех одинаковых букв (единиц или нулей) подходят. Если в замощении есть и 1, и 0, то должны быть соседние 1 и 0, причём 1 стоит слева. Далее понятно, что левее единицы могут стоять только единицы, а правее нуля – только нули.

1	1	1	1	1	1	1	1	1	1	1	1

0	0	0	0	0	0	0	0	0	0	0	0

1	1	1	1	1	1	0	0	0	0	0	0

A2 Примеров очень много. Например, если в одной клетке стоит 0, а в остальных – единицы, то при любом сдвиге этот ноль перейдёт в единицу.

1	1	1	1	1	0	1	1	1	1	1	1

A3 Предлагаем убедиться, что если запретить слова aa, ac, ba, bb, cb и cc, то у любой буквы однозначно определяются оба соседа и получается именно то, что нам нужно.

A4 *Ответ: да.* Например, можно ввести такие запреты, чтобы разрешёнными были периодические замощения с периодами $01, 001, \ldots, 0^{100}1$. Запретим слова $11, 0^{101}$, а также $100 \cdot 99$ слов вида 10^a10^b1 при всевозможных неравных a и b от 1 до 100.
Первые два запрета вынуждают, чтобы между двумя соседними единицами было от 1 до 100 нулей. Остальные запреты гарантируют, что слева и справа от любой единицы подряд идущих нулей поровну.

A5 Напомним, что циклическим сдвигом слова $a_1a_2\ldots a_n$ называется любое из слов $a_{i+1}a_{i+2}\ldots a_na_1a_2\ldots a_i$ при $0 \leqslant i < n$ (то есть то, что получится, если отрезать начало длины i и переставить в конец).
Пусть длина слова A равняется n, а в алфавите k букв. Всего есть k^n слов длины n, запретим из них все, не являющиеся циклическими сдвигами A.
Во всех циклических сдвигах A поровну букв каждого вида, поэтому в любом разрешённом замощении плитки на расстоянии n обязаны совпадать, то есть разрешённое замощение периодично с длиной периода n. Если периодом является какой-то циклический сдвиг A, а значит, и A тоже является периодом.

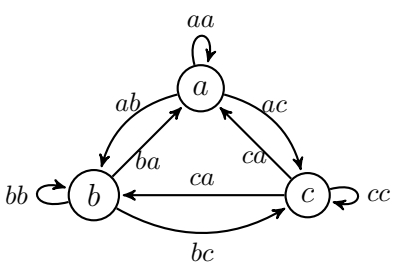
A6 Покажем, что для любой конечной системы запретов, для которой есть хотя бы одно разрешённое замощение полосы, найдётся и периодическое замощение. Пусть N – длина наибольшего из запретов. Возьмём какое-нибудь разрешённое замощение и найдём в нём два непересекающихся блока длины N, обозначим их U, а часть между ними обозначим W.

$\cdots$	U	W	U	$\cdots$

Тогда замощение с периодом UW разрешено. В самом деле, все прямоугольники длины не больше N встречаются и в исходном замощении (а значит, не содержат запрещённых), а запретов длинее N у нас нет.

$\cdots$	W	U	W	U	W	$\cdots$

A7 *Ответ:* $n(n+1)/2$.
Пример: Пусть алфавит состоит из чисел от 1 до n и запрещены слова ab при $a \geqslant b$. Тогда не получится замостить кусок длинее n, ибо при движении слева направо каждая слебующая буква должна быть больше предыдущей.
Оценка: Запреты длины 2 – это ограничения на то, какие плитки-буквы могут быть соседними. Нарисуем полный ориентированный граф на n вершинах (с петлями):



Каждый запрет длины 2 убирает в этом графе одно ребро. Легко понять, что если остался хотя бы один цикл, то бесконечный путь по этому циклу – это разрешённое периодичное замощение.

Теперь покажем индукцией по n, что если в ориентированном графе нет ориентированных циклов, то рёбер не более $n(n-1)/2$. Переход от n к $n+1$: если из каждой вершины выходит хотя бы одно ребро, то цикл есть. Если из какой-то вершины рёбер нет, то с ней связано не более n рёбер, а в подграфе на оставшихся вершинах не более $n(n-1)/2$ рёбер, что и даёт переход. А база $n=1$ очевидна.

B. Плоский случай: локальные правила и подстановки

B1 Достаточно запретить все квадраты 2×2 кроме двух шахматно раскрашенных. Тогда в разрешённом замощении белые будут граничить только с чёрными, а чёрные – только с белыми.

B2 *Ответ:* 2^{m+n-1}. Можно заметить, что разрешённые квадраты 2×2 – это те, в которых чётное число единиц. Значит, каждая клетка единственным образом определяется по трём соседним (слева, сверху, слева-сверху). Поэтому для любого заполнения левого столбца и верхней строки прямоугольника оставшиеся клетки можно заполнить однозначно.

a_2	a_3
a_1	?

B3 *Ответ: замощения горизонталями, замощения вертикалями и одно замощение квадрантами.*

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0

0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1

0	0	0	0	1	1	1	1
0	0	0	0	1	1	1	1
0	0	0	0	1	1	1	1
0	0	0	**0**	**1**	1	1	1
1	1	1	**1**	**0**	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0

Разберём два случая: встречается ли в замощении квадрат с единицами на побочной диагонали (выделен жирным) или нет.

Встречается. Сначала однозначно заполняется «крест» ширины 2 с центром в этом квадрате, потом одна за одной заполняются оставшиеся клетки и получим замощение квадрантами.

Не встречается. Любой квадрат 2×2 либо одноцветный, либо граница между нулями и единицами делит квадрат на две доминошки. Если замощение не одноцветное, то в нём есть соседние по стороне 0 и 1. Далее однозначно заполняется содержащая их полоса ширины 2: это либо либо две горизонтали, либо две вертикали. В первом случае получается, что все горизонтали одноцветные; во втором – что все вертикали одноцветные.

B4 *Ответ:* $6(2^n+2^m-4)$.

В двух доминошках, расположенных через одну, буквы могут располагаться

так:

a	a
b	b

или так:

a	b
b	a

Назовём линию (горизонталь или вертикаль) *полосатой*, если в ней два типа букв и буквы чередуются. Легко видеть, что если какая-то линия полосатая, то все параллельные ей тоже полосатые.

c	d	c	d	c	d	c	d	c	d	c	d
a	b	a	b	a	b	a	b	a	b	a	b

Покажем, что найдётся хотя бы одна полосатая линия. Пусть верхняя горизонталь таблицы не полосатая, тогда в ней есть различные буквы (пусть a и b) на расстоянии 2.

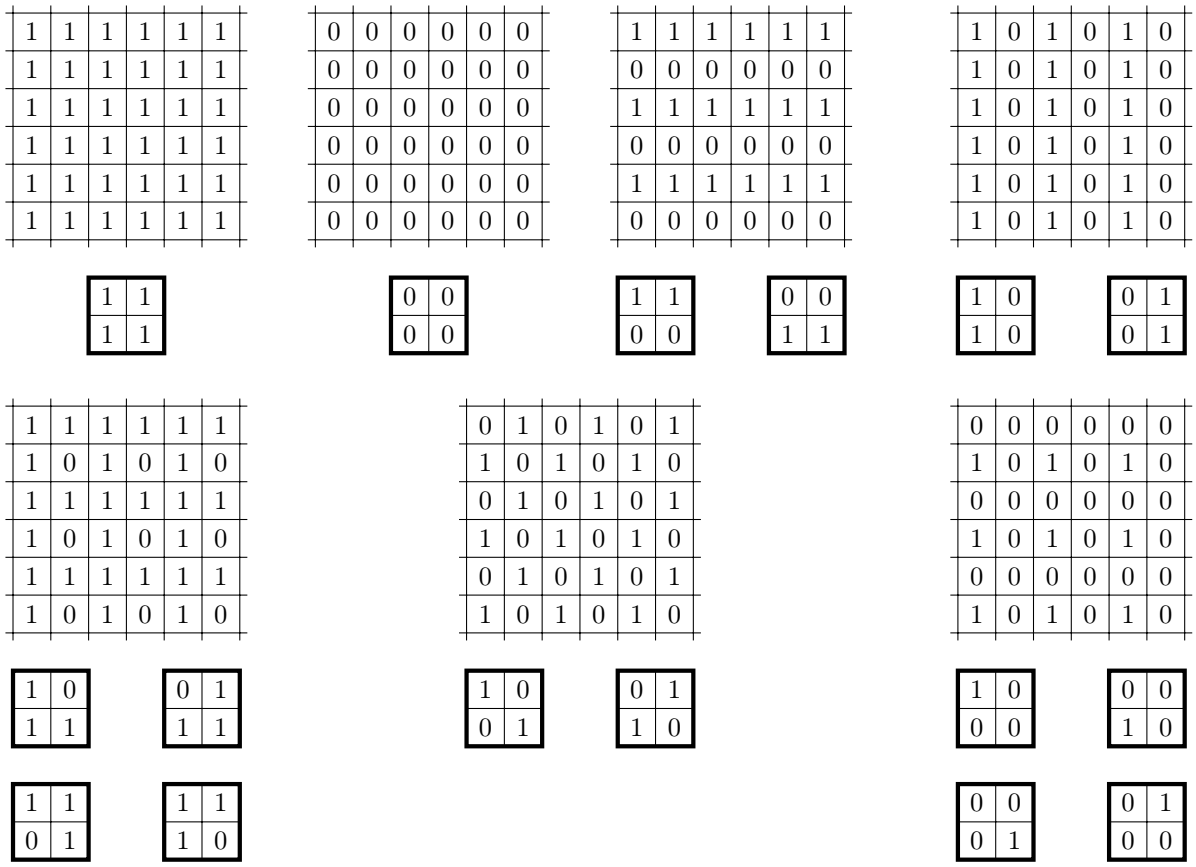
			a		b		
			b		a		
			a		b		
			b		a		

Тогда нетрудно понять, что эти клетки находятся в полосатых вертикалях.

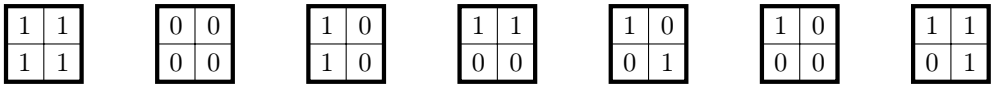
Разрешённых замощений, в которых все горизонтали полосатые, $6 \cdot 2^n$ (одна горизонталь красится в шахматном порядке 12ю способами, а остальные 2мя). Замощений, в которых все горизонтали полосатые, $6 \cdot 2^m$. Дважды подсчитано 24 замощения, они определяются перестановкой цветов в левом верхнем квадрате 2×2.

B5 *Ответ: 7.*

Всего есть 16 квадратов 2×2. Они разбиваются на 7 групп, и для того чтобы запретить 7 периодичных замощений, нужно запретить хотя бы по одному квадрату из каждой группы.



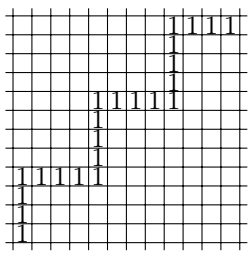
Приведём пример из семи запрещённых квадратов:



Из последних четырёх запретов следует, что под единицей не может стоять ноль. Вместе с первым запретом это даёт, что единицы не могут находиться в соседних столбцах, а вместе со вторым – что нули не могут находиться в соседних столбцах. Тогда единственное возможное замощение – это периодичное замощение чередующимися столбцами, но третье локальное правило запрещает и его.

B6 Пусть $N \times N$ – наибольший размер локального правила. Нетрудно понять, что если мы заполним всю плоскость нулями, а потом нарисуем несколько картинок, чтобы расстояние между любыми двумя было больше N, то получится разрешённое замощение.

B7 Назовём *лесенкой* бесконечную ступенчатую фигуру из единичек, мы нарисовали фрагмент лесенки с шагом 4 (все пустые клетки заполнены нулями).



Если N – размер наибольшего локального правила, то все лесенки с шагом большим чем N являются разрешёнными, потому что все квадраты размера $N \times N$ выглядят как части какой-то большой рамки.

Так как лесенка не содержит ни одной рамки, она не является красивым замощением.

B8 На первый взгляд кажется, что доказывать здесь нечего, так как плоскость – это, в некотором роде, круг бесконечного радиуса. Но на самом деле из того, что мы умеем покрывать плитками *сколь угодно большой* круг не следует автоматически, что мы сможем покрыть *бесконечно большой* круг.

Лирическое отступление. Кащей Бессмертный гулял по лесу и нашёл волшебный обменник валюты. В нём можно за один раз обменять один самоцвет на любое натуральное число золотых монет, или одну золотую монету на любое число серебряных, или одну серебряную на любое число медных. Изначально у Кащея сто самоцветов. Для поддержания бессмертия Кащею в день требуется одна медная монетка. Сможет ли он жить за счёт обменов сколь угодно долго? А бесконечно долго?

Вернёмся к задаче. Будем считать, что в соответствии с локальными правилами замощаются круги с центром в начале координат. Если к набору плиток A можно добавить ещё несколько плиток и получить замощение B, то будем говорить, что замощение A *продолжается до замощения* B или является его *подзамощением*.

Если бы мы нашли бесконечную последовательность замощений A_1, A_2, A_3 такую, что каждое предыдущее замощение продолжается до следующего, а для любого k замощение A_k покрывает круг радиуса k, то задача была бы решена – мы взяли бы объединение плиток во всех этих замощениях.

Назовём замощение конечной области *хорошим*, если для любого R его можно продолжить до замощения, покрывающего круг радиуса R. Достаточно показать, что хорошее замощение можно для любого R продолжить до *хорошего* замощения, покрывающего круг радиуса R.

Пусть есть хорошее замощение. Рассмотрим все возможные способы продолжить его до такого замощения, что его плитки покрывают круг радиуса R и пересекаются с этим кругом. Этих способов конечное число. Если ни одно из этих продолжений не является хорошим замощением, то для каждого из них есть такой радиус, до которого нельзя продолжить. Берём максимум из этих радиусов и получаем, что исходное замощение также не хорошее.

B9 Следует из задач следующих циклов.

B10 Следует из задач следующих циклов.

B11 Прежде всего, пара слов о бесконечно декодируемых замощениях. Если операцию подстановки σ применить к фигуре A, получится к $\sigma(A)$. Если применить σ к $\sigma(A)$, получится $\sigma(\sigma(A))$, мы это обозначаем $\sigma^2(A)$.

1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	0	**1**	**1**	0	**1**	**1**	0	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	**1**	**1**	0	0	0	**1**	**1**	**1**
1	0	**1**	0	0	0	**1**	0	**1**
1	**1**	**1**	0	0	0	**1**	**1**	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	0	**1**	**1**	0	**1**	**1**	0	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

а) Дадим решение, использующее некоторые факты теории множеств, а именно то, что континуум больше счётного множества. Обозначим подстановку буквой s. Заметим, что $s^k(1)$ это квадрат размера $3^k \times 3^k$, составленный из восьми квадратов $s^{k-1}(1)$ и одного квадрата $s^{k-1}(0)$, все квадраты вида $s^k(0)$ заполнены нулями.

Если на клетчатой плоскости выложено замощение $3^k \times 3^k$ вида $s^k(1)$, то его можно продолжить до замощения $s^{k+1}(1)$ восемью способами, каждый способ соответствует одной из восьми крайних клеток квадрата 3×3 и при этом получаются различные сдвиги квадрата $3^{k+1} \times 3^{k+1}$. Обратите внимание, что мы рассматриваем не абстрактные квадраты, а квадраты, расположенные в плоскости.

Начнём с квадрата A_1 размера 1×1, в котором стоит единица, и будем каждый ход делать одно из таких продолжений, увеличивая заполненную область. Мы получим последовательность замощений $A_1, A_2, A_3, \ldots$

Такие последовательности кодируются рядом из цифр от 1 до 8, их континуум. Объединение квадратов A_i может быть или четвертью плоскости, или полуплоскостью, или всей плоскостью. Если мы получили не всю плоскость, значит, начиная с какого-то момента расширяли квадраты только в одну сторону.

Нетрудно понять, что тех последовательностей $\{A_i\}$, объединение которых замощает всю плоскость, также континуум. Получающиеся замощения плоскости будум называть *предельными*.

Покажем, что разные последовательности $\{A_i\}$ дают разные предельные замощения (обратите внимание, мы не утверждаем, что они не эквивалентны, то есть что не получаются друг из друга сдвигом).

Рассмотрим в предельном замощении квадраты $(3^k+2)\times(3^k+2)$, по краям которых стоят единицы, а внутри нули. Понятно, что центры всех таких квадратов сдвинуты относительно центра квадрата A_k на вектор, обе координаты которого кратны 3^k. Поэтому по предельному замощению можно определить координаты центра A^k по модулю 3^k. Но несложно убедиться, что координаты центра A_k отличаются от координат центра A_1 меньше, чем $3^k/2$, поэтому одинаковые предельные замощения могут давать только совпадающие последовательности квадратов.

Легко видеть, что каждое предельное замощение однозначно декодируемо, поэтому есть хотя бы континуум различных ковров Серпинского. А так как эквивалентными друг другу могут быть лишь счётное число ковров, то классов эквивалентности бесконечно.

b) Периодичный ковёр Серпинского – это тот, который состоит из одних нулей. Покажем, что все остальные ковры Серпинского непериодичны. Заметим, что если в ковре Серпинского есть хотя бы одна единица, то он для любого натурального k содержит квадрат $s^k(1)$, в центре которого есть квадрат $3^{k-1}\times 3^{k-1}$ из нулей, обрамлённый каёмкой толщины 1 из единиц. При сдвиге на любой ненулевой вектор, обе координаты которого меньше 3^{k-1}, эта каёмка будет пересекаться с квадратом из нулей, значит, хотя бы одна из координат вектора периодичности больше чем 3^{k-1}, и так для любого k. А значит, векторов периодичности нет.

c) *Ответ: нет.*

Пусть есть локальные правила размера n, выберем k таким, что $3^k > n$. Рассмотрим замощение A, состоящее из одних единиц. Оно не декодируемое, поэтому и замощение $s^k(A)$ не является бесконечно декодируемым. Покажем, что $s^k(A)$ допустимое.

$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$

Фрагмент замощения $s^k(A)$

$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$

$s^{k+1}(1)$

Видно, что любой квадрат со стороной не более чем n, встречающийся в $s^k(A)$, встречается в каком-то блоке, составленном из четырёх квадратов $s^k(1)$. Но этот блок содержится внутри $s^{k+1}(1)$, а значит содержится внутри ковров Серпинского и не содержит запрещённых квадратов.

B12 Пусть размер подстановки σ равен n. Замощение $\sigma(A)$ состоит из квадратов $n\times n$ – образов от плиткобукв. Любой квадрат 2×2 находится в квадрате $2n\times 2n$ – объединении четырёх таких квадратов, то есть $\sigma\left(\begin{smallmatrix}a_1 & a_2\\ a_3 & a_4\end{smallmatrix}\right)$. Так как квадрат $\begin{smallmatrix}a_1 & a_2\\ a_3 & a_4\end{smallmatrix}$ разрешённый и σ согласована с локальными правилами, то $\sigma\left(\begin{smallmatrix}a_1 & a_2\\ a_3 & a_4\end{smallmatrix}\right)$ не содержит запрещённых квадратов.

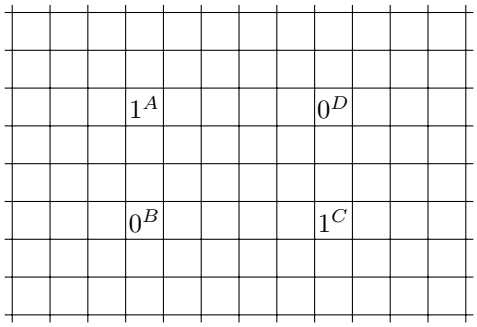
B13 Рассмотрим какую-нибудь плитко-букву a и последовательность квадратов

$$A_0 = a, A_1 = \sigma(a), A_2 = \sigma^2(a) \dots$$

В этой последовательность A_i имеет размер $n^i \times n_i$, а из предыдущей задачи следует, что все A_i – разрешённые. Из задачи **B8** следует, что есть разрешённое замощение всей плоскости.

B14 *Ответ: нет.* Покажем, что в алфавите $\{0,1\}$ у подстановки $\sigma(0) = \begin{smallmatrix}1&1\\1&1\end{smallmatrix}$, $\sigma(1) = \begin{smallmatrix}0&0\\0&0\end{smallmatrix}$ любо замощение переходит в неэквивалентное ему. Предположим противное: A – замощение, и $\sigma(A)$ эквивалентно A. Назовём *отрезком* длины k прямоугольник $1 \times (k+2)$ или $(k+2) \times 1$, у которого две крайние клетки одного цвета, а остальные k клеток – другого. Легко понять, что если в A есть отрезки и минимальная длина отрезка равна k_0, то в $\sigma(A)$ минимальная длина отрезка – $2k_0$. Значит, в A отрезков нет вообще. Поэтому каждая линия (горизонталь или вертикаль) либо одноцветная, либо одна её половина заполнена единицами, а другая – нулями.

Замощение A не одноцветное, значит в нём есть соседние 1 и 0. Не умаляя общности, 1 слева от 0. Тогда в $\sigma(A)$ есть 0, стоящий левее единицы. А так как в A нет отрезков, то найдутся вершины прямоугольника, раскрашенные в шахматном порядке, например, так:



Далее получаем, что все клетки в том же ряду, что и 1^A и левее, заполнены единицами, а все клетки в том же ряду, что 0^B и левее, заполнены нулями. Тогда прямой угол с вершиной в клетке 1^A, смотрящий вверх и налево, заполнен единицами. Но в таком случае в $\sigma(A)$ так же ориентированный угол заполнен нулями, чего не может быть.

Критерий на существование замощения. (набросок) У подстановки σ есть неподвижная точка тогда и только тогда, когда одна буква находится строго внутри своего образа ИЛИ две буквы находятся внутри своих образов на противоположных сторонах квадратов на одинаковом расстоянии от края ИЛИ четыре буквы появляются в углах своих образов во всех возможных позициях.

Пусть σ размера $k \times k$. Прежде всего заметим, что требование $S = \sigma(S)$ использовало бы задание системы координат, если же мы просто говорим, что S эквивалентно $\sigma(S)$, то этого не нужно. Квадратик 1×1 переходит в квадрат $k \times k$ композицией гомотетии и сдвига. Это снова гомотетия, её неподвижная точка где-то находится. Она может быть в центре клетки, на границе двух клеток или в узле сетки, эти три случая соответствуют трём описанным ситуациям.

С другой стороны, пусть $\sigma(a)$ содержит a строго внутри себя, например в позиции i, j. Тогда $\sigma^t(a)$ можно рассматривать как квадратный паттерн размера $k^t \times k^t$, и мы можем указать их как $-k^t i/(k-1) \cdots k^t(k-1-i)/(k-1)$ (аналогично по ординате) так, что a это клетка с координатами $0,0$. Квадрат растёт во все стороны, и в итоге любая клетка (x,y) покрыта каким-то квадратом. Каждый следующий квадрат содержит предыдущий, квадрат $\sigma^t(a)$ встречаестя в середине $\sigma^{t'}(a)$ при $t' \geq t$. поэтому можно определить замощение S в клетке (x,y) как букву $\sigma^t(a)(x,y)$ дял достаточно больших t. По построению $\sigma(S)$ будет сдвигом S.

Другие случаи (две буквы на сторонах и 4 буквы в углу) разбираются аналогично.

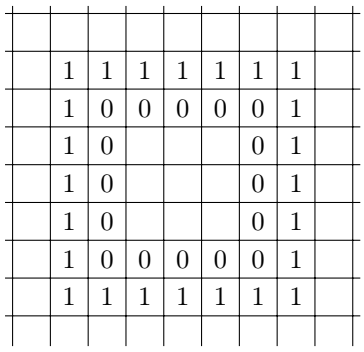
C. Примеры непериодичности

C1 а) Например, такая подстановка σ:

$$\boxed{1} \longrightarrow \begin{array}{|c|c|c|}\hline 1&1&1\\\hline 1&0&1\\\hline 1&1&1\\\hline\end{array} \qquad \boxed{0} \longrightarrow \begin{array}{|c|c|c|}\hline 0&0&0\\\hline 0&1&0\\\hline 0&0&0\\\hline\end{array}$$

То, что множество бесконечно декодируемых замощений не задаётся локальными правилами, доказывается так же, как и для ковров Серпинского.

Вот такую фигуру (а также если поменять местами 0 и 1) будем называть *двойной рамкой*.



Будем говорить, что размер двойной рамки на рисунке равен 5. Если в замощении встречается двойная рамка размера N, то у замощения не может быть вектора периодичности с абсолютными значениями координат меньшими N. Индукцией по k показывается, что $\sigma^k(0)$ и $\sigma^k(1)$ содержат двойные рамки размера 3^{k-1}.

b) Пусть, например, в алфавите всего одна буква.

C2 Пусть в плиточном алфавите 8 букв a_i, b_i, c_i, d_i, где индекс i принимает значения 1 и 2. Образы всех букв будут $\begin{smallmatrix} a_i & b_j \\ c_k & d_l \end{smallmatrix}$. Есть 16 способов выбрать индексы, можно взять разные способы для всех восьми букв.

C3 Следует из следующих задач.

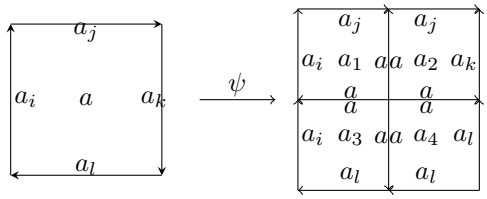
C4 Докажем непериодичность бесконечно декодируемого замощения A. Прежде всего заметим, что из свойства разделения образов следует, что обе координаты вектора периодичности v должны делиться на 2, а потом заметим, что вектор $v/2$ является вектором периодичности для замощения $\sigma^{-1}(A)$. Ненулевой целочисленный вектор можно делить пополам конечное число раз, после чего придём к противоречию.

C5 Обозначения: влево – W, вправо – E, вверх – N, вниз – S. Влево-вверх будем обозначать NW, аналогично с другими диагональными направлениями. Считаем, что у подстановки со свойством разделения образов каждая буква a_i плиточного алфавита A относится к одному из типов NW, NE, SW, SE.

Буквы нового алфавита B (декорации) будем рисовать как плитки, в центре которых написаны буквы из A, а на сторонах проведены стрелки и на каждой стороне написано по метке – букве из A. Таким образом, буква из B задаётся упорядоченной пятеркой букв из A и четырьмя битами (направления стрелок).

В дальнейшем будем говорить о типе плитки (NE, NW, SE, SW), типе стороны плитки (N, E, S, W в зависимости от направления стрелки), типе метки на стороне (NE, NW, SE, SW).

Подстановка ψ на алфавите B определяется следующим образом. Если в центре плитки записана буква a и какие-то метки по краям, и $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$, то в центре плиток образа записаны соответственные буквы алфавита, крайние рёбра образа 2×2 имеют такие же метки и направления, что и соответствующее ребро прообраза, а центральные четыре ребра исходят из центра квадрата 2×2 и на них метки a, смотри рисунок:



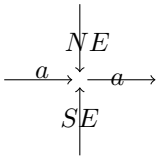
Смысл такой декорации в следующем: бесконечно декодируемое замощение состоит из блоков $2^k \times 2^k$, а каждый блок $2^k \times 2^k$ – из четырёх блоков $2^{k-1} \times 2^{k-1}$, и границы между этими четырьмя блоками образуют крест, на рёбрах которого написана одна и та же буква. Эти кресты разграничивают блоки большого размера друг от друга. В примере с коврами Серпинского такой границы не было, и локальными правилами нельзя было отличить границу большого блока от его средней части.

Локальные правила строились по такому принципу: изучалось, что в бесконечно декодируемом замощении может находиться на стыке двух и четырёх плиток, и эти свойства записывались в правила. Нужно, с одной стороны, записать достаточно правил, чтобы можно было определить декодирование, а с другой стороны – проверить, что после декодирования все записанные правила выполняются. По этой причине мы не используем больших локальных правил, про далёкие плитки: сложно проверять их выполнение после декодирования.

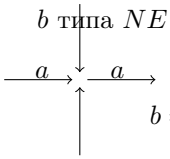
Будем говорить, что направление NE симметрично относительно вертикали направлению NW, а SW симметрично относительно вертикали направлению SE. Симметрия относительно горизонтали определяется аналогично.

Итак, локальные правила:

1) На соседних плитках смежные стороны имеют одинаковые направление и метку (то есть можно говорить о направлении и метке ребра во всём замощении).
2) Граничить по вертикальной стороне могут только плитки типов, симметричных относительно вертикали. Граничить по горизонтальной стороне могут только плитки типов, симметричных относительно горизонтали.
3) Узлы между типов могут иметь только такие степени вхождения: 4 исходят или 3 входит и одно исходит.
4) Если из узла 4 ребра исходят, то на них должны быть одинаковые метки.
5) Если слева-сверху от узла находится плитка типа NW, назовём такой узел *центральным*. Потребуем, чтобы из центрального узла выходило 4 ребра. Если на этих рёбрах метки a, и при этом $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$, то в центре плитки к северо-западу от узла должна быть буква a_1, аналогично про три другие плитки.
6) В узле типа 3-1 есть исходящее ребро, *центральное входящее* ребро, и два *боковых входящих*. Потребуем, чтобы метки на центральном входящем и на исходящем совпадали, а также чтобы типы меток на боковых входящих были симметричны относительно исходящего ребра. Например так:

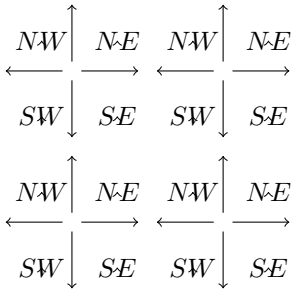


7) Пусть есть узел типа $3-1$, на исходящем ребре v_1 метка a, на боковом входящем ребре v_2 метка b и $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$.
Если угол между типом b и направлением v_2 равен $135°$ (например, v_2 идёт вниз, а b типа NE), то угол между v_1 и типом b должен равняться $45°$, а сама буква b должна встречаться в $\sigma(a)$ на месте, соответствующем типу b.



$b = a_2$, где a_2 – правая верхняя (NE) буква в $\sigma(a)$

Анализ разрешённых замощений. Теперь нужно понять, какие бывают замощения с данными локальными правилами. Из 1) получаем, что плоскость разбивается на квадраты 2×2, в каждом из которых типы плиток $\begin{smallmatrix} NW & NE \\ SW & SE \end{smallmatrix}$. Далее будем их называть *базовыми блоками*. Из 5) и 4) следует, что центры базовых блоков – центральные узлы, из них всех выходит по 4 стрелки с одинаковыми буквами.



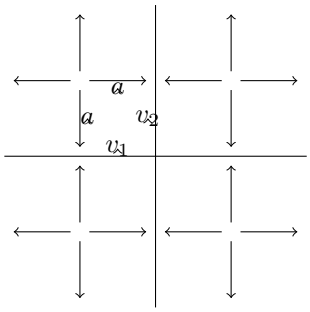
Все узлы разделим на центральные, *боковые* (те, в которые на картинке выше ведут по 2 стрелки) и остальные. Из 3) следует, что середины сторон базовых блоков (боковые узлы) имеют тип $3-1$, а вместе с 6) это даёт, что на каждой стороне базового блока стрелки сонаправлены и на них одинаковые метки.

Вместе со свойством 4) это даёт, что каждый базовый блок является образом какой-то буквы при подстановке ψ, таким образом, однозначно определён переход от разрешённого замощения T к $\psi^{-1}(T)$. Это замощение можно получить из T, стирая линии внутри базовых блоков и записывая внутрь блока ту букву, которая является меткой всех рёбер, выходящих из его центра.

Нужно проверить для $\psi^{-1}(T)$ свойства $1) - -7)$. Свойства 1), 3), 4) и 6) выполняются автоматически, так как новых ситуаций в узлах (какие бетки и стрелки написаны на входящих рёбрах) не возникает.

Для свойства 2) надо проверить, что любые два базовых блока, имеющие общую сторону, декодируются в буквы симметричных типов. Но тип после декодирования совпадает с типом метки, написанной на внутреннем кресте базового блока. Локальное правило 5) гарантирует, что метки у двух блоков симметричны, и после декодирования выполняется 2).

А значит, базовые блоки объединяются в четвёрки, которые после декодирования имеют вид $\begin{smallmatrix} NW & NE \\ SW & SE \end{smallmatrix}$. Рассмотрим одну такую четвёрку.



Метка a имеет тип NW, поэтому, согласно 6), ребро v_1 направлено влево, а v_2 – вверх. Значит, v_1 и v_2 выходят из узла, из которого 4 выходящих ребра. Из 4) следует, что метки на этих рёбрах совпадают. Также из 6) следует, что в верхнем левом углу образа этой метки при σ стоит a. Аналогично и про остальные базовые блоки, а значит, после декодирования выполняется свойство 5). Итак, декодированное замощение является разрешённым, а значит, все разрешённые замощения – бесконечно декодируемые.

Вообще говоря, задачу мы пока решили не до конца. Мы не показали, что *каждое* бесконечно декодируемое при помощи σ замощение допускает разрешённую декорацию. Можно показать, что такая декорация существует для тех замощений, у которых каждая плитка находится строго внутри некоторого блока вида $\sigma^k(a_i)$. Можно описать остальные замощения и слегка подправить нашу конструкцию, оставляем это читателю в качестве упражнения.

C6 Эту задачу мы оставляем в качестве упражнения. Как тебе такое, Питер Шольц?

C7 Воспользуемся задачей $C5$. Пусть наша подстановка σ над алфавитом A. Возьмём подстановку τ 2×2 с разделением образов над алфавитом B (такая существует, см. задачу $C2$). Рассмотрим алфавит C размера $|A| \cdot |B|$, буквы которого – пары букв $(a_i, b_j) | a_i \in A, b_j \in B$. Определим на нём подстановку ψ размера 2×2, заданную так: $(a, b) \to \begin{smallmatrix} (a_i,b_j) & (a_k,b_l) \\ (a_m,b_n) & (a_p,b_r) \end{smallmatrix}$, где $\sigma(a) = \begin{smallmatrix} a_i & a_k \\ a_m & a_p \end{smallmatrix}$ и $\tau(b) = \begin{smallmatrix} b_j & b_l \\ b_n & b_r \end{smallmatrix}$. Легко видеть, что она является декорацией σ и у неё есть свойство разделения образов.

D. Различные формализмы и перевод непериодичности на другие языки.

D1 Допустим, есть апериодический набор в формализме Ванга. Введем для каждой буквы на ребре противоположную. Теперь в каждой плитке набора поменяем буквы верхнего и правого ребра на противоположные. Получится набор в другом формализме, причем каждому замощению в одном наборе соответствует замощение в другом. То есть апериодичность сохраняется. Аналогично в другую сторону.

D2 Назовем многоугольник *квадратно-составленным*, если он представляет собой фигуру полимино, составленную из единичных квадратов (связную и без дыр внутри). Постройте апериодический набор из квадратно-составленных многоугольников, которые можно поворачивать и переворачивать. *Указание.* Такой набор можно построить, используя набор Робинсона. Сначала представим что каждая плитка это квадрат $k \times k$ для большого k. Реализуем каждую засечку на стороне квадрата из набора робинсона (их три вида) в виде выреза по контуру из

D3 а) *Ответ: нет.*

b) Пусть теперь по-прежнему плитки разрешается прикладывать по правилам дополняющих цветов, но перевернутые плитки не могут иметь общую сторону. Докажите, что существует апериодический набор.

E. Декорации

E1. а) алфавит $\{a_1, a_2, b\}$; запретим $\{ba_1, a_2b, bb, a_2a_1\}$.

b) Алфавит $\{a_1, a_2, b\}$; запретим горизонтальные пары $\{ba_1, a_2b, bb, a_2a_1\}$, вертикальные пары $\{\begin{smallmatrix} b \\ a_2 \end{smallmatrix}, \begin{smallmatrix} a_1 \\ b \end{smallmatrix}, \begin{smallmatrix} ba_2 \\ ba_1 \end{smallmatrix}\}$, а также $\{\begin{smallmatrix} a_1 & a_2 \\ a_2 \end{smallmatrix}\}$.

E2. Плитками без b (декорированными) можно замостить сколь угодно большой квадрат. Согласно задаче **B8**, можно замостить всю плоскость, не используя b.

E3.

a) *Ответ: нет.* Допустим противное, пусть k – размер максимального запрета. Рассмотрим замощение, в котором одна компонента связности – горизонтальный путь длины k, и другое замощение – путь длины $k+1$. У этих замощений одинаковый набор паттернов размера $k \times k$, поэтому они оба должны быть или разрешены, или запрещены. А должно быть только одно из них.

b) алфавит $\{a, b_1, b_2\}$; запреты $\{ab_2, b_1b_1, b_2b_2, b_1a\}$.

c) Набросок одного из возможных решений. Пусть декорации изображают остовный лес для связной компоненты, то есть объединение непересекающихся деревьев, у каждого дерева отмечен корень и каждая вершина компоненты входит ровно в одно дерево. Наложим условие на чётность числа вершин в компоненте: каждая вершина может считать по модулю 2 число вершин у своих сыновей, прибавлять единицу и передавать результат родителю (считаем, что дальше от корня находятся сыновья, а ближе к корню – родитель). С одной стороны, в каждой связной компоненте есть остовное дерево с чётным числом вершин, которое можно так раскрасить. С другой – в каждом разрешённом замощении каждая связная компонента состоит из одного или нескольких таких деревьев, т.е. содержит чётное число вершин.

E4*. В размерности 1 это просто: алфавит $\{a, b_1, b_2\}$; запреты $\{ab_2, b_1b_1, b_2b_2, b_2a\}$.

В размерности 2 это тоже возможно, но весьма и весьма нетривиально :-)

E5. Пример: возьмём такой набор плиток, чтобы с их помощью можно было нарисовать на плоскости любой граф. Тогда декорацией можно задать правильную раскрашиваемость графа в 3 цвета.

E6. a) Все квадраты 2×2 появляются или и там и там, или нигде.

b) Пусть k – размер декорированного алфавита. Декораций границы квадрата $n \times n$ не более чем $k^{4(n-1)}$.

c) Рассмотрим множество замощений, где c-шки образуют колонку. Смотрим множество паттернов $n \times n$, которые могут быть слева от колонки. Их хотя бы 2^{n^2} (декорации всевозможных замощений из a и b). При достаточно большом n (параметр k фиксирован) есть два таких замощения, что у них совпадают границы, и по пункту a) одно можно заменить на второе. Тогда мы получим разрешённое, но не симметричное.

d) Если $\mathcal{S}$ – такое множество замощений, то должно существовать такое k, что для любого n среди любого набора из k^n замощений квадрата $n \times n$ можно выбрать 2 и одинаково продолжить до замощения всей плоскости.

Tilings: substitutions and decorations

Alexei Belov, Pierre Guillon, Ilya Ivanov-Pogodaev, Ivan Mitrofanov

This project is devoted to plane tilings. Usually, if we can tile a plane with some types of tiles, then we use construction which structure is periodic. Correctly, a tiling is called *periodical* if it doesn't change after shift on non-zero distance. In 1961 chinese mathematician Hao Wang have stated the following problem:

Consider unit squares. Each square's side is colored by one color of several possible ones. Consider some types of these squares. We can attach any square to another side to side if these sides have the same color. Suppose that we can use unlimited number of each type's squares. Is it true that if we can tile a plane then we can do it periodically?

Firstly Wang expected that the answer is positive, namely if there exists some tiling then there is a periodic one. But in 1966 Robert Berger (student of Wang) have constructed a set consisting of 20426 squares such that there exist non periodical tilings only. Lately Berger reduced his set to 104 squares, and in 1971 Raphael Robinson greatly simplified the construction and introduced a set of six poligons such that one can tile a plane using them only non periodically.

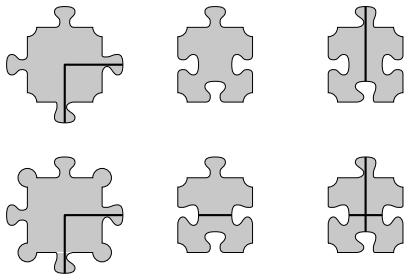


FIGURE 1. Robinson's tiles.

This problem has some philosophical background. The point is to reach global condition (non periodicity) using local sources (boundary conditions). There are many such problems. How to organize a computation network such that any local fault can not violate global processes. Or how interaction of molecules leads to crystals growing.

In this project we will study some ideas and methods to solve such problems in various settings. The main problem of first half is to construct a set of polygons such that there exist non periodical tilings only (problem B10). In fact, this problem can be reduced to constuction of local rules: boundary conditions which define when we can attach tiles to each other. This construction uses some ideas. In B and C we study some tricks that can be used to construct aperiodic tilesets.

A. One dimensional case

Consider two-side infinite tape which consists of cells (equal squares). We will assign one letter of the finite alphabet for each cell. A cell with assigned letter is called a *tile*.

If every cell contains some letter (or the tape is covered by non intersecting tiles) then we say that this is *the tiling*. A tiling is called *periodical* if it doesn't change after shift on non zero integer p. It is easy to see that periodical tiling is actually periodical repeat of some combination of p tiles. This combination is called *period* of tiling, p is length of period.

A *forbidden word* or *local rule* is a combination of several adjacent tiles. We will consider tilings which contain no forbidden words. In notations we use letters of a finite alphabet to denote tiles and we do words to denote combinations of tiles. Tilings which contain no forbidden words are called *permitted* ones. Further we assume that the number of local rules is finite.

Two tiling which transforms to each other after some shift are called *equivalent*. Below we consider such tilings as the same.

A1 Consider an alphabet $\{0, 1\}$. The word 01 is forbidden. How many non-equivalent tilings exist?

A2 Show that for two letters there exists a non periodical tiling.

A3 Construct a finite set of forbidden words in the alphabet $\{a, b, c\}$, such that the periodic tiling with period abc is the only permitted tiling.

A4 Does there exist a set of local rules such that there are exactly 100 nonequivalent permitted tilings?

A5 Let A be a finite word. Prove that there exists a of forbidden words such that the tiling with period A is the only permitted one.

A6 Let A be an aperiodic tiling. Prove that there is no a finite set of forbidden words such that A is permitted and all the permitted tilings are equivalent to A.

A7 Consider an alphabet with size n. Suppose that there are k forbidden words, and each of them has length 2. Also, there are no permitted tilings. Find the minimal possible k.

B. Dimension two: local rules and substitutions

Conclusion from one dimensional case. In one dimensional case forbidden word is some kind of local condition. Using these conditions we want to obtain some global property. But in one dimensional case finite number of local rules does not allow us to force non periodical tilings.

Let us proceed to two dimensional case. We will start with basic definitions and notation.

Consider an infinite square grid and a finite alphabet L (*alphabet of tiles*). We will write letters of L into cells of an infinite square grid, one letter to one cell. This alignment is called a *tiling*.

Similarly to one dimensional case, a tiling is called *periodic*, if it doesn't change after translation by a non zero vector (a, b), and is called *aperiodic* in the opposite case.

Equivalence of tilings. Definition. Consider two tilings S_1 and S_2. Suppose that we can translate S_1 by integer vector and obtain S_2. In this case we say that S_1 and S_2 are *equivalent*. *Remark.* Different tilings of finite regions are never equivalent.

Local rules. Definition. Let $n > 1$ be an integer. Consider a set of all squares $n \times n$, compiled from letter-tiles. Formally, this set is L^{n^2} (set of all $(n^2)-$tuples of letters from L). Let R be a subset of this set. So, R is a set of several squares 2×2 compiled by L letters. Let us call these squares as *forbidden* ones. A tiling is called *permitted by* R if there are no forbidden squares in the tiling. The squares from R are also called *local rules*, the number n is the *size* of the local rules.

Using local rules we can force some properties of permitted tilings. Let's do some practice.

B1 Suppose that the alphabet contains only two letters (black and white squares). Construct local rules such that the chessboard tiling is the only permitted tiling.

B2 Suppose that the alphabet contains two letters and eight squares 2×2 are forbidden (look at the picture). For given m and n, how many permitted tilings of a $m \times n$ rectangle exist?

1	1
0	1

1	1
1	0

1	0
1	1

0	1
1	1

1	0
0	0

0	1
0	0

0	0
0	1

0	0
1	0

B3 Suppose that the alphabet contains two letters. The set of local rules is the same as in the previous problem, and also the square with 1 on main diagonal (see picture below) is forbidden. Classify all different permitted tilings of the infinite plane.

1	1
0	1

1	1
1	0

1	0
1	1

0	1
1	1

1	0
0	0

0	1
0	0

0	0
0	1

0	0
1	0

1	0
0	1

B4 Suppose that alphabet contains four letters and a 2×2 square is permitted if and only if it consists of four different letters. How many permitted tilings do exist for the rectangle $m \times n$?

B5 Consider a binary alphabet. Suppose that there are k forbidden squares 2×2 and suppose that there are no permitted tilings. Find the minimal possible k.

B6 Consider some set of local rules in the alphabet $\{0, 1\}$. Suppose that the tiling on picture below is permitted (other cells except these nine contain 0). Prove that there exists infinite number of nonequivalent permitted tilings.

0	1	0
1	0	1
1	1	1

This problem show that sometimes[1] it is not possible to determine one precise tiling by local rules. But if we cannot force one tiling, maybe we can determine some set of similar tilings? We say that some set of tilings is *defined by local rules* if tilings from this set are the only permitted tilings according with these local rules.

B7 A *frame* is a figure consisting of $2(m + n) - 4$ boundary cells of a rectangle $m \times n$ for some $m, n > 1$. We call a $\{0; 1\}$-tiling *pretty*, if union of some (maybe infinite) set of frames is filled with units, and zeroes are placed in the remaining cells. Suppose we have a finite set of local rules such that all pretty tilings are permitted. Prove that there are infinitely many non-equivalent permitted not pretty tilings.

B8 Suppose we have a set of local rules, and suppose that for any positive r we can tile an area including circle of radius r such that there are no forbidden squares. Prove that we can tile the whole plane with the same condition.

[1] Further we will prove that for aperiodic tilings it is *never* possible.

Using local rules we can obtain really complicated tilings. For example, we can force all the permitted tilings to be aperiodic. It is hard to solve this problem now and we recommend to return to it in C-part and use some additional methods.

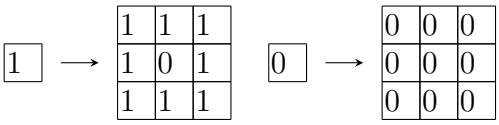
B9* Construct a set of local rules such that all permitted tilings are non periodic.

B10* Construct a finite set of polygons such that all tilings are non-periodic. All polygons can be rotated and reflected; they should be arranged without holes or overlaps.

Definition. Suppose that for any letter in the alphabet L corresponds a some square $k \times k$ compiled by letters of this alphabet. This correspondence is called a *substitution*.

For a given substitution σ and a tiling A of some (finite or infinite) region we can construct a new tiling $\sigma(A)$ by simultaneous replacement of tile-letters by corresponding squares $k \times k$. Starting with one tile and iterating this procedure, we obtain tilings of bigger and bigger squares.

Definition. Consider a $k \times k$ substitution σ. Suppose that a tiling S can be uniquely divided by horizontal and vertical lines to squares $k \times k$ such that each square is image of some letter (any square is $\sigma(a)$ for some letter a). In this case we can write a letter instead of each $k \times k$ square (a instead of $\sigma(a)$). Thus we obtain a new tiling $\sigma^{-1}(S)$. If $\sigma^{-1}(S)$ is defined in a unique way, we say that for tiling S we can find an inverse image $\sigma^{-1}(S)$. A tiling is called *infinitely decodable by* σ if one can find inverse image any number of times.



B11 Consider the substitution above. An infinitely decodable tiling for this substitution is called a *Sierpinski carpet*.

a) Prove that there are infinitely many nonequivalent Sierpinski carpets.

b) Prove that all Sierpinski carpets besides one of them are aperiodic tilings.

c) Is the set of all Sierpinski carpets defined by local rules?

If one wants to define infinitely decodable tilings with local rules, it is natural to require that a substitution map permitted tilings only to permitted tilings.

Definition. We say that a substitution σ *agrees with local rules* R of size k if the following conditions hold:

1) the square $\sigma(a)$ is permitted for every letter a;

2) if X is permitted square then the $2n \times 2n$ square $\sigma(X)$ contains only permitted $k \times k$ squares.

B12 Consider some local rules R. Suppose that $k = 2$ (all forbidden squares are 2×2). Also, suppose that a $N \times N$ square A is permitted (it contains no forbidden 2×2 squares). Let a substitution σ agree with local rules. Prove that the square $\sigma(A)$ is also permitted.

B13 Suppose that substitution σ agrees with the local rules of size 2. Prove that there exists a permitted tiling.

B14 Consider a substitution σ. Does there exist a tiling S such that $\sigma(S)$ is equivalent to S? Find sufficient conditions on σ for existence of such a tiling.

C. Examples of non periodicity

Definition. A tileset is *aperiodic*, if it admits at least one tiling of the plane but doesn't admit a periodic one.

Conclusions from parts A and B. We want to find a set of tilings such that it is defined by local rules and contains only aperiodical tilings. There is no such an example in one-dimensional case (why?). The simplest two-dimensional examples we know are infinitely decodable tilings for some substitutions.

Not any substitution is suitable.

C1 a) Find a substitution such that all infinitely decodable tilings are aperiodical, but the set of them is not defined by local rules.

b) Find a substitution such that all infinitely decodable tilings are periodical.

It is not easy to find a suitable substitution "from scratch", so we'll "improve" not suitable ones.

Transition to another alphabet. Decorations. Consider a tile alphabet $a, b, c \ldots$. We can make finite number of duplicates (shades) for each letter and consider the extended alphabet of tiles $a_1, \ldots a_k, b_1, \ldots b_k, c_1, \ldots c_k, \ldots$ Now we can set up local rules for this extended alphabet. After that we can take permitted tilings and ignore the shades. This approach is called *setting up decorations*.

Definition. Let A_1 and A_2 be two tile alphabets and let σ_1 and σ_2 be two substitutions in alphabets A_1 and A_2 respectively. We call the substitution σ_2 *a decoration* for σ_1 if the following conditions are satisfied:

1) there exists a mapping f from A_2 to A_1;

2) if $\sigma_2(a) = M$ is a square made of letters from A_2, then $\sigma_1(f(a)) = f(M)$.

We consider f as "forgetting the shade", and $f(M)$ is a square obtained from M by applying f to each letter.

Our main goal is to prove that a given substitution can be decorated in such a way that the set of infinitely decodable tilings is defined by local rules.

Firstly we deal with some useful special cases. Consider a 2×2 substitution σ. If a is a letter, then $\sigma(a)$ is a 2×2 square which consists of four letters. We assume that different letters correspond to different 2×2 squares.

Images separating. Definition. Let us define σ_{UL} mapping. It maps letter a to the upper left corner of the square $\sigma(a)$. Similarly we can define mappings σ_{DL}, σ_{UR}, σ_{DR}. We say that the substitution *separate the images* (or has property of separating images) if every letter occurs exactly at one image of these four mappings.

C2 Construct a substitution with property of separating images.

The property of separating images helps us to construct local rules. Firstly we try to archive the goal for particular case – some fixed substitution. After this, we will study substitutions with separating images. And finally we will proceed to the common case.

The idea of construction. Firstly try to color sides of squares in different colors and formulate local rules in terms of these colors combinations. The main goal is to obtain the property that any permitted tiling can be decoded that is to proceed to next level of hierarchy. A substitution make this transition.

C3 Find some substitution σ and local rules such that any permitted tiling S can be decoded and tiling $\sigma^{-1}(S)$ is also permitted. Prove that any permitted tiling is aperiodical.

C4 Consider a 2×2 substitution σ with property of separating images. Suppose that there exist local rules R such that for any permitted tiling S there exists inverse image $\sigma^{-1}(S)$ which is also permitted by the same local rules R. Prove that any permitted tiling is aperiodic.

C5 Consider a 2×2 substitution with property of separating images. Prove that there is a decoration such that the set of infinitely decodable tilings is defined by local rules.

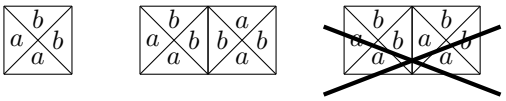
C6 Consider a 3×3 substitution with property of separating images. Prove that there is a decoration such that the set of infinitely decodable tilings is defined by local rules.

C7 Consider a 2×2 substitution (maybe there is no separating images property). Prove that there is a decoration such that the set of infinitely decodable tilings is defined by local rules.

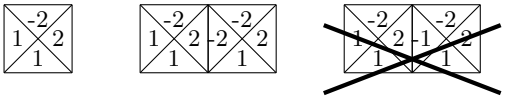
D. Other formalisms and transitions of non-periodicity to other languages

In addition to local rules and forbidden squares, there are other formalisms to specify tilings. Sometimes the interaction of different formalisms is useful.

Wang tiles formalism. There are finitely many colors, a *Wang tile* is a unit square with a color on each side. There is a finite set of Wang tiles, colors of common sides should match in tilings of the plane.



Complementary colors formalism. There is a finite set of non-zero integers (we call them colors). A tile is a unit square with an integer on each side. There is a finite set of tiles, numbers on common sides should be opposite.



D1 Prove that Wang's formalisms and complementary colors formalism are equivalent, i.e. if there is an aperiodic tileset in one formalism, then there is a corresponding aperiodic tileset in the other.

Sometimes a tileset along with any tile contains the rotated on 90 degree tile. In this case we say that we can rotate tiles.

Consider a tile A with integers (a_1, a_2, a_3, a_4) written on its sides *clockwise*. The tile with $(-a_3, -a_2, -a_1, -a_4)$ integers written on the same sides is called *flipped* tile (with respect to A). If a tileset contains the flipped tile for every tile then we say that we can flip tiles.

D2 We call a polygon *square-composed*, if it is connected polymino composed of unit squares without holes inside. Construct an aperiodic set of square-composed polygons such that with every polygon Φ the tileset contains all 8 rotations and reflections of Φ.

D3 Suppose that a tileset in complementary colors formalism with any tiles contains all its rotated and flipped tiles. a) Can such a tileset be aperiodic?

b) Add extra rule to the formalism: a tile can not be a side-neighbor of its flipped tile. Prove that such a tileset can be aperiodic.

Tilings: substitutions and decorations. Solutions.

A. One dimensional case

A1 *Answer: 3.*

It is clear that two tilings with all identical letters (ones or zeros) are permitted. If there are both 1 and 0, then there must be adjacent 1 and 0, and 1 is on the left. It's clear that only 1's can be to the left of 1, and only 0's can be to the right of 0.

1	1	1	1	1	1	1	1	1	1	1	1

0	0	0	0	0	0	0	0	0	0	0	0

1	1	1	1	1	1	0	0	0	0	0	0

A2 There are a lot of examples. For instance, one 0, and the other cells are filled with 1-s. Then for any nonzero shift this zero will map to a different one.

1	1	1	1	1	0	1	1	1	1	1	1

A3 See for yourself that if you forbid the words aa, ac, ba, bb, cb, and cc, then any letter uniquely forces both of its neighbours.

A4 *Answer: yes.* For example, we can forbid all tilings except 100 periodic sequences with periods $01, 001, \ldots, 0^{100}1$. We forbid $11, 0^{101}$, and $100 \cdot 99$ words of form 10^a10^b1 for all $a \neq b$ from 1 to 100.
The first two rules force that the number of zeroes between two neighbouring 1's is from 1 to 100. The rest of them guarantee that any two neighbouring blocks of zeroes are equal.

A5 Recall that a cyclic shift of a word $a_1a_2 \ldots a_n$ is any one of the words $a_{i+1}a_{i+2} \ldots a_na_1a_2 \ldots a_i$ for $0 \leqslant i < n$. Let $|A| = n$, and let k be the size of the alphabet. There are k^n words of length n; we forbid all of them that are not cyclic shifts of A. In all cyclic shifts of A, the number of letters of each type is the same, so in any permitted tiling the tiles at the distance n must coincide, that is, the permitted tiling is periodic with period length n. If some cyclic shift of A is a period, then A is also a period.

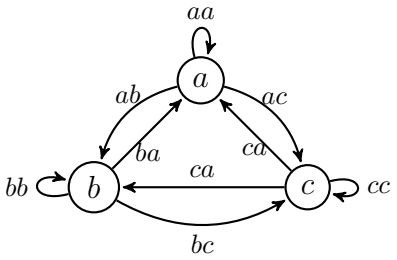
A6 We show that for any finite set of local rules that admit at least one permitted tiling of the line, there exists a permitted periodic tiling. Let N be the length of the largest of the forbidden words. Consider a permitted tiling, and by pigeonhole principle, find in it two disjoint occurrences of the same block of length N; we denote it U, and the part between the two occurrences is denoted by W.

$\cdots$	U	W	U	$\cdots$

Then the tiling with period UW is permitted. Indeed, all the rectangles of length no greater than N occur in the original tiling (and therefore do not contain forbidden ones), and we do not have local rules longer than N.

$\cdots$	W	U	W	U	W	$\cdots$

A7 *Answer:* $n(n+1)/2$.
example: Let the alphabet consist of numbers from 1 to n and the words ab are forbidden for $a \geqslant b$. Then it will not be possible to tile a block that is longer than n, because when moving from left to right, each letter should be larger than the previous one. *Estimate:* Forbidden words of length 2 are constraints of adjacent pairs of letters. Draw a complete directed graph on n vertices (with loops):



Each forbidden word of length 2 removes one edge in this graph. It is easy to understand that if there is at least one cycle left, then an infinite path along this cycle is a a permitted periodic tiling. Now we show by induction on n that if there are no oriented cycles in the oriented graph, then the edges are not more than $n(n-1)/2$. Step from n to $n+1$: if there is at least one edge from each vertex, then there is a cycle. So there is at least one vertex without outgoing edge; removing it removes at most n (incoming) edges, and leaves us with a graph with $n-1$ vertices, to which we can apply the induction hypothesis, and get $n + n(n-1)/2$ edges, which is the wanted value. And the base $n = 1$ is obvious.

B. Dimension two: local rules and substitutions

B1 It is enough to forbid all the 2×2-squares except for the two chess-colored ones. Then in the permitted tiling, white cells will border only with black, and black – only with white. Conversely, the chessboard tiling is permitted.

B2 *Answer:* 2^{m+n-1}. Note that the allowed 2×2-squares are those with an even number of 1-s. Hence, each cell is uniquely determined by its three (left, top, left-top) neighbours. Therefore, for any filling of the left column and of the top row of the rectangle, the remaining cells can be filled in a unique way. Moreover, all possible binary (left, top, left-top) triples are extendable, so that every filling of the left column and of the top row is extendable as a permitted rectangle.

a_2	a_3
a_1	?

B3 *Answer: tilings by rows, tiling by columns and one tiling by quadrants.*

0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0

0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1
0	1	1	1	0	0	0	1

0	0	0	0	1	1	1	1
0	0	0	0	1	1	1	1
0	0	0	0	1	1	1	1
0	0	0	**0**	**1**	1	1	1
1	1	1	**1**	**0**	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0
1	1	1	1	0	0	0	0

We consider two cases: whether a square with units on the side diagonal (bold) appears in the tiling or not.
It appears. First, the "cross"of width 2 with the center in this square is uniquely filled, then one by one the remaining cells are filled and we get the tiling by the quadrants.

It does not. Any 2×2-square is either monochrome, or the boundary between zeroes and ones divides a square into two dominoes. If the tiling is not monochrome, then there are neighbours on the side 0 and 1. Further, the strip of width 2 containing them is uniquely filled: it is either two monochrome rows or columns. In the first case, it turns out that all the horizontals are monochrome; in the second - that all verticals are monochrome.

B4 *Answer:* $6(2^n + 2^m - 4)$.

In two vertical dominoes located at distance one, the letters can be located

in such way: | a | | a |
|---|---|---|
| b | | b |

or in such way: | a | | b |
|---|---|---|
| b | | a |

We call a line (horizontal or vertical) *striped*, if in it two types of letters alternate. It is easy to see that if a line is striped, then all the lines parallel to it are also striped.

c	d	c	d	c	d	c	d	c	d	c	d
a	b	a	b	a	b	a	b	a	b	a	b

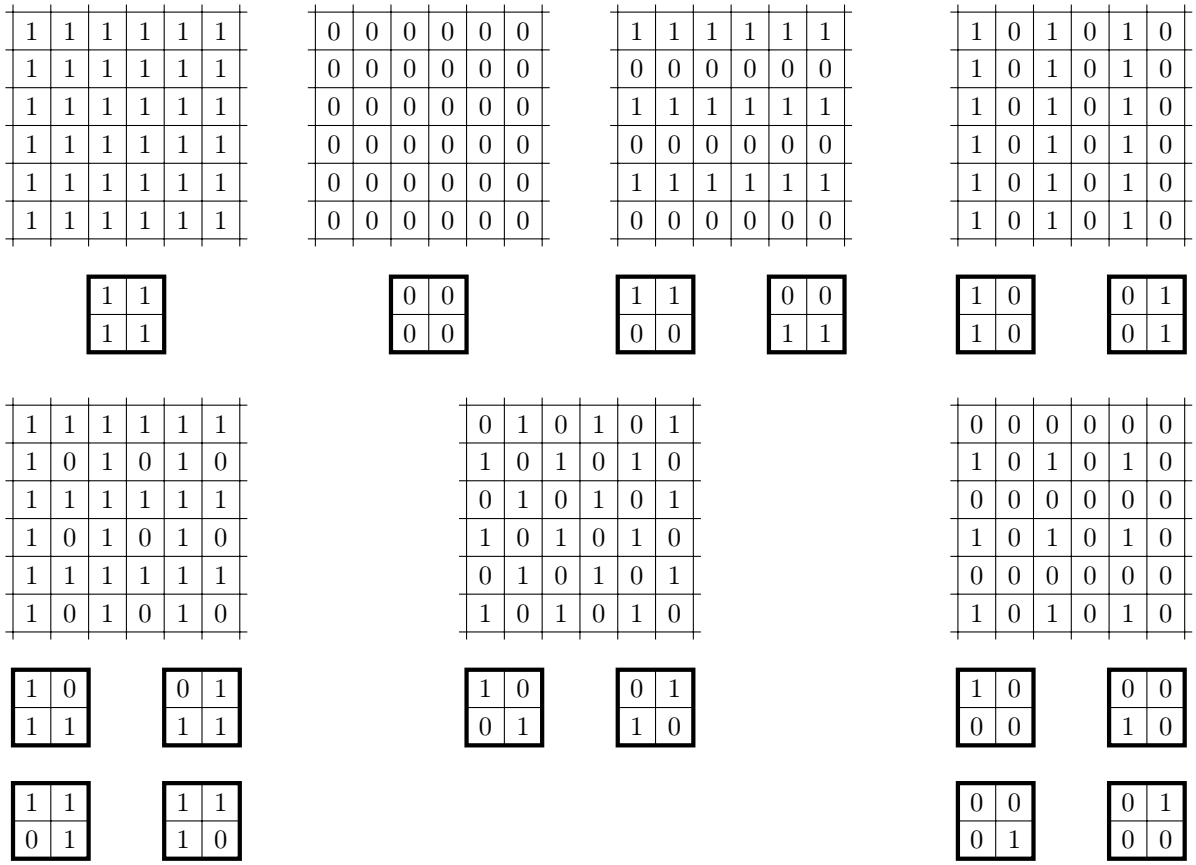
We show that there is at least one striped line. Suppose the top row of the table is not striped, then it has different letters (let a and b) at a distance of 2.

			a		b		
			b		a		
			a		b		
			b		a		

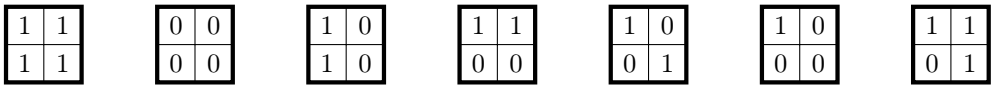
Then it is clear that these cells are in striped columns.
There are $6 \cdot 2^n$ tilings with striped columns and $6 \cdot 2^m$ tilings with striped rows. 24 of them are counted twice.

B5 *Answer: 7.*

There are 16 squares 2×2. They are divided into 7 groups, and in order to prohibit 7 periodic tilings, it is necessary to ban at least one square from each group (we illustrate for each group a periodic tiling which would be permitted no square of the group were forbidden).



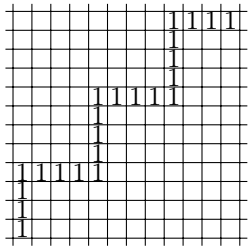
Example of 7 forbidden squares:



The 4 last local rules force that there is no zero below a one. Together with the first rule, this gives that ones cannot be in adjacent columns, and together with the second – that zeroes cannot be in adjacent columns. Then the only possible tiling is a periodic tiling with alternating columns, but the third local rule also prohibits it.

B6 Let $N \times N$ be the size of the largest local rule. It's clear that if we fill the entire plane with zeroes and draw several occurrences of the allowed picture so that the distance between any two of them is greater than N, then we obtain a permitted tiling.

B7 A *ladder* is an infinite stepped figure of units, we have drawn a fragment of the ladder with step 4 (all empty cells are filled with zeros).



If N is the size of the largest local rule, then all ladders with a step greater than N are permitted, because all the $N \times N$ patterns already appear in some large frame, so they are permitted.

Since a ladder is not a union of frames, it is not a beautiful tiling.

B8 At first glance it seems that there is nothing to prove here, since the plane is, in some way, a circle of infinite radius. But in fact, from the fact that we know how to cover *arbitrarily large* circle it does not follow automatically that we can cover an *infinitely large* circle.

Extra problem about types of infinity. Kashchei the Immortal (russian folklore villain) uses a magical currency exchange. It allows to change one gem for any positive integer number of gold coins, or one gold coin for any number of silver coins, or one silver coins for any number of copper coins. Initially, Kashchei has one hundred of gems. To maintain his immortality, Kashchei has to spend one copper coin per day Suppose he has no any other income. Will he be able to live for a billion of years? A googol of years? For eternity?

Let's return to the problem. If we add a few more tiles to a tiling A of some finite region and obtain a tiling B, we say that the tiling A *can be extended* to B.
If we find an infinite sequence of tilings A_1, A_2, A_3 such that each previous tiling can be extended to the next one, and for any k the tiling A_k covers a circle of radius k with center in $(0, 0)$, then we win – we take the union of these tilings.

We call a tiling of a finite region *good* if for any R it can be extended to a tiling, covering a disc of radius R with center at zero. It suffices to show that a good tiling can be extended for any R to a good tiling that covers a circle of radius R.

Let D be a good tiling. Consider all possible ways to extend it to a tiling that covers a circle of radius R. There is a finite number of such extensions; if none of these extensions is a good tiling, then for each of them there is a radius to which you cannot tile. We take the maximum of these radii and find that the original tiling is also not good.

B9 It follows from the tasks of the following sections.

B10 It follows from the tasks of the following sections..

B11

1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	0	**1**	**1**	0	**1**	**1**	0	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	**1**	**1**	0	0	0	**1**	**1**	**1**
1	0	**1**	0	0	0	**1**	0	**1**
1	**1**	**1**	0	0	0	**1**	**1**	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**
1	0	**1**	**1**	0	**1**	**1**	0	**1**
1	**1**	**1**	**1**	**1**	**1**	**1**	**1**	**1**

a) We give a solution that uses some facts of set theory, namely, that the continuum is greater than the countable set. We denote the substitution by the letter s. Note that $s^k(1)$ is a square of size $3^k \times 3^k$, consisting of eight squares $s^{k-1}(1)$ and one square $s^{k-1}(0)$; all the squares of form $s^k(0)$ are filled with zeroes.

Any $3^k \times 3^k$-tiling of form $s^k(1)$ can be extended to the tiling $s^{k+1}(1)$ in eight ways; each extension corresponds to one of the eight external cells of the square 3×3 and different shifts of the square $3^{k+1} \times 3^{k+1}$ are obtained. Notice that we are interested in squares in the plane, not only in abstract squares.

We start with the square A_1 of size 1×1, in which there is a one, and we will do one of such extensions at each step; the filled area will expand. We obtain a sequence of tilings $A_1, A_2, A_3, \ldots$

Such sequences correspond to sequences of digits from 1 to 8, there is continuum of such sequences. The union of squares A_i can be either a quarter-plane, or a half-plane, or the whole plane. If we did not obtain the entire plane, then, starting at some point, we expanded the squares at only one direction. It is clear that there are uncountably many sequences $\{A_i\}$, the union of which fills the entire plane. The resulting tilings of the plane will be called *limit tilings*.

We show that different sequences $\{A_i\}$ lead to different limit tilings (note that we do not claim that they are not equivalent).

We consider in limit tiling squares $(3^k + 2) \times (3^k + 2)$, at the boundary of which there are ones, and zeroes inside. It is clear that the centers of all such squares are shifted relatively to the center of the square A_k by a vector, both coordinates of which are multiples of 3^k. Therefore, knowing the limit tiling, we can determine the coordinates of the center A^k modulo 3^k. But it is easy to see that the coordinates of its center cannot differ from the coordinates of the center of A_1 by more than $3^k/2$, therefore two limit tilings that coincide determine the same sequence of squares.

It is easy to see that each limit tiling is uniquely decodable, therefore there is at least a continuum of various Sierpinski carpets. And since only a countable number of carpets can be equivalent to one another, the number of equivalence classes is infinite.

b) The periodic Sierpinski carpet is one that consists of only zeroes. We show that all the remaining Sierpinski carpets are non-periodic. We note that if there is at least one 1 in the Sierpinski carpet, then for any natural number k the carpet contains the square $s^k(1)$, in the center of which there is a square of size $3^{k-1} \times 3^{k-1}$ filled with zeroes, and this square is framed by units. If we consider a translation by some nonzero vector whose coordinates are less than 3^{k-1}, the image of the border will intersect the square of zeroes, and so for any k. So, there are no vectors of periodicity.

c) *Answer: no.*

Let n be the size of the largest local rule; take k such that $3^k > n$. Consider a tiling A of the plane by 1's. It is not decodable, so the tiling $s^k(A)$ is not infinitely decodable. We show that the tiling $s^k(A)$ is permitted.

$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$

a pattern of $s^k(A)$

$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(0)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$
$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$	$s^k(1)$	$s^k(0)$	$s^k(1)$
$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$	$s^k(1)$

$s^{k+1}(1)$

It can be shown that any square with side no more than n that occurs in $s^k(A)$, occurs in some block composed of four squares $s^k(1)$. But this block is located inside $s^{k+1}(1)$, and therefore it is a pattern of Sierpinski carpets and does not contain forbidden squares.

B12 Let n be the size of σ. The tiling $\sigma(A)$ is composed of $n \times n$-squares – images of letters. Any 2×2-square is located inside some $2n \times 2n$-square (union of 4 such squares), which is of the form $\sigma\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$. Since the square $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ is permitted and σ agrees with local rules, $\sigma\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}\right)$ does not contain forbidden patterns.

B13 Consider a tile with letter a and a sequence of squares

$$A_0 = a, A_1 = \sigma(a), A_2 = \sigma^2(a) \dots$$

In this sequence A_i has size $n^i \times n^i$, and it follows from the previous problem that A_i is permitted for any i. From **B8**, it follows that there exists a permitted tiling of the whole plane.

B14 *Answer: not always.* For alphabet $\{0, 1\}$ and substitution $\sigma(0) = \left(\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right)$, $\sigma(1) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ such a tiling does not exist.

The criterion for the existence of a fixed tiling. σ admits a fixed tiling if and only if one letter appears strictly inside its own image, or two letters appear in their own images in some opposite side of the square, strictly, or four letters appear in their own images in all possible corners.

Sketch of proof. Let σ be a $k \times k$-substitution. First note that requiring $S = \sigma(S)$ would involve the choice of an origin tile, which is not a problem here: we just want S and $\sigma(S)$ to be equivalent. This means that there exist integers i, j such that, in S, the image by σ of any cell (x, y) is the pattern appearing at positions $(i + kx \cdots i + kx + k - 1, j + ky \cdots j + ky + k - 1)$. We can do a euclidean division of i by $1 - k$, and get $i = (1 - k)x + i'$ for some i' with $0 \leq i' < k - 1$. This x has the property that $i + kx \leq x < i + kx + k - 2$. Similarly, there is some y such that $j + ky \leq y < j + ky + k - 2$. We get that the image of the letter a which appears in cell (x, y) of S contains the letter a itself. A little more precisely, the inequalities give that the letter appears in its own image, but not on the bottom or right boundary (because we have divided by $k - 1$ rather than k). It it appears in the left boundary, then $x = i + kx$, so that the image of cell $(x - 1, y)$ is

$(x+k-1\cdots x, j+ky\cdots j+ky+k-1)$: again the letter at cell $(x-1,y)$ appears in its own image. The same is true if (x,y) was in the top boundary of the square.

Conversely, suppose σ admits one letter a which appears stricly inside its own image, say at position i,j. Then $\sigma^t(a)$ can be seen as a square pattern of size $k^t \times k^t$, that we can index in $-k^t i/(k-1)\cdots k^t(k-1-i)/(k-1)$ (and similary for the vertical coordinate) so that a is in cell $0,0$. This square grows on all four sides, so that, ultimately, every pair (x,y) of integers is mapped to a letter for these large enough squares. Moreover, this letter is constant, once defined. Indeed, an easy induction allows to show that then the square $\sigma^t(a)$ appears in the middle of any $\sigma^{t'}(a)$, for $t' \geq t$. Thus we can define S as holding, in cell (x,y) the letter that appears as $\sigma^t(a)(x,y)$ for large enough t. By construction $\sigma(S)$ will be the shift of S (with respect to i,j).

If σ admits two letters that appear in their own images in some side of the square, strictly, or four letters that appear in their own images in all possible corners, then we can do the same kind of iterations, starting with the pattern consisting in these two or four letters.

C. Examples of non periodicity

C1 a) For example, such a substitution σ:

1	⟶	1	1	1
		1	0	1
		1	1	1

0	⟶	0	0	0
		0	1	0
		0	0	0

The fact that the set of infinitely decoded tilings cannot be defined by local rules is proved in the same way as for Sierpinski carpets.

We call such a figure (and also if we swap 0 and 1) *a double frame.*

	1	1	1	1	1	1	1	
	1	0	0	0	0	0	1	
	1	0				0	1	
	1	0				0	1	
	1	0				0	1	
	1	0	0	0	0	0	1	
	1	1	1	1	1	1	1	

We say that the *size* of the double frame in the figure above is 5. If a double frame of size N occurs in the tiling, then the tiling cannot have a vector of periodicity with absolute values of coordinates less than N. By induction on k, it is shown that $\sigma^k(0)$ and $\sigma^k(1)$ contain a double frame of size 3^{k-1}.

b) Consider a one-letter alphabet.

C2 Suppose that in there are 8 letters a_i, b_i, c_i, d_i, for $i = 1$ or 2. The images of any letter is of form $\begin{smallmatrix} a_i & b_j \\ c_k & d_l \end{smallmatrix}$. There are 16 ways to choose indices, so we can choose different images for all eight letters.

C3 It is a consequence of some following problems.

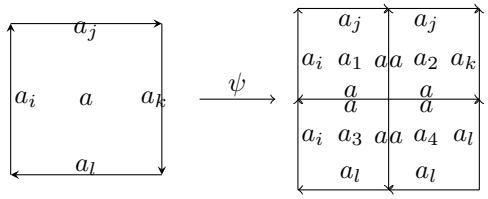
C4 Let us prove the aperiodicity of any infinitely decodable tiling A. Firstly note that, from the separation images property, it follows that both coordinates of any periodicity vector v must be divisible by 2, and then note that the vector $v/2$ is a periodicity vector for the tiling $\sigma^{-1}(A)$. Applying this to a tiling with the smallest nonzero period, we have a contradiction.

C5 We use notation W for left direction, E for right, N for up, and U for down. We will denote by NW the left-up direction (and similar notations for other diagonal directions). Our substitution has the image separation property, so each letter a_i of the alphabet A belongs to one of the types NW, NE, SW, SE.

We draw letters of the new (decorated) alphabet B as tiles, in the center of each tile a letter from A is written, there are arrows on the sides and on each side has a *label* – a letter of A. Thus, a letter from B is defined by a 5-tuple of letters of A and four extra bits (arrow directions).

We will talk about types of tiles (i.e. NE, NW, SE or SW, types of central letters), types of tile sides (N, E, S, W depending on the direction of the arrow), types of side labels (NE, NW, SE, SW). The substitution $\psi : B \to B^4$ is defined as follows. If the letter a is written in the center of a tile and some labels are written on the edges, and $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$, then we write the letters a_1, a_2, a_3, a_4 in centers of coresponding tiles, preserve

labels and directions for outer sides of tiles, direct central arrows from the center of 2×2-square and draw labels a on them, see pic.:

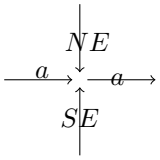


The idea of such a decoration is as follows: an infinitely decoded tiling consists of blocks $2^k \times 2^k$, and each $2^k \times 2^k-$block consists of four $2^{k-1} \times 2^{k-1}-$blocks, and boundaries between these four blocks form a cross, on the edges of which the same labels are written. These crosses separate blocks of large size from each other. In the Sierpinski carpets example, there was no such boundary, and local rules could not distinguish the boundary of a large block from its middle part.

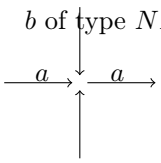
We say that the direction NE is symmetric to NW with respect to the vertical direction, and SW is symmetric to SE with respect to the vertical direction. Symmetry relative to the horizontal direction is defined similarly.

We define the following local rules:

1) On neighbouring tiles, adjacent sides have the same direction and label (that is, one can speak about the direction and label of edges in the entire tiling).
2) Only tiles of vertically symmetrical types can have a common vertical side. Only tiles of horizontally symmetrical types can have a common horizontal side.
3) Nodes between tiles can have only such degrees of: outgoing degree 4 OR indegree 3 and outdegree 1.
4) If 4 edges go from one node, their labels coincide.
5) If there is a tile of type NW to the up-left side of a given node, we call this node *central*. We require that central nodes have outgoing degree 4. If these edges have labels a, and $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$, then in the center of the tile to the north-west of the node there should be the letter a_1, similarly for the other three tiles.
6) From a node of type 3-1 there is an *outgoing arrow*, *central ingoing arrow* and two *lateral arrows*. We require that the labels on the central incoming and outgoing arrows coincide, and also that the types of labels on the lateral arrows are symmetrical with respect to the outgoing edge. For example:



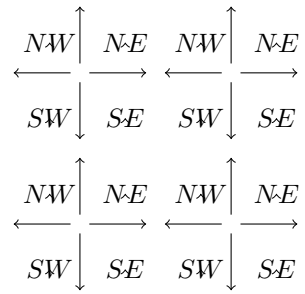
7) For a node of type 3-1, suppose there is a label a on the outgoing v_1, and a label b on a lateral ingoing arrow v_2. Let $\sigma(a) = \begin{smallmatrix} a_1 & a_2 \\ a_3 & a_4 \end{smallmatrix}$.
If the angle between the type of b and the direction of v_2 is equal to 135° (for instance, v_2 goes down, and b has type NE), then the angle between v_1 and the type of b must equal to 45°, and the letter b must occur in $\sigma(a)$ at the position corresponding to the type of b.



$b = a_2$, where a_2 is the NE letter in $\sigma(a)$

To construct this set of rules, we looked closely at an infinitely decodable tiling, and forbid everything that did not occur there. It is necessary, on the one hand, to write enough rules so that decoding can be determined, and on the other hand – to check that after the decoding all the local properties hold. For this reason, we do not use larger local rules (involving non-neighbouring tiles): it is difficult to verify them after decoding.

Analysis of permitted tilings. Now we want to investigate permitted tilings. From 1) we find that the plane is divided into 2×2-squares, in each of which the tiles have the form $\begin{smallmatrix} NW & NE \\ SW & SE \end{smallmatrix}$. We will call these blocks *basic blocks*. From 5) and 4) it follows that the centers of the basic blocks are central nodes; moreover each of them has 4 outgoing arrows, which have the same labels.

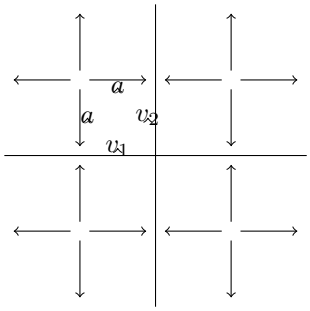


All the nodes are divided into central, *lateral* (those which have 2 ingoing arrows at the picture above) and the rest. From 3) it follows that the midpoints of the sides of the basic blocks (lateral nodes) are of the type $3-1$, and together with 6) it implies that the arrows on each side of the basic block are co-directional and have the same labels.

Together with property 4) this gives that each base block is a $\psi-$ image of some letter. Thus, the decoding from a permitted tiling T to $\psi^{-1}(T)$ is well defined. This tiling can be obtained from T by erasing the lines inside the base blocks and writing inside them the letters which are the labels of arrows, outgoing from its center. We need to check for $\psi^{-1}(T)$ the properties of $1)-7)$. Properties 1), 3), 4), and 6) are automatically satisfied, since no new situation at the nodes (in terms of which labels and arrows are written on the incoming edges) arises.

For property 2), we must check that any two base blocks having a common side are decoded into symmetric type of letters. But the type after decoding coincides with the type of the label written on the inner cross of the basic block. The local rule 5) guarantees that the marks of the two blocks are symmetric, and after decoding, 2) holds. So, the basic blocks are combined into 4×4-blocks, which after decoding have the form $\begin{smallmatrix} NW & NE \\ SW & SE. \end{smallmatrix}$

Consider a 4-tuple like in the following figure.



The label a has type NW, therefore, according to 6), the edge v_1 is directed to the left, and v_2 to the top. Hence, v_1 and v_2 go out from a central node. From 4) it follows that the labels on these edges coincide. Also, from 6) it follows that a is in the upper left corner of the image of this label under σ. Similarly we can speak about the rest of the basic blocks, and therefore, after decoding, property 5) holds. So, the decoded tiling is permitted, and therefore all the permitted tilings are infinitely decoded.

Generally speaking, we have not solved the problem yet. We have not shown that *each* tiling that is infinitely decodable by σ allows a permitted decorations. It can be shown that such a decoration exists for those tilings for which each tile lies strictly inside some block of form $\sigma^k(a_i)$. You can describe the rest of the tilings and slightly modify our decoration; we leave this it to the reader as an exercise.

C6 We leave this task as an exercise.

C7 We'll use $C5$. Let σ be a substitution $A\to A^4$. Take τ 2×2 with property of separating images $B\to B^4$. Construct a new alphabet C of size $|A|\cdot|B|$; its letters are pairs $(a_i,b_j)|a_i\in A, b_j\in B$. We define on it a substitution ψ of size 2×2 given as follows: $(a,b)\to \begin{smallmatrix} (a_i,b_j) & (a_k,b_l) \\ (a_m,b_n) & (a_p,b_r) \end{smallmatrix}$, where $\sigma(a)=\begin{smallmatrix} a_i & a_k \\ a_m & a_p \end{smallmatrix}$ и $\tau(b)=\begin{smallmatrix} b_j & b_l \\ b_n & b_r \end{smallmatrix}$. It is easy to see that it is a decoration of σ and it has the property of separating images.

D. Different formalisms.

D1 Replace letters at up and right sides by opposite ones.

D2 *Hint.* Use Robinson tilings, divide them by small squares and give local rules that force small tiles to form big Robinson tiles.

D3 a) *Answer: no.* It's easy to construct a periodic tiling repeating a 2×2 block made of one tile and all its reflections.

b) *Answer: yes.*

E. Decorations.

E1. a) alphabet $\{a_1, a_2, b\}$; forbid $\{ba_1, a_2b, bb, a_2a_1\}$.

b) alphabet $\{a_1, a_2, b\}$; forbid $\{ba_1, a_2b, bb, a_2a_1\}$ horizontally, $\{\begin{smallmatrix} b \\ a_2 \end{smallmatrix}, \begin{smallmatrix} a_1 \\ b \end{smallmatrix}, \begin{smallmatrix} b \\ b \end{smallmatrix}, \begin{smallmatrix} a_2 \\ a_1 \end{smallmatrix}\}$ vertically, and $\{\begin{smallmatrix} a_1 & a_2 \\ a_2 & \end{smallmatrix}\}$.

E2. The set of tiles with decorations, without those labeled b, tiles arbitrarily large squares (in every infinite tiling). By **B8**, there is a tiling of the plane using those tiles. It is labeled by only a's.

E3. a) *Answer: no.* Assume it could, and let k be the maximal size of the local rules. Consider a tiling with a single connected component which is a horizontal path of size k, and another tiling, similar but with size $k+1$. These two tilings have the same patterns of size k, so they should be either both forbidden or both permitted. Nevertheless, exactly one of these two is in the wanted set.

b) alphabet $\{a, b_1, b_2\}$; forbid $\{ab_2, b_1b_1, b_2b_2, b_1a\}$.

c) One possible solution (among many possibilities): Decorations draw a spanning forest for the connected component, that is the disjoint union of rooted directed trees that cover the whole component. Each tree should have even cardinality: this can be counted at each node by addition modulo 2 of the value carried by possible son nodes. On the one hand, every connected component can be decorated by an even spanning tree, hence permitted. On the other hand, if a tiling is permitted, every connected component is spanned by several trees of even cardinality, so that it itself has even cardinality.

E4*. In 1D: yes, easy: alphabet $\{a, b_1, b_2\}$; forbid $\{ab_2, b_1b_1, b_2b_2, b_2a\}$.

In 2D: no, it's much more difficult, because the sum of two odd numbers is not odd. It's hard to force the connected component to be spanned by only one tree (rather than a forest). This question is currently the purpose of ongoing research, on so-called *soficity* of sets of tilings.

E5. The set of tilings representing 3-colorable planar graphs, for instance.

E6.

a) All 2×2 patterns that appear in the new tiling already appeared in one of the two previous permitted tilings.

b) Let k bet the cardinality of the decorated alphabet. The number of possible decorations for the border of $n \times n$ tilings is $k^{4(n-1)}$.

c) Consider the set of configurations such that all c's form a column, and consider the set of $n \times n$-squares that appear on the left of this column. They can be any tiling over $\{a, b\}$, so there are 2^{n^2} different ones. If n is big with respect to k, then by the previous question, two of these tilings have the same decorations within the corresponding infinite tilings, and by Question a), we can replace one by the other. But then (at least) one of the two does not have the correct mirror image on the other side of the column.

d) If $\mathcal{S}$ is a set of tilings that is defineable by decorations and local rules, then there exists k such that, for every n, any set of $n \times n$ tilings which have nonintersecting pairwise extension sets (set of possible ways to extend as a tiling of the plane) has cardinality at most k^n.

К алгоритмам решения алгебраических уравнений

представляют Б. Вукорепа, А. Глебов,
А. Еннэ, А. Скопенков, А. Чиликов *

1 Введение и формулировки результатов

1.1 О чём этот цикл задач

Знаменитые теоремы[1] Руффини 2.7, Абеля и Галуа 1.3, 1.4 о неразрешимости алгебраических уравнений в радикалах — классический результат алгебры, интересный для информатики (теории символьных вычислений). Формулировки этих теорем приведены ниже.

Основное содержание данного текста — изложение глубоких идей алгебры (точнее, теории Галуа) на красивых простых доказательствах этих теорем, см. [ZSS, § 27]. Замечательно, что при этом для понимания приводимых доказательств достаточно уметь делить многочлены с остатком, извлекать корни из комплексных чисел, умножать перестановки и решать системы линейных уравнений. И тот, кто не дойдёт до полного доказательства основных резуль-

*Благодарим Я. Абрамова, Д. Елисеева, А. Канунникова, О. Орел, А. Петухова, Н. Хорошавкину, Г. Челнокова и жюри ЛКТГ за обсуждения и перевод частей текста.

Б. Вукорепа: Загребский Университет. *А. Глебов:* Новосибирский Государственный Университет. *А. Еннэ:* Петрозаводский Государственный Университет. *А. Скопенков:* Московский Физико-Технический Институт, Независимый Московский Университет. `http://www.mccme.ru/~skopenko`. *А. Чиликов:* Московский Государственный Технический Университет им. Баумана, Московский Физико-Технический Институт.

[1] Из §1 далее используется только §1.5, можно сразу перейти к нему и решению задач.

татов, сможет порешать задачи для исследования, см. [E2, Es, AB, Ko17, Saf] и ссылки в этих работах.

Перед доказательствами неразрешимости алгебраических уравнений мы разберем общий способ их решения — метод резольвент Лагранжа. Идея Абеля и Галуа фактически заключается в том, что если уравнение разрешимо в радикалах, то его можно решить этим методом. Этим же методом строятся и алгоритмы — например, распознаваемости разрешимости уравнений в радикалах.

Для практики приближённые методы решения уравнений более полезны, чем радикальные формулы. Кроме того, уравнения можно решать при помощи трансцендентных функций (см. метод Виета [ZSS, п. 4.2] и [PSo]). Однако проблема разрешимости в радикалах интересна как пробная задача современных теорий символьных вычислений и сложности вычислений.

О новизне. Приводимые в решениях доказательства не претендуют на новизну (хотя, возможно, читатели сумеют придумать что-то новое). Все же в этом тексте имеется много методических находок, см. [ZSS, п. 5.2.1, 5.2.2], и доказательства отличны от приведенных и цитированных в [ZSS, §5]. Однако, к сожалению, приводимые доказательства 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), а напрямую [2] — но при этом, конечно, переоткрывая и используя базовые идеи этой теории.

[2] Как, например, в [Dor, §25], [Pr07-2, дополнение 8], [FT, Лекция 5], [ZSS, §5], [Dor, St94, Kol, Ler, T, Sk11, Sk15] и здесь. Изложение в [Al] ближе к этому стилю. Хотя большая часть [Al] посвящена изложению теории, не нужной для доказательства ослабленной версии теоремы Абеля, объявленной в качестве основного результата (см. [Sk15, конец замечания 7]), автору книги [Al] удалось избежать немотивированного изложения части этой теории. Доказательство из [Al] более коротко и понятно изложено в [FT, Лекция 5] и, возможно, в [Sk11]. Заметим, что доказательства в большинстве этих источников неполны, см. [ZSS, сноска 12 на стр. 113 и конец §5.5.4], [Sk15, Обсуждение]. Несмотря на эти недостатки, вышеупомянутые элементарные изложения были для нас полезнее, 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. Немотивированное изложение служит «главным образом для

1.2 Неразрешимость в вещественных радикалах

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,

$$\text{чисел} \quad x+y, x-y, xy, \quad \text{числа } x/y \text{ при } y \neq 0$$

$$\text{и числа } \sqrt[n]{x} \text{ при } x > 0 \text{ и целом } n > 0.$$

Вещественная радикальность числа α равносильна существованию таких

- целых положительных чисел $s, k_1, \ldots, k_s$,
- вещественных чисел $f_1, \ldots, f_s$ и многочленов $p_0, p_1, \ldots, p_s$ от $0, 1, \ldots, s$ переменных, соответственно, с рациональными коэффициентами, что

$$\begin{cases} f_1^{k_1} = p_0 \\ f_2^{k_2} = p_1(f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(f_1, \ldots, f_{s-1}) \\ \alpha = p_s(f_1, \ldots, f_s) \end{cases}.$$

Замечание 1.1. (a) 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 [ZSS, п. 4.2], см. также задачу 2.8 (c).

(c) Уравнение $x^4 + 4x - 1 = 0$ имеет два вещественных корня, каждый из которых вещественно радикален [ZSS, п. 4.2], см. также задачу 2.10 (d).

того, чтобы затруднить непосвященным овладение своей наукой и тем самым повысить ее авторитет» [Ar84, стр. 49]. Заметим, что для многих именно *мотивированное* изложение повышает авторитет математики.

(d) Любое вещественно построимое число [ZSS, п. 5.1.2] вещественно радикально.

(e) 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 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 1.2 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 1.2 (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 $(p/3)^3+(q/2)^2>0$» [ZSS, задача 8.1.5.d].

Равносильность $(ii)\Leftrightarrow(iii)$ очевидна и следует из замечания 1.1.a. Разрешимость в теореме 1.2 (т.е. $(i)\Rightarrow(ii)$) доказывается *методом дель Ферро* [ZSS, п. 4.2]; см. другое доказательство в п. 2.3. Неразрешимость в теореме 1.2 (т.е. $(ii)\Rightarrow(i)$) доказывается сложнее. Более просто доказывается аналогичный результат о *неразрешимости в многочленах*, см. п. 2.5.

1.3 Неразрешимость в комплексных радикалах

Перейдём к формулам, которые могут содержать комплексные числа. Оказывается, кубическое уравнение (например, x^3-3x+1), не-

разрешимое 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 $n > 0$.

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* [ZSS, п. 4.2]; см. другое доказательство в п. 2.3. Однако аналог этих утверждений для более высоких степеней неверен.

Теорема 1.3 (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 2.7 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 следующую теорему Галуа (более слабую и более просто доказываемую, чем теорема Галуа 1.3). 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 1.4 (Галуа)**.** Существуют такие $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$, что ни один корень уравнения $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ не является $\{a_0, a_1, \ldots, a_4\}$-радикальным.

Теорема 1.5. Существует алгоритм, определяющий для данных $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$, все ли корни уравнения $x^n + a_{n-1}x^{n-1} + \ldots +$

$a_1x + a_0 = 0$ радикальны.

Теорема 1.5 доказывается при помощи критерия разрешимости Галуа 2.13.b и оценки на число операций.

1.4 План

Этот проект распадается на три формально независимых куска (в первых двух используется определение радикальности из п. 2.2).

(1) В п. 2.3 обсуждается метод (резольвент Лагранжа) решения уравнений. Формально он не используется в доказательствах неразрешимости. Однако знакомство с ним будет полезно, поскольку доказательства неразрешимости были придуманы при анализе этого метода, поскольку это знакомство поможет контролировать правильность промежуточных гипотез, возникающих при доказательствах неразрешимости, и поскольку этот метод нужен для доказательства теоремы 1.5.

(2) Доказательство теоремы Руффини 2.7 основано на идее симметрии и намечено в п. 3.1. К нему подводит п. 2.5. П. 2.4 подводит и к п. 2.5, и к доказательству теоремы Галуа 1.4.

(3) Доказательство теоремы 1.2 о разрешимости в вещественных радикалах основано на идее сопряжения (или алгебраической симметрии). К нему подводят п. 2.1, 3.2 и 3.3.

Теоремы 1.3 и 1.5 не доказываются в этом тексте, см. доказательство первой в [ZSS, §5], [Sk19, §9]. Теорема Галуа 1.4 доказывается в дополнительных задачах, ср. [Sk15, Sk19], при помощи редукции к теореме Руффини 2.7, использующей идею сопряжения (п. 2.1, 3.2 и 3.3).

1.5 Рекомендации участникам

Участник (или группа участников) конференции, решающий задачи проекта, получает «боб» за каждое *записанное* решение, оцененное в «+» или «+.». Дополнительные бобы могут выдаваться за красивые решения, решения сложных проблем, или оформление некоторых решений в системе TEX. У жюри бесконечно много бобов. Решения можно сдавать и устно, отдавая один боб за каждые пять попыток (неважно, удачных или нет).

Если задача выделена словом «теорема» («лемма», «следствие» и т. д.) и жирным шрифтом, то её утверждение более важное. Как правило, мы приводим (в виде задачи) *формулировку* красивого или важного утверждения *перед* его *доказательством*. В таких случаях для доказательства утверждения могут потребоваться последующие задачи. Если Вы застряли на какой-то другой задаче, также перейдите к следующим, они могут помочь.

Приглашаем Вас обсуждать с жюри возникающие вопросы. Особо успешным решателям мы выдаем *дополнительные задачи* для исследования.

Пожалуйста, сообщите нам, если Вы знаете решения каких-то из предложенных задач. Если Вы подтвердите свои знания, сообщив нам решения некоторых из них, Вам будет разрешено не получать плюсы по всем этим задачам, но пользоваться ими при решении остальных.

2 Задачи до промежуточного финиша

В этом тексте равенства, включающие многочлен f (или f_j) означают равенство многочленов (покоэффициентное). В п. 2.1, 3.2 и 3.3 «многочлен с рациональными коэффициентами» коротко называется многочленом. Обозначим

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

2.1 Одно извлечение квадратного корня

2.1. 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) $\cos(2\pi/5)$;
(e) $\sqrt[3]{2}$; (f) $\sqrt{2}+\sqrt[3]{2}$; (g) $\cos(2\pi/9)$;
(h)* $\sqrt{2+\sqrt{2}}$; (i)* $\cos(2\pi/7)$; (j) $\sqrt{2}+\sqrt{3}+\sqrt{5}$.

Лемма 2.2. Пусть $r \in \mathbb{R}-\mathbb{Q}$ и $r^2 \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен x^2-r^2 неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если $a, b \in \mathbb{Q}$ и $a+br=0$, то $a=b=0$.

(c) Если многочлен имеет корень r, то этот многочлен делится на x^2-r^2.

(d) **О сопряжении.** Если многочлен имеет корень r, то корнем этого многочлена является также число $-r$.

(e) **О сопряжении.** Если $a, b \in \mathbb{Q}$ и многочлен имеет корень $a + br$, то корнем этого многочлена является также число $a - br$.

(f) Если $a, b \in \mathbb{Q}$ и кубический многочлен имеет корень $a + br$, то он имеет рациональный корень.

Теорема 2.3. Если многочлен степени выше второй неприводим над $\mathbb{Q}$, то ни один из его корней не представим в виде $a \pm \sqrt{b}$, где $a, b \in \mathbb{Q}$.

Лемма 2.4 (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 $b > 0$.

2.5.* Для каких n число $\cos(2\pi/n)$ представимо в виде $a + \sqrt{b}$, где $a, b \in \mathbb{Q}$?

Подсказки к п. 2.1

2.2. (a) Если многочлен $x^2 - r^2$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(b) Если $b \neq 0$, то $r = -a/b \in \mathbb{Q}$, что невозможно. Поэтому $b = 0$, а значит, $a = 0$.

(c) Поделим многочлен с остатком[3] 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. (b)) получаем, что остаток нулевой.

(d) Из п. (c) следует, что если $R^2 = r^2$, то R есть корень многочлена.

Указание к другому решению. Отображение $u \mapsto \overline{u}$ множества $\mathbb{Q}[\sqrt{2}] := \{a + b\sqrt{2} \colon a, b \in \mathbb{Q}\}$ в себя корректно определено формулой $\overline{a + br} := a - br$. Кроме того, $\overline{u + v} = \overline{u} + \overline{v}$ и $\overline{u \cdot v} = \overline{u} \cdot \overline{v}$ для любых $u, v \in \mathbb{Q}[\sqrt{2}]$.

[3] Это деление с остатком — то же самое, что «замена» x^2 на r^2.

(e) Обозначим через P многочлен из условия, и пусть $G(t){:=}P(a+bt)$. Тогда $G(r)=0$. Значит, по пункту (d) имеем $G(-r)=0$.

(f) Если $b=0$, то утверждение доказано. В противном случае по п. (e) многочлен имеет (различные) корни $a\pm br$, значит третий корень рационален по теореме Виета.

2.4. 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!).

2.2 Определение радикальности многочлена

Решение квадратного уравнения $t^2+bt+c=0$ можно выразить формулами

$$(x{-}y)^2=(x{+}y)^2{-}4xy=b^2{-}4c \text{ и } x=\frac{x+y+(x-y)}{2}=\frac{-b+(x-y)}{2}.$$

Эти формулы показывают, что корень x квадратного уравнения *выразим в радикалах* (в смысле, строго определенном ниже) через коэффициенты $-b=x+y$, $c=xy$ квадратного уравнения.

Обозначим элементарные симметрические многочлены

$$\sigma_1(x_1,\dots,x_n):=x_1+\ldots+x_n,\quad \dots,\quad \sigma_n(x_1,\dots,x_n)=x_1\cdot\ldots\cdot x_n.$$

Если число n и аргументы $x_1,\dots,x_n$ ясны из контекста, то они пропускаются из обозначений.

Многочлен $p\in\mathbb{C}[x_1,\dots,x_n]$ называется (комплексно) **радикальным** если p можно добавить в набор $\{\sigma_1,\dots,\sigma_n\}\cup\mathbb{C}$ многочленов цепочкой операций следующего вида:

- добавить в набор сумму или произведение уже имеющихся многочленов;
- если многочлен из набора равен f^k для некоторых $f\in\mathbb{C}[x_1,\dots,x_n]$ и целого $k>1$, то добавить в набор многочлен f.

Замечание 2.6. (a) 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 $y-x$).

(b) Операции первого типа добавляют многочлен с комплексными коэффициентами от уже имеющихся.

(c) По теореме Виета $\sigma_1, \ldots, \sigma_n$ есть коэффициенты многочлена

$$t^n - \sigma_1 t^{n-1} + \ldots + (-1)^{n-1}\sigma_{n-1}t + (-1)^n\sigma_n \in \mathbb{C}[x_1, \ldots, x_n][t]$$

с корнями $x_1, \ldots, x_n$. Поэтому радикальность многочлена x_1 равносильна выразимости (в указанном смысле) через коэффициенты этого многочлена его корня x_1.

(d) Радикальность многочлена x_1 равносильна существованию таких

- целых положительных чисел $s, k_1, \ldots, k_s$,
- многочленов $f_1, \ldots, f_s$ от n переменных и $p_0, p_1, \ldots, p_s$ от $n, n+1, \ldots, n+s$ переменных, соответственно, с комплексными коэффициентами, что

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \ldots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \ldots, \sigma_n, f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s) \end{cases}.$$

В этих равенствах мы опускаем переменные $(x_1, \ldots, x_n)$ многочленов $\sigma_1, \ldots, \sigma_n, f_1, \ldots, f_s$.

(e) Всегда ли можно, зная $x + y$ и xy, однозначно найти x?

Вот простейшая формализация этого вопроса: *существует ли отображение* $f\colon \mathbb{R}^2 \to \mathbb{R}$, *для которого* $f(x + y, xy) = x$ *при любых* $x, y \in \mathbb{R}$? Ответ: не существует (действительно, рассмотрите пары $x = 1, y = 2$ и $x = 2, y = 1$). Итак, радикальность не дает «нахождения» в указанном выше смысле.

Аналогично, зная $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$ и $\sigma_3 = xyz$, невозможно однозначно найти $(x - y)(y - z)(z - x)$ (действительно, рассмотрите тройки $x = 0, y = 1, z = -1$ и $x = 0, y = -1, z = 1$).

Теорема 2.7 (Руффини)**.** Ни для какого $n \geqslant 5$ многочлен x_1 не радикален.

Из доказательства будет вытекать, что даже многочлен $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ не радикален для $n = 5$.

2.3 Решение уравнений малых степеней

2.8. Какие из следующих многочленов радикальны для $n = 3$?
(a) $(x-y)(y-z)(z-x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

В задаче 2.8 и далее используйте основную теорему о симметрических многочленах, см., например, [ZSS, 4.6.3c]. Подсказкой к п. (c) являются следующие задачи 2.9.a и 2.11.c.

2.9. Многочлен $f \in \mathbb{R}[u_1, u_2, \ldots, u_n]$ называется **циклически симметрическим**, если $f(u_1, u_2, \ldots, u_n) = f(u_2, u_3, \ldots, u_{n-1}, u_n, u_1)$.

(a) 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.

(b) 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 $x_1, x_2, \ldots, x_{10}$.

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.

2.11. Решите системы уравнений (x, y, z, t — неизвестные, a, b, c, d известны):

$$\text{(a)} \quad \begin{cases} x+y+z+t=a, \\ x+y-z-t=b, \\ x-y+z-t=c, \\ x-y-z+t=d; \end{cases} \qquad \text{(b)} \quad \begin{cases} x+y+z+t=a, \\ x+iy-z-it=b, \\ x-y+z-t=c, \\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)} \quad \begin{cases} x+y+z=a, \\ x+\varepsilon_3 y+\varepsilon_3^2 z=b, \\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Выражения из задачи 2.11 называются *резольвентами Лагранжа*. Они «лучше» корней, поскольку «симметричнее» в следующем смысле.

Решение кубического уравнения при помощи резольвент Лагранжа (решение задачи 2.8(c)). Для нахождения корней x, y, z кубического уравнения достаточно найти выражения a, b, c из задачи 2.11 (c). (Заметим, что метод дель Ферро из задачи [ZSS, 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 [ZSS, 4.6.3c]) 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.

Ввиду теоремы Руффини 2.7 метод резольвент Лагранжа, продемонстрированный на примере решения уравнений 3-й и 4-й степени (задачи 2.8 (c) и 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

$$\vec{u}_\alpha := (u_{\alpha(1)}, \ldots, u_{\alpha(q)}).$$

Определим *резольвенту Лагранжа* как

$$t(u_1, \ldots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \ldots + \varepsilon_q^q u_q.$$

Определим *резольвенту Галуа* как

$$Q(u_1, \ldots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, y].$$

2.12. (a) Имеем $Q(\varepsilon_q u_1, \ldots, \varepsilon_q u_q, y) = Q(u_1, \ldots, u_q, y)$.

(b) Для некоторого $R_Q \in \mathbb{Q}[\varepsilon_q][z]$ имеем $Q(u_1, \ldots, u_q, y) = R_Q(u_1, \ldots, u_q, y^q)$.

(c) Если $x_1, \ldots, x_5$ — корни многочлена $f \in \mathbb{Q}[x]$ 5-й степени, то $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ и даже $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[y]$.

Многочлен $R_Q(x_1, \ldots, x_5, z) \in \mathbb{Q}[z]$ называется *разрешающим многочленом* для f.

(d)* Все корни разрешающего многочлена для $f(x) = x^5 + 15x + 11$ (а значит, и самого многочлена f) радикальны.

Теорема 2.13.* (a) При $a, b \in \mathbb{R}$ все корни уравнения $x^5 + ax + b = 0$ радикальны тогда и только тогда, когда $a = \dfrac{15 \pm 20c}{c^2+1}$ и $b = \dfrac{44 \mp 8c}{c^2+1}$ для некоторого $c \in \mathbb{Q}$, $c \geqslant 0$.

(b) (**Критерий Галуа разрешимости**) Для любых $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ все корни уравнения $A(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ 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 $P_1 P_2$ для некоторых $P_1, P_2 \in \mathbb{Q}[x]$, не являющихся константами, то заменим $P_1 P_2$ 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 $Q(y_1, \ldots, y_q, y)$, где $y_1, \ldots, y_q$ – все корни многочлена P. (По задаче 2.12.c $Q(y_1, \ldots, y_q, y) \in \mathbb{Q}[y]$.)

Часть (a) выводится из (b) [PSo]. Часть «тогда» в (b) проще и доказывается методом резольвент Лагранжа, разобранным в этом пункте. Часть «только тогда» в (b) сложнее и доказывается аналогично теоремам Галуа 1.3, 1.4.

2.4 Единственность способа решения квадратного уравнения

Системы уравнений из этого и следующего пунктов возникают при решении уравнений в радикалах («при помощи одного радикала»), см. замечание 2.6.d.

2.14. (a,b) Решите систему уравнений в многочленах $f(x, y)$, $p(u, v)$ и $q(u, v, w)$ с вещественными коэффициентами:

(a) $\begin{cases} f^2(x,y) = p(x+y, xy) \\ x = q\left(x+y, xy, f(x,y)\right) \end{cases}$.

(b) $\begin{cases} f^k(x,y) = p(x+y, xy) \\ x = q\left(x+y, xy, f(x,y)\right) \end{cases}$, где $k > 0$ целое.

(c,d*) Решите аналоги п. (a,b) с заменой многочлена f на функцию $f : \mathbb{R}^2 \to \mathbb{R}$ (не предполагаемую непрерывной).

Системе уравнений из 2.14.a удовлетворяют, например, многочлены

$$f(x,y) = x - y, \quad p(u,v) = u^2 - 4v \quad \text{и} \quad q(u,v,w) = \frac{u+w}{2}.$$

2.15. Пусть $f, g \in \mathbb{R}[x,y]$.

(a) **Лемма.** Если $fg = 0$, то $f = 0$ или $g = 0$.

Предостережения: существуют функции $F, G : \mathbb{R} \to \mathbb{R}$, 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 тем, что если значения многочленов от двух переменных совпадают в любой точке, то эти многочлены равны.

(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) $f^5 - g^5 = (f-g)(f-\varepsilon_5 g)(f-\varepsilon_5^2 g)(f-\varepsilon_5^3 g)(f-\varepsilon_5^4 g)$.

Для доказательства утверждений 2.14.bd полезны следующие понятия и лемма.

Многочлен f от двух переменных x, y называется *симметрическим*, если $f(x,y) = f(y,x)$, и *антисимметрическим*, если $f(x,y) = -f(y,x)$.

2.16. (a) **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.

(b) **Лемма.** Если $f \in \mathbb{R}[x,y]$ и многочлен f^{2k+1} симметрический, то f симметрический.

(c) Если $f \in \mathbb{R}[x,y]$ антисимметрический, то существует симметрический многочлен $a \in \mathbb{R}[x,y]$, для которого $f = (x-y)a$.

Для доказательства полезна лемма 2.15.a, очень полезная и при решении других задач.

2.17. Для каких из утверждений 2.15 и 2.16 справедливы аналоги для многочленов с комплексными коэффициентами?

Вот обобщение утверждения 2.14 на любое количество шагов из определения радикальности (п. 2.2).

2.18. *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 $(f, 1)$.

(a) Дайте определения суммы и произведения рациональных функций. Проверьте их корректность.

(b) Возьмем систему из замечания 2.6.(d) 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 $x + y, xy, f_1, \ldots, f_{j-1}$ ни для каких $j = 1, \ldots, s$ и $k < k_j$. Тогда $s = 1$, $k_1 = 2$ и существует рациональная функция $a \in \mathbb{R}(u, v)$, для которой $f_1(x, y) = (x - y)a(x + y, xy)$.

(c)* Сформулируйте и докажите аналог п. (b) с заменой рациональных функции $f_1, \ldots, f_s$ на функции $\mathbb{R}^2 \to \mathbb{R}$ ($p_0, \ldots, p_s$ попрежнему рациональные функции), и равенств рациональных функций — на равенства функций, определенных для всех $(x, y) \in \mathbb{R}^2$.

2.5 Неразрешимость «в вещественных многочленах»

В этом пункте аргументы (x, y, z) многочленов в формулах часто пропускаются.

2.19. Не существует многочленов $f(x, y, z)$, $p(u, v, w)$ и $q(u, v, w, \tau)$ с вещественными коэффициентами, для которых

$$\begin{cases} f(x,y,z)^k = p\big(\sigma_1(x,y,z), \sigma_2(x,y,z), \sigma_3(x,y,z)\big) \\ x = q\big(\sigma_1(x,y,z), \sigma_2(x,y,z), \sigma_3(x,y,z), f(x,y,z)\big) \end{cases}.$$

(a) для $k = 1$; (b) для $k = 3$; (c) для $k = 2$;
(d) для любого целого $k > 0$.

Для доказательства полезны следующие понятие и утверждение. Многочлен $f \in \mathbb{R}[x, y, z]$ называется **циклически симметрическим**, если $f(x, y, z) = f(y, z, x)$.

2.20. Если $f \in \mathbb{R}[x, y, z]$ и многочлен

(a) f^3; (b) f^2

циклически симметрический, то f циклически симметрический.

Замечание 2.21 (ср. с решением задачи 2.8.c)**.** Не существует таких многочленов

$$f_1(x,y,z), \quad f_2(x,y,z), \quad p_0(u,v,w), \quad p_1(u,v,w,\tau_1), \quad p_2(u,v,w,\tau_1,\tau_2)$$

с вещественными коэффициентами, для которых

$$\begin{cases} f_1^2 = p_0(\sigma_1,\sigma_2,\sigma_3) \\ f_2^3 = p_1(\sigma_1,\sigma_2,\sigma_3,f_1) \\ x = p_2(\sigma_1,\sigma_2,\sigma_3,f_1,f_2) \end{cases}.$$

Обобщение замечания 2.21 на любое количество шагов формализуется определением *вещественной радикальности*, которое получается из его комплексного аналога (§2.3) заменой комплексных коэффициентов на вещественные.

Формулы в начале п. 2.2 показывают, что многочлен x вещественно радикален для $n = 2$. Решение задачи 2.8.ab показывает, что оба многочлена

$$(x-y)(y-z)(z-x) \quad \text{и} \quad x^9y + y^9z + z^9x$$

вещественно радикальны для $n = 3$.

Теорема 2.22. Многочлен x не является вещественно радикальным для $n = 3$.

Теорема 2.22 есть еще одна формализация того, что *корень кубического уравнения не выразим в вещественных радикалах через его коэффициенты*, ср. с замечанием 1.1.e. Она вытекает из следующей леммы.

Лемма 2.23 (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.

2.24. Аналоги каких утверждений этого пункта справедливы для многочленов с комплексными коэффициентами?

3 Задачи после промежуточного финиша

3.1 Неразрешимость «в многочленах»

Определение радикальности многочлена приведено в п. 2.2. Формально, теорема Руффини 2.7 вытекает из леммы 3.4. Самое трудное и интересное — придумать формулировку этой леммы. Для этого докажем следующие более простые факты. Сообразите, почему многочлен x не является многочленом от $x+y$ и xy.

3.1. Многочлен x_1 не радикален для $n=3$ так, что вторая операция из определения радикальности применяется только для

(a) $k=2$ (*подсказка:* см. задачу 2.24); (b) $k=3$.

3.2. Какие из следующих утверждений верны для любого $f \in \mathbb{C}[x_1,\dots,x_5]$?

(a) Если f^3 циклически симметрический, то f циклически симметрический.

(b) Если f^5 циклически симметрический, то f циклически симметрический.

(c) Если f^3 симметрический, то f симметрический.

(d) Если f^2 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 для любого цикла α длины 3 многочлены $f(x_1,x_2,\dots,x_n)$ и $f(x_{\alpha(1)},x_{\alpha(2)},\dots,x_{\alpha(n)})$ равны.

3.3. (a) Придумайте циклически симметрический многочлен, не являющийся четносимметрическим.

(b) Если перестановка переводит в себя многочлен, построенный Вами в решении задачи 3.2.d, то она представляется в виде композиции циклов длины 3.

Лемма 3.4 (о сохранении четносимметричности)**.** Если $q > 0$ целое, $f \in \mathbb{C}[x_1, \ldots, x_5]$ и многочлен f^q четносимметрический, то f четносимметрический.

3.5. Пусть $f \in \mathbb{C}[x_1, \ldots, x_n]$ — многочлен.

(a) Если многочлен f^7 четносимметрический, то f четносимметрический.

(b) Если $n \geqslant 5$ и многочлен f^3 четносимметрический, то f четносимметрический.

(c) Если $n \geqslant 5$, 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).

3.6. Определение *рациональной* вещественной (комплексной) радикальности аналогично определению радикальности, только вместо многочленов берутся рациональные функции (с соответствующими коэффициентами; см. определение в задаче 2.18). Является ли многочлен x_1

(a) вещественно рационально радикальным для $n = 3$?

(b) (комплексно) рационально радикальным для $n = 5$?

3.2 Одно извлечение корня третьей степени

Здесь развиваются идеи из п. 2.1.

3.7. Представимо ли следующее число в виде $a+b\sqrt[3]{2}+c\sqrt[3]{4}$, где $a, b, c \in \mathbb{Q}$:

(a) $\sqrt{3}$; (b) $\frac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$; (c) $\cos(2\pi/9)$; (d) $\sqrt[5]{3}$; (e) $\sqrt[3]{3}$;

(f) наибольший вещественный корень многочлена $x^3 - 4x + 2$;

(g)* единственный вещественный корень многочлена $x^3 - 6x - 6$;

(h)* единственный вещественный корень многочлена $x^3 - 9x - 12$?

Лемма 3.8. Пусть $r \in \mathbb{R} - \mathbb{Q}$ и $r^3 \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если $a, b, c \in \mathbb{Q}$ и $a+br+cr^2 = 0$, то $a = b = c = 0$.

(b′) **О линейной независимости над $\mathbb{Q}[\varepsilon_3]$.** Если

$$k, l, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 \colon u, v \in \mathbb{Q}\}$$

и $k + lr + mr^2 = 0$, то $k = l = m = 0$.

(c) Если многочлен имеет корень r, то этот многочлен делится на $x^3 - r^3$.

(d) **О сопряжении.** Если многочлен имеет корень r, то корнями этого многочлена являются также числа $\varepsilon_3 r$ и $\varepsilon_3^2 r$.

(e) **О сопряжении.** Если $a, b, c \in \mathbb{Q}$ и многочлен имеет корень $x_0 := a + br + cr^2$, то корнями этого многочлена являются также числа

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{и} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2.$$

(f) **О рациональности.** Если $a, b, c \in \mathbb{Q}$, то число $a + br + cr^2$ является корнем некоторого ненулевого многочлена степени 3.

Теорема 3.9. Если многочлен неприводим над $\mathbb{Q}$ и имеет корень вида $a + br + cr^2 \notin \mathbb{Q}$, где $r \in \mathbb{R} - \mathbb{Q}$ и $a, b, c, r^3 \in \mathbb{Q}$, то степень многочлена равна 3 и он имеет ровно один вещественный корень.

Лемма 3.10 (о расширении)**.** Число, вещественно радикальное с извлечением корня только один раз, причём третьей степени, имеет вид $a + br + cr^2$, где $r \in \mathbb{R}$ и $a, b, c, r^3 \in \mathbb{Q}$.

3.3 Одно извлечение корня простой степени

3.11. Представимо ли следующее число в виде

$$a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \ldots + a_6\sqrt[7]{2^6},$$

где $a_0, a_1, a_2, \ldots, a_6 \in \mathbb{Q}$?

(a) $\sqrt{3}$; (b) $\cos\frac{2\pi}{21}$; (c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$;

(e) какой-нибудь из корней многочлена $x^7 - 4x + 2$.

Ответы: не представимы. Доказательства аналогичны решениям задач 3.7. Используйте сформулированные ниже леммы.

Лемма 3.12. Пусть q простое, $r \in \mathbb{R} - \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(a) **О неприводимости.** Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}$.

(b) **О линейной независимости.** Если A — многочлен степени меньше q и $A(r) = 0$, то $A = 0$.

(c) **О сопряжении.** Если многочлен имеет корень r, то он имеет также корни $r\varepsilon_q^k$ для каждого $k = 1, 2, 3, \ldots, q - 1$.

(d) **О рациональности.** Если A — многочлен, то число $A(r)$ является корнем некоторого ненулевого многочлена степени не выше q.

Обозначим

$$\mathbb{Q}[\varepsilon_q] := \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \ldots + a_{q-2}\varepsilon_q^{q-2} \ : \ a_0, \ldots, a_{q-2} \in \mathbb{Q}\}.$$

3.13. Пусть q простое, $r \in \mathbb{C} - \mathbb{Q}[\varepsilon_q]$ и $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b), (c) Докажите аналоги пунктов (b), (c) предыдущей задачи для многочлена с коэффициентами в $\mathbb{Q}[\varepsilon_q]$.

Лемма 3.14.* Пусть q простое, $r \in \mathbb{R} - \mathbb{Q}$ и $r^q \in \mathbb{Q}$.

(a) **О неприводимости над** $\mathbb{Q}[\varepsilon_q]$**.** Многочлен $x^q - r^q$ неприводим над $\mathbb{Q}[\varepsilon_q]$.

(b) **О линейной независимости над** $\mathbb{Q}[\varepsilon_q]$**.** Если A — многочлен степени меньше q с коэффициентами в $\mathbb{Q}[\varepsilon_q]$ и $A(r) = 0$, то $A = 0$.

Теорема 3.15. Пусть многочлен неприводим над $\mathbb{Q}$ и имеет иррациональный корень $A(r)$ для некоторых многочлена $A \in \mathbb{Q}[x]$ и $r \in \mathbb{R}$, причём $r^q \in \mathbb{Q}$ для некоторого простого q. Тогда многочлен имеет степень q и при $q \neq 2$ не имеет других вещественных корней.

Доказательство аналогично доказательствам теорем 2.3, 3.9 и решениям задач 3.11 (abc). Используйте леммы о сопряжении 3.12 (c), о рациональности 3.12 (d) и о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b).

Лемма 3.16 (о расширении)**.** Число, вещественно радикальное с извлечением корня только один раз, равно $A(r)$ для некоторых $A \in \mathbb{Q}[x]$ и $r \in \mathbb{R}$, причём $r^q \in \mathbb{Q}$ для некоторого $q \in \mathbb{Z}$.

Доказательство аналогично лемме 3.10 о расширении.

3.17. (a–d) Докажите аналоги утверждений задачи 3.12 с заменой $\mathbb{Q}$ на произвольное подмножество $F \subset \mathbb{R}$, замкнутое относительно операций сложения, вычитания, умножения и деления на ненулевое число (и многочленов с коэффициентами в $\mathbb{Q}$ на многочлены с коэффициентами в F).

Решения задач до промежуточного финиша

2.1. *Ответы*: (a), (b), (c), (d) — да, (e), (f), (g), (h), (i) — нет.

(a), (c) Имеем $\sqrt{3+2\sqrt{2}} = \sqrt[3]{7+5\sqrt{2}} = 1+\sqrt{2}$.

(b) Имеем $\frac{1}{7+5\sqrt{2}} = \frac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7+5\sqrt{2}$.

(d) Имеем $\cos(2\pi/5) = (\sqrt{5}-1)/4$.

(e) Пусть число $\sqrt[3]{2}$ представимо. Тогда

$$2 = (\sqrt[3]{2})^3 = (a^3+3ab)+(3a^2+b)\sqrt{b}.$$

Так как $3a^2+b \neq 0$, то $\sqrt{b} \in \mathbb{Q}$. Значит, $\sqrt[3]{2} \in \mathbb{Q}$ — противоречие.

Другой способ — аналогично теореме 2.3.

(f) *Набросок первого решения.* Проще доказать сразу, что

$$\sqrt[3]{2} \neq a+p\sqrt{b}+q\sqrt{c}+r\sqrt{bc}, \quad \text{ни для каких} \quad a,b,c,p,q,r \in \mathbb{Q}.$$

Для этого достаточно доказать, что $\sqrt[3]{2} \neq u+v\sqrt{c}$ ни для каких чисел $u,v,c \in \mathbb{Q}[\sqrt{b}] := \{x+y\sqrt{b}\colon x,y \in \mathbb{Q}\}$. Идея доказательства состоит в том, что числа из $\mathbb{Q}[\sqrt{b}]$ (с фиксированным b) «ничуть не хуже» рациональных чисел, т. е. сумма, разность, произведение и частное чисел из $\mathbb{Q}[\sqrt{b}]$ тоже являются числами из $\mathbb{Q}[\sqrt{b}]$ (или, говоря научно, $\mathbb{Q}[\sqrt{b}]$ — *числовое поле*). Поэтому можно доказывать утверждение аналогично п. (e).

Набросок второго решения. Пусть число $\sqrt{2}+\sqrt[3]{2} = a+\sqrt{b}$ представимо. Оно является корнем многочлена $P(x) := ((x-\sqrt{2})^3-2)((x+\sqrt{2})^3-2)$ с рациональными коэффициентами. По п. (e) $\sqrt{2}+\sqrt[3]{2} \notin \mathbb{Q}$. Значит, $\sqrt{b} \notin \mathbb{Q}$. По лемме о сопряжении 2.2 (e) для $r=\sqrt{b}$, многочлен P имеет корень $a-\sqrt{b}$. Так как $\sqrt{b} \notin \mathbb{Q}$, то корни $a \pm \sqrt{b}$ различны. Но у многочлена P только два вещественных корня: $\sqrt{2}+\sqrt[3]{2}$ и $-\sqrt{2}+\sqrt[3]{2}$. Поэтому $a+\sqrt{b} = \sqrt{2}+\sqrt[3]{2}$ и $a-\sqrt{b} = -\sqrt{2}+\sqrt[3]{2}$. Отсюда $\sqrt[3]{2} = a \in \mathbb{Q}$. Противоречие.

(g) Пусть число $\cos(2\pi/9)$ представимо. По формуле косинуса тройного угла оно является корнем уравнения $4x^3-3x = -\frac{1}{2}$. По лемме 2.2 (f) это уравнение имеет рациональный корень. Противоречие.

Другой способ — аналогично теореме 2.3.

(h) Корнями многочлена $P(x) := (x^2-2)^2-2$ являются четыре числа $\pm\sqrt{2\pm\sqrt{2}}$, где знаки + и − не обязательно согласованы. Все

эти числа иррациональны. Значит, по теореме 2.3 достаточно доказать, что многочлен P не разлагается в произведение двух квадратных трехчленов с рациональными коэффициентами. Эта неразложимость следует из того, что произведение любых двух корней многочлена P иррационально.

(i) (Использован текст И. Брауде-Золотарёва.) Из равенства

$$\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) + \ldots + \cos(14\pi/7) = 0$$

получаем $\cos(2\pi/7)+\cos(4\pi/7)+\cos(6\pi/7) = -1/2$. Используя формулы косинуса двойного и тройного угла, получаем, что число $\cos(2\pi/7)$ является корнем уравнения $8t^3 + 4t^2 - 4t - 1 = 0$. Сделав замену $u = 2t$, получим $u^3+u^2-2u-1 = 0$. Это уравнение не имеет рациональных корней. Значит, уравнение $8t^3+4t^2-4t-1 = 0$ тоже не имеет рациональных корней. Поэтому многочлен $8t^3+4t^2-4t-1 = 0$ неприводим над $\mathbb{Q}$. Теперь непредставимость вытекает из леммы 2.2 (f).

(j) Аналогично п. (f).

2.3. Пусть, напротив, данный многочлен P имеет корень $x_0 = a \pm \sqrt{b}$. По лемме 2.2 (e) о сопряжении и аналогично ей, корнем многочлена P является также число $x_1 = a \mp \sqrt{b}$. При $b = 0$ утверждение очевидно. Поэтому считаем, что $b \neq 0$. Тогда $x_0 \neq x_1$. Значит, $P(x)$ делится на $(x - a)^2 - b$. Так как $\deg P > 2$, то многочлен P приводим. Противоречие.

2.4. Обозначим через $\sqrt{c}$ число, полученное при единственном извлечении корня, где $c \in \mathbb{Q}$. Докажите, что все полученные числа имеют вид $a + b\sqrt{c}$, где $a, b \in \mathbb{Q}$.

2.5. Ответ: тогда и только тогда, когда $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Или, эквивалентно, $\varphi(n) \in \{1, 2, 4\}$.

2.8. (a) $(x - y)^2(y - z)^2(z - x)^2$ — симметрический многочлен.

(Пункт (a) 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

$\sigma_1, \sigma_2, \sigma_3$. Само же M выражается через $M+N$ и MN по «формуле корней квадратного уравнения», см. формулы в начале п. 2.2.

2.9. (a) $x + y\varepsilon_3 + z\varepsilon_3^2$.

(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 2.8.b.

2.10. (a) Квадрат $(x-y)^2(x-z)^2(x-t)^2(y-z)^2(y-t)^2(z-t)^2$ симметричен, см. 2.8.a.

(b) Положим

$$M = xy + zt, \quad N = xz + yt, \quad K = xt + yz.$$

По 2.8.c, M «выразим в радикалах при помощи многочленов»

$$M + N + K, \quad MN + MK + NK, \quad MNK.$$

Аналогично решениям задач 2.8.c выше и 2.10.d ниже, эти многочлены симметрические. Поэтому $M = xy + zt$ радикален.

(c) 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 $x+y-z-t$.

Решение уравнения 4-й степени при помощи резольвент Лагранжа (решение задачи 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 2.11.a. 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 $x \to y \to z \to t \to x$ 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.

2.11. Используйте равенства $1 + \varepsilon + \varepsilon^2 = 0$ и $1 + i + i^2 + i^3 = 0$.

2.12. Для наглядности приведем решения при $q = 5$.

(a) 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,

$$Q(\varepsilon_5 u_1, \ldots, \varepsilon_5 u_5, y) = \prod_{\alpha\in\Sigma_5} (y - t(\varepsilon_5 \vec{u}_\alpha)) =$$

$$= \prod_{\alpha\in\Sigma_5} (y - t(\vec{u}_{\alpha\circ(54321)}) = Q(u_1, \ldots, u_5, y).$$

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 $\alpha \circ (54321)$.

(b) Для каждого $k = 0, 1, 2, \ldots, 120$ найдётся однородный многочлен $P_k \in \mathbb{Q}[\varepsilon_5][u_1, \ldots, u_5]$ («степени» $120 - k$) такой, что коэффициент при y^k в Q равен $P(u_1, \ldots, u_5)$, т.е.

$$Q(u_1, \ldots, u_5, y) = \sum_{k=0}^{120} P_k(u_1, \ldots, u_5) y^k.$$

По (a) и из однородности имеем

$$P_k(u_1, \ldots, u_5) = P_k(\varepsilon_5 u_1, \ldots \varepsilon_5 u_5) = \varepsilon_5^{-k} P_k(u_1, \ldots, u_5).$$

Если k не кратно 5, то $P_k(u_1, \ldots, u_5) = 0$, что и требовалось.

(c) Многочлен $Q(u_1, \ldots, u_5, y)$ симметричен по $u_1, \ldots, u_5$. Значит, все коэффициенты (P_k из пункта (b)) соответствующего многочлена из $\mathbb{Q}[\varepsilon_5, u_1, \ldots, u_q][y]$ симметричны по $u_1, \ldots, u_5$. Теперь утверждение $Q(x_1, \ldots, x_5, y) \in \mathbb{Q}[\varepsilon_5][y]$ следует из основной теоремы о

симметрических многочленах, формул Виета и того факта, что коэффициенты f рациональны.

Теперь утверждение $Q(x_1, \dots, x_5, y) \in \mathbb{Q}[y]$ доказывается аналогично [ZSS, !]

2.14. (a) Докажем, что существует такое $\alpha \in \mathbb{R}$, что $f(x, y) = \alpha(x - y)$.

Так как многочлен $f^2 = p$ симметрический, то можно считать, что многочлен q линеен по третьей переменной, т.е. $q(u, v, w) = a(u, v) + b(u, v)w$ для некоторых $a, b \in \mathbb{R}[u, v]$ (иначе изменим q, сохраняя f, p). Тогда $x = a(x + y, xy) + b(x + y, xy)f(x, y)$.

Первое завершение решения. Получаем $pb^2 = f^2b^2 = (x - a)^2 = (y - a)^2$. Отсюда по лемме 2.15.b $x - a = a - y$, так как случай $x - a = y - a$ невозможен. Значит, $a = (x + y)/2$. Тогда $(x - y)^2 = 4f^2b^2 = 4pb^2$. Если многочлен $p = f^2$ постоянный, то многочлен $b = \pm(x - y)/2\sqrt{p}$ не симметрический — противоречие. Поэтому многочлен p не постоянный. Тогда многочлен b постоянный. Значит, $2x = 2q = x + y + 2bf$, откуда $b \neq 0$ и $f = \alpha(x - y)$ для $\alpha = 1/2b$.

Второе завершение решения (написано с использованием текста И. Богданова). Так как многочлен x не симметрический и $x = q(x + y, xy, f(x, y))$, то многочлен f не симметрический. Тогда по лемме 2.16.a f антисимметрический. Значит, $y = q(x + y, xy, -f(x, y))$. Итак,

$$x = a + bf \quad \text{и} \quad y = a - bf,$$

$$\text{где} \quad a = a(x + y, xy), \quad b = b(x + y, xy) \quad \text{и} \quad f = f(x, y).$$

Тогда $x+y = 2a$ и $xy = a^2-b^2f^2$. Отсюда $(x-y)^2 = 4b^2f^2$. Аналогично первому завершению решения многочлен b постоянный. Значит, $f = \alpha(x - y)$ для $\alpha = \pm 1/2b$.

(b) Докажем, что k четно и существует такое $\alpha \in \mathbb{R}$, что $f(x, y) = \alpha(x - y)$. Индукция по k с применением п. (a) и обобщения лемм 2.15.be, 2.16. Если k нечетно, то из утверждения 2.16.b получаем, что f симметрический, что противоречит равенству $x = q(x + y, xy, f(x, y))$. Если $k = 4$, то 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).

2.15. (a) Определите *старший член* многочлена так, чтобы старший член произведения равнялся произведению старших членов сомножителей.

(b) Следует из п. (a).

(c) Имеем $f^2 + fg + g^2 = \left(f + \frac{g}{2}\right)^2 + \frac{3}{4}g^2 = (f - \varepsilon_3 g)(f - \varepsilon_3^2 g)$.

(d) Следует из п. (c).

(e) Следует из п. (f).

(f) Докажите и примените теорему Безу для многочленов от u с коэффициентами в $\mathbb{R}[v]$.

2.16. (a) Так как f^2 симметрический, то $f(x, y)^2 = f(y, x)^2$. Отсюда по утверждению 2.15.b $f(x, y) = \pm f(y, x)$.

(b) Используйте аналог утверждений 2.15.ce.

(c) См. указание к 2.15.f.

2.17. *Ответ:* 2.15.abf, 2.16.abc.

2.22. 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 2.23 о сохранении циклической симметричности.

Поскольку многочлен x не является циклически симметрическим, то он не является вещественно радикальным.

2.23. Доказательство можно найти в [Sk19, п. 9.4.2].

2.24. *Ответ:* 2.19.abcd, 2.20.b, 2.23 для всех q, не делящихся на 3.

К алгоритмам решения алгебраических уравнений

представляют Б. Вукорепа, А. Глебов,
А. Еннэ, А. Скопенков, А. Чиликов

Решения задач после промежуточного финиша

3.1. (b) Используйте аналог задачи 3.2.c для $n = 3$.

3.2. *Ответ:* (c) — верно, (a), (b), (d) — неверно.

(a) См. 2.9.a.

(b) Рассмотрите многочлен $x_1 + \varepsilon_5 x_2 + \varepsilon_5^2 x_3 + \varepsilon_5^3 x_4 + \varepsilon_5^4 x_5$.

(d) Рассмотрите многочлен $\prod\limits_{i<j}(x_i - x_j)$.

(c) Так как f^3 симметрический, то

$$f^3(x_1, x_2, x_3, x_4, x_5) = f^3(x_2, x_1, x_3, x_4, x_5).$$

Извлекая корень третьей степени, имеем

$$f(x_1, x_2, x_3, x_4, x_5) = \varepsilon_3^q f(x_2, x_1, x_3, x_4, x_5) = \varepsilon_3^{2q} f(x_1, x_2, x_3, x_4, x_5).$$

Отсюда $\varepsilon_3^{2q} = 1$, поэтому $\varepsilon_3^q = 1$. Аналогично $f(\vec{x}) = f(\vec{x}_\alpha)$ для любой перестановки α, меняющей местами два элемента из множества $\{x_1, x_2, x_3, x_4, x_5\}$. Поэтому f симметрический.

3.3. (a) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$.

(b) Докажите, что любая перестановка, переводящая в себя многочлен из задачи 3.2.d, является четной. А тогда она представляется в виде композиции циклов длины 3, см. [ZSS, п. 23.2.4].

3.4. Доказательство можно найти в [Sk15].

3.5. (c) Обозначим через a, b, c, d, e пять различных элементов данного множества. $(abc) = (ac)(de)(ab)(de)$.

3.6. *Ответ:* (a), (b) — нет.

Леммы 2.23 о сохранении циклической симметричности и 3.4 о сохранении четносимметричности верны и для рациональных функций, см. [Sk15], [Sk19, п. 9.4.2]. Далее аналогично решению задачи 2.22.

3.7. *Ответы*: (a), (c), (d), (e), (f), (h) — нет, (b), (g) — да.

Обозначим $r := \sqrt[3]{2}$.

(a) Пусть число $\sqrt{3}$ представимо.

Первое решение. Тогда

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Так как многочлен $x^3 - 2$ не имеет рациональных корней, то он неприводим над $\mathbb{Q}$. Значит, $2ab + 2c^2 = 2ac + b^2 = 0$ (ср. с задачей 3.8 (b)). Поэтому $b^3 = -2abc = 2c^3$. Тогда либо $b = c = 0$, либо $\sqrt[3]{2} = b/c$. Оба случая невозможны.

Второе решение. Обозначим $P(x) := x^2 - 3$. По лемме 3.8 (e) о сопряжении P имеет три корня x_0, x_1, x_2, введённых в формулировке леммы. Так как ни один из них не рационален, то равенство $b = c = 0$ невозможно. Значит, по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) эти корни различны. Противоречие.

(b) Имеем $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (Это равенство несложно получить методом неопределённых коэффициентов или при помощи алгоритма Евклида для многочленов $x^3 - 2$ и $x^2 + 5x + 1$, см. решение задачи 3.10.) Поэтому

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(c) Пусть число $\cos(2\pi/9)$ представимо. Оно является корнем уравнения $4x^3 - 3x = -\frac{1}{2}$. Два других его вещественных корня есть $\cos(8\pi/9)$ и $\cos(4\pi/9)$.

Применим второе решение пункта (a) для $P(x) := 8x^3 - 6x - 1$. Получим, что корни x_0, x_1, x_2 различны. Так как $\overline{\varepsilon_3} = \varepsilon_3^2$, то $\overline{x_2} = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Противоречие.

(d) Если число $\sqrt[5]{3}$ представимо, то по лемме о рациональности 3.8 (f) оно является корнем некоторого кубического многочлена. Противоречие с неприводимостью многочлена $x^5 - 3$ над $\mathbb{Q}$.

(e) Аналогично п. (a), (c) получаем, что комплексные корни многочлена $x^3 - 3$ есть числа x_0, x_1, x_2, введённые в формулировке леммы 3.8 (e). Поэтому $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ для некоторого $s \in \{1, 2\}$. Отсюда по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$

3.8 (b′) получаем, что $a = 0$ и $bc = 0$. Поэтому либо $\sqrt[3]{3} = br$, либо $\sqrt[3]{3} = cr^2$. Противоречие.

(f) Доказательство аналогично п. (c).

(g) Это уравнение имеет корень $\sqrt[3]{2} + \sqrt[3]{4}$.

(h) Единственный вещественный корень этого уравнения — $\sqrt[3]{3} + \sqrt[3]{9}$. Пусть, напротив, это число выражается в требуемом виде. Применим второе решение пункта (a) для $P(x) := x^3 - 9x - 12$. Получим, что числа x_0, x_1, x_2 — все корни многочлена P.

С другой стороны, все корни данного уравнения —

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Поскольку данное уравнение имеет ровно один вещественный корень, получаем, что $x_0 = y_0$ и либо $x_1 = y_1$, $x_2 = y_2$, либо, наоборот, $x_2 = y_1$, $x_1 = y_2$.

Обозначим $R(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$, а также $S(x) := a + brx + cr^2x^2$ и $S(x) := a + brx^2 + cr^2x$ для первого и второго случая соответственно. Тогда многочлен $R(x) - S(x)$ имеет 3 различных корня $1, \varepsilon_3, \varepsilon_3^2$. Но его степень не выше второй. Поэтому $R = S$. Значит, $\sqrt[3]{3} = br$ или $\sqrt[3]{3} = cr^2$. Противоречие.

3.8. (a) Если многочлен $x^3 - r^3$ приводим над $\mathbb{Q}$, то он имеет рациональный корень. Противоречие.

(b) Предположим противное. Поделим $x^3 - r^3$ на $a + bx + cx^2$ с остатком. По п. (a) остаток ненулевой. Оба многочлена $x^3 - r^3$ и $a + bx + cx^2$ имеют корень $x = r$. Значит, остаток имеет корень $x = r$. Следовательно, остаток имеет иррациональный корень. Противоречие с тем, что степень остатка равна 1.

(b′) Рассмотрите вещественную и мнимую части.

Замечание. Это утверждение равносильно неприводимости многочлена $x^3 - r^3$ над $\mathbb{Q}[\varepsilon_3]$. Если многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}[\varepsilon_3]$, то многочлен $k + lx + mx^2 \in \mathbb{Q}[\varepsilon_3][x]$ не может иметь корень r. Если многочлен $x^3 - r^3$ приводим над $\mathbb{Q}[\varepsilon_3]$, то один из сомножителей дает линейную зависимость чисел $1, r, r^2$ над $\mathbb{Q}[\varepsilon_3]$.

(c) Поделим многочлен с остатком на $x^3 - r^3$. Подставляя $x = r$, по лемме о линейной независимости п. (b) получаем, что остаток нулевой.

(d) По п. (c) получаем, что если $R^3 = r^3$, то R есть корень многочлена.

(e) Обозначим через P многочлен из условия, и пусть $G(t) := P(a + bt + ct^2)$. Тогда $G(r) = 0$. Значит, по п. (d) имеем $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(f) *Первое доказательство.* Достаточно доказать утверждение для $a = 0$. Для числа $t = br + cr^2$ выполнено равенство $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

Иными словами, ввиду того, что $u^3 + v^3 + w^3 - 3uvw$ делится на $u + v + w$, число $a + br + cr^2$ является корнем многочлена

$$(x - a)^3 - 3bcr^3(x - a) - b^3r^3 - c^3r^6.$$

Второе доказательство. Обозначим $x_0 = a + br + cr^2$. Разложим числа x_0^k при $k = 0, 1, 2, 3$ по степеням числа r:

$$x_0^k = a_k + b_k r + c_k r^2.$$

Достаточно найти числа $\lambda_0, \lambda_1, \lambda_2, \lambda_3 \in \mathbb{Q}$, не все из которых равны нулю, удовлетворяющие условию $\lambda_0 + \lambda_1 x_0 + \lambda_2 x_0^2 + \lambda_3 x_0^3 = 0$. Для этого нужно, чтобы эти числа удовлетворяли системе уравнений

$$\begin{cases} \lambda_0 a_0 + \ldots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \ldots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \ldots + \lambda_3 c_3 = 0. \end{cases}$$

Как известно, однородная (т. е. с нулевыми правыми частями) система линейных уравнений с рациональными коэффициентами, в которой уравнений меньше, чем переменных, имеет нетривиальное рациональное решение. Значит, требуемые числа найдутся.

Полученный многочлен имеет степень ровно 3 ввиду лемм 3.8 (e, b′).

Третье доказательство. Обозначим $A(x) := a + bx + cx^2$. Произведение $(x - A(t_0))(x - A(t_1))(x - A(t_2))$ является симметрическим многочленом от t_0, t_1, t_2. Значит, оно является многочленом от x и от элементарных симметрических многочленов от t_0, t_1, t_2. Значения этих элементарных симметрических многочленов при $t_k = r\varepsilon_3^k$, $k = 0, 1, 2$, равны коэффициентам многочлена $x^3 - r^3$, которые рациональны. Поэтому рассмотренное произведение является искомым многочленом.

3.9. По лемме о рациональности 3.8 (f) существует многочлен степени не выше 3 с корнем $a+br+cr^2$. Из этого факта и из неприводимости над $\mathbb{Q}$ данного многочлена P получаем, что $\deg P \leqslant 3$. По лемме о сопряжении 3.8 (e) многочлен P имеет три корня x_0, x_1, x_2, введённых в формулировке леммы. Так как многочлен P неприводим над $\mathbb{Q}$, то ни один из корней не рационален. Поэтому равенство $b = c = 0$ невозможно. Значит, по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) корни x_0, x_1, x_2 различны. Следовательно, $\deg P = 3$.

Так как $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, то $\overline{x_2} = x_1$. Значит, x_2 и x_1 не могут быть вещественными и различными. Следовательно, $x_2, x_1 \in \mathbb{C} - \mathbb{R}$. Поэтому P имеет ровно один вещественный корень.

3.10. Пусть при извлечении корня третьей степени получилось число r. Если $|r| \in \mathbb{Q}$, то утверждение очевидно. Если $|r| \notin \mathbb{Q}$, то многочлен $x^3 - r^3$ неприводим над $\mathbb{Q}$.

Достаточно доказать, что $\frac{1}{a+br+cr^2} = h(r)$ для некоторого многочлена h. По лемме о неприводимости, многочлен x^3-r^3 неприводим над $\mathbb{Q}$. Поэтому он взаимно прост с $a+bx+cx^2$. Значит, существуют многочлены g и h, для которых $h(x)(a+bx+cx^2)+g(x)(x^3-r^3) = 1$. Тогда h — искомый многочлен.

3.11. Обозначим $r := \sqrt[7]{2}$ и $A(x) := a_0 + a_1x + a_2x^2 + \ldots + a_6x^6$.

(a) Пусть число $\sqrt{3}$ представимо. Тогда по лемме о сопряжении 3.12 (c) многочлен $x^2 - 3$ имеет корни $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как этот многочлен не имеет рациональных корней, то по то по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) эти корни различны. Противоречие.

(b) Обозначим через P многочлен, для которого $\cos 7x = P(\cos x)$ (Докажите, что такой многочлен существует!).

Первое решение. Пусть число $\cos\frac{2\pi}{21}$ представимо. Аналогично п. (a) данный многочлен P имеет попарно различные корни $x_k := A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как $P(0) > 0$, $P(1) < 0$ и $P(2) > 0$, то многочлен P имеет вещественный корень x_k, отличный от x_0. Имеем $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Поэтому $x_k = \overline{x_k} = x_{7-k}$. Противоречие.

Второе решение. Корнями многочлена $2P(x)+1$ являются вещественные числа $y_k := \cos\frac{2(3k+1)\pi}{21}$ при $k = 0, \ldots, 6$. Одно из них, а именно $y_2 = -1/2$, рационально.

В следубщем абзаце мы докажем, что число y_0 иррационально. (Иначе из равенства $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$ следует, что $\varepsilon_{21} = a + i\sqrt{b}$ для некоторых $a, b \in \mathbb{Q}$. Тогда и число $\varepsilon_7 = \varepsilon_{21}^3$ тоже имеет такой вид. Но ε_7 является корнем неприводимого[4] многочлена $1 + x + \ldots + x^6$, что противоречит аналогу теоремы 2.3 для чисел вида $a + i\sqrt{b}$.)

Итак, число y_0 иррационально и является корнем многочлена $\frac{2P(x)+1}{2x+1}$ степени 6. Тогда по леммам о сопряжении 3.12 (c) и о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) этот многочлен имеет семь попарно различных корней, что невозможно.

(c) Пусть число $\sqrt[11]{3}$ представимо. Тогда по лемме о рациональности 3.12 (d) существует ненулевой многочлен степени не выше 7 с корнем $\sqrt[11]{3}$. Противоречие с неприводимостью многочлена $x^{11} - 3$ над $\mathbb{Q}$.

(d) Пусть число $\sqrt[7]{3}$ представимо. Аналогично п. (a) все комплексные корни многочлена $x^7 - 3$ есть $A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Поэтому $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ для некоторого $s \in \{1, 2, 3, 4, 5, 6\}$. Отсюда по лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) $a_k = 0$ для любого $k \neq s$. Поэтому $\sqrt[7]{3} = a_s r^s$. Противоречие.

(e) Пусть какой-нибудь из корней представим. Данный многочлен P не имеет рациональных корней. Тогда по лемме о сопряжении 3.12.c и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14.b P имеет попарно различные корни $x_k := A(r\varepsilon_7^k)$ для $k = 0, 1, 2, \ldots, 6$. Так как $P(0) > 0$, $P(1) < 0$ и $P(2) > 0$, то P имеет вещественный корень x_k, отличный от x_0. Имеем $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Поэтому $x_k = \overline{x_k} = x_{7-k}$. Противоречие.

3.12. (a) Все корни многочлена $x^q - r^q$ есть $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Пусть он приводим над $\mathbb{Q}$. Модуль свободного члена одного из унитарных сомножителей разложения рационален и равен произведе-

[4]Неприводимость многочлена $g(x) = 1 + x + \ldots + x^6$ можно показать, например, применив признак Эйзенштейна [ZSS, п. 5.5.2] к многочлену $g(x+1)$. Впрочем, здесь достаточно доказать, что у него нет рациональных делителей степени 1 и 2.

нию модулей некоторых k из этих корней, $0 < k < q$. Значит, $r^k \in \mathbb{Q}$. Так как q простое, то имеем $kx + qy = 1$ для некоторых целых x, y. Тогда $r = (r^k)^x (r^q)^y \in \mathbb{Q}$. Противоречие.

(b) Предположим противное. Рассмотрим многочлен $A(x)$ наименьшей степени, для которого лемма не выполняется. Поделим $x^q - r^q$ на $A(x)$ с остатком $R(x)$. Тогда $\deg R < \deg A$, $R(r) = 0$ и по п. (a) многочлен $R(x)$ ненулевой. Противоречие с выбором A.

(c) Доказательство аналогично задачам 2.2 (c, d), 3.8 (d). Используйте п. (b).

(d) Доказательства повторяют второе и третье доказательства леммы о рациональности 3.8 (f). Нужно только везде заменить 3 на q и 2 на $q-1$ (например, во второй строчке второго доказательства $k = 0, 1, 2, \ldots, q$).

3.13. (a) Пусть многочлен приводим. Свободный член одного из унитарных сомножителей разложения лежит в $\mathbb{Q}[\varepsilon_q]$ и равен $\pm r^k \varepsilon_q^m$ для некоторого m. Поэтому $r^k \in \mathbb{Q}[\varepsilon_q]$. Далее аналогично лемме 3.12 (a) получаем $r \in \mathbb{Q}[\varepsilon_q]$. Противоречие.

Пункты (b) и (c) выводятся из п. (a) аналогично соответствующим пунктам задачи 3.12.

3.14. (a) Пусть многочлен приводим. Аналогично доказательству леммы о неприводимости над $\mathbb{Q}[\varepsilon_q]$ 3.13 (a) имеем $r \in \mathbb{Q}[\varepsilon_q]$. Поэтому $r^2, r^3, \ldots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

В следубщем абзаце мы докажем, что имеется многочлен степени меньше q с корнем r. Это будет противоречить неприводимости многочлена $x^q - r^q$ над $\mathbb{Q}$.

Разложим число r^k по степеням числа ε_q для $k = 0, 1, \ldots, q-1$:

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \ldots + a_{k,q-2}\varepsilon_q^{q-2}.$$

Достаточно найти числа $\lambda_0, \ldots, \lambda_{q-1} \in \mathbb{Q}$, не равные одновременно нулю, для которых

$$\lambda_0 a_{0,m} + \ldots + \lambda_{q-1} a_{q-1,m} = 0 \quad \text{при любом} \quad m = 0, 1, \ldots, q-2.$$

Такие числа существуют по аналогии с соответствующим рассуждением во втором доказательстве леммы о рациональности 3.8 (f).

(b) Утверждение вытекает из п. (a).

3.15. Предположим противное. Обозначим данный многочлен через P. При $q < \deg P$ получаем противоречие с леммой о рациональности 3.12 (d). При $q \geqslant \deg P$ по лемме о сопряжении 3.12 (c) и лемме о линейной независимости над $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) многочлен P имеет попарно различные корни $x_k = A(r\varepsilon_q^k)$ для $k = 0, 1, 2, \ldots, q-1$. При $q > \deg P$ получаем противоречие. При $q = \deg P$ из условий $q \neq 2$ и $\overline{x_k} = x_{q-k} \neq x_k$ получаем единственность вещественного корня.

Список литературы

[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.

[Ar84] *Арнольд В.И.* Обыкновенные дифференциальные уравнения, М. Наука, 1984.

[Dor] *Dörrie H.* 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[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.

[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.

[Ka] *Канунников А. Л.* Начала теории Галуа: разрешимость алгебраических уравнений в радикалах. http://www.mathnet.ru/conf1015.

[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.

[Ler] *Lerner L.* Galois Theory without abstract algebra. http://arxiv.org/abs/1108.4593.

[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.

[Saf] *Сафин А.* Программа для построения правильных многоугольников циркулем и линейкой (доклад на ММКШ-2008). http://www.mccme.ru/mmks/dec08/Safin.pdf.

[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.

[Sk19] *Skopenkov A.* Mathematics via problems: from olympiades and math circles to a profession. Algebra. AMS, Providence, to appear.

[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.

[ZSS] Элементы математики в задачах: через олимпиады и кружки к профессии. Сборник под редакцией А. Заславского, А. Скопенкова и М. Скопенкова. МЦНМО, 2018. http://www.mccme.ru/circles/oim/materials/sturm.pdf.

4 Additional problems for successful teams

4.1. (a) Let $x, y, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$ and

$$\begin{cases} r^2 = p(x + y, xy) \\ g(x, y) = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.c). Then $r \in \mathbb{Q}(x, y)$.

(b) Let $x, y, r \in \mathbb{R}$, $p \in \mathbb{Q}[\sqrt{2}][u, v]$, $g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy, \sqrt{2})$ and the equations of (a) hold. Then there are $\rho \in \mathbb{Q}(x, y)$, $\pi \in \mathbb{Q}[\sqrt{2}][u, v]$ and $\pi_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ such that the equations of (a) hold with r, p, p_1 replaced by ρ, π, π_1.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing $x + y, xy, r^2$ but not r. If $F(r) \cap \mathbb{Q}(x, y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x, y)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

4.2. Denote $a_j = \sigma_j(x_1, x_2, x_3)$, $j = 1, 2, 3$.

(a) Let $x_1, x_2, x_3, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u_1, u_2, u_3]$ and $p_1 \in \mathbb{Q}[u_1, u_2, u_3, v]$ be such that $g(x_1, x_2, x_3) \notin \mathbb{Q}(a_1, a_2, a_3)$ and

$$\begin{cases} r^2 = p(a_1, a_2, a_3) \\ g(x_1, x_2, x_3) = p_1(a_1, a_2, a_3, r) \end{cases}.$$

Then $r \in \mathbb{Q}(x_1, x_2, x_3)$.

(b) **Rationalization Lemma.** Let $x_1, x_2, x_3, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing a_1, a_2, a_3, r^2 but not r. If $F(r) \cap \mathbb{Q}(x_1, x_2, x_3) \not\subset F$, then there is $\rho \in \mathbb{Q}(x_1, x_2, x_3)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

(c) **Proposition.** If $x_1, x_2, x_3 \in \mathbb{R}$ and x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals, then x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals so that every radical is in $\mathbb{Q}(x_1, x_2, x_3)$.

4.3. (a) Let $x, y, r \in \mathbb{C}$, $p \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that

$$\begin{cases} r^3 = p(x + y, xy) \\ x = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.d for $k = 3$). Then $r \in \mathbb{Q}[\varepsilon_3](x, y)$.

(b) Same as (a) with $x = p_1(x + y, xy, r)$ replaced by $g(x, y) = p_1(x + y, xy, r)$ for some $g \in \mathbb{Q}[u, v]$ such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{C}$ and $F \subset \mathbb{C}$ a field containing $x+y, xy, \varepsilon_3, r^3$ but not r. If $F(r) \cap \mathbb{Q}(x,y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x,y)$ such that $\rho^3 \in F$ and $F(\rho) = F(r)$.

(d) **Rationalization Lemma.** Same as (c) with x, y replaced by $x_1, \ldots, x_n$ and $x+y, xy$ replaced by $\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)$.

(e) **Rationalization Lemma.** Same as (d) with r^3, ρ^3 replaced by r^q, ρ^q for a prime q and ε_3 replaced by ε_q.

(f) **Proposition.** If

$$x_1, \ldots, x_n \in \mathbb{C}, \quad M := \{\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\}$$

and x_1 is M-expressible by radicals, then x_1 is M-expressible by radicals so that every radical is in $\bigcup_{q=3}^{\infty} \mathbb{Q}[\varepsilon_q](x_1, \ldots, x_n)$.

4.4. There are numbers $x, y \in \mathbb{R}$ such that if $p \in \mathbb{Q}[u,v]$ and $p(x,y) = 0$, then $p = 0$.

Such numbers are called *algebraically independent over* $\mathbb{Q}$.

4.5. (a) Докажите достаточность в критерии 2.13 Галуа разрешимости уравнения.

(b) Докажите необходимость в критерии 2.13 для $n \leqslant 4$.

(c) Сформулируйте и докажите аналог критерия 2.13 для 1-радикальности (т.е. для радикальности с одним извлечением корня).

(d) Сформулируйте и докажите вещественный аналог критерия 2.13.

4.6. Пусть $x_1, \ldots, x_n \in \mathbb{C}$ — все корни многочлена $A \in \mathbb{Q}[t]$ с учетом кратности, q простое, $r \in \mathbb{C} - \mathbb{Q}$, $r^q \in \mathbb{Q}$, $U \in \mathbb{Q}[\vec{u}]$,v $U(\vec{x}) \in \mathbb{Q}[r] - \mathbb{Q}$ и $\mathrm{id} \in G \subset \Sigma_n$.

(a) Верно ли, что если $\sum_{\alpha \in G} U(\vec{x}_\alpha) \in \mathbb{Q}$, то $\sum_{\alpha \in G} U(\vec{x}_{\alpha\tau}) \in \mathbb{Q}$ для любой перестановки $\tau \in \Sigma_n$?

(b) Верно ли, что если $\prod_{\alpha \in G} (t - U(\vec{x}_\alpha)) \in \mathbb{Q}[t]$, то $\sum_{\alpha \in G} (t - U(\vec{x}_{\alpha\tau})) \in \mathbb{Q}[t]$ для любой перестановки $\tau \in \Sigma_n$?

Toward algorithms of solving algebraic equations

presented by A. Enne, A. Chilikov,
A. Glebov, A. Skopenkov, B. Vukorepa *

1 Introduction and statements of results

1.1 What is this collection of problems about

There are famous Ruffini, Abel and Galois Theorems 2.7, 1.3, 1.4[1] on insolvability of algebraic equations in radicals. They are classical results of algebra, which are interesting for the computer science (theory of symbolic computations). All these theorems are formulated below.

The main content of this text is exposition of deep algebraic ideas (more precisely, of Galois theory) via simple and beautiful proofs of these theorems (see [ZSS, § 27]). It is the more remarkable that for these proofs one only needs the abilities to prove irrationality, to divide polynomials with a remainder, to take the root of a complex number, to multiply permutations, and to solve systems of linear equations. Even those who will not arrive to a complete proof of main results could solve research problems (see [E2, Es, AB, Ko17, Saf] and the references therein).

*We are grateful to Ya. Abramov, G. Chelnokov, D. Eliseev, A. Kanunnikov, N. Khoroshavkina, O. Orel, A. Petukhov and the jury of SCTT for useful discussions and for translation of some parts of the text.

A. Enne: Petrozavodsk State University.
A. Chilikov: Bauman Moscow State Technical University, Moscow Institute of Physics and Technology.
A. Glebov: Novosibirsk State University.
A. Skopenkov: Moscow Institute of Physics and Technology, Independent University of Moscow. http://www.mccme.ru/~skopenko.
B. Vukorepa: University of Zagreb.

[1]From §1 in what follows we use only §1.5, so you can read that subsection and start solving problems.

Before proving the insolvability of algebraic equations we consider a general way for their solution: Lagrange resolvent method . In fact, the main idea of Abel and Galois is the following: if an equation is solvable in radicals at all, then it is solvable by Lagrange method. Lagrange method is used to construct algorithms, e.g. to recognize whether the equation is solvable by radicals.

For practical purposes approximative methods of solving equations are more useful than 'radical formulae'. Besides, the equation can be solved using transcendental functions (see Vieta method [ZSS, § 4.2] and [PSo]; for further development of these ideas see e.g. [Sk10]). However, the problem of 'solvability in radicals' is interesting as a test problem of the modern theories of symbolic computations and computational complexity.

On the novelty. Proofs which are provided in solutions are not assumed to be new (but the reader could find new proofs). However, this text contains many pedagogical inventions (see [ZSS, §5.2.1, 5.2.2]). The proofs are different from proofs which are presented and quoted in [ZSS, §5]. Unfortunately, the proofs presented here are not well-known. Standard textbooks of algebra first expose Galois theory and then use its results to prove these theorems. However, it is much more economic and clearer not only to solve directly quadratic and cubic equations but also to prove corresponding theorems directly[2] . Of course, for such direct proofs, one should re-discover and use key ideas of Galois theory.

[2]See e.g. [Dor, § 25], [Pr07-2, appendix 8], [FT, Lecture 5], [ZSS, §5], [Dor, St94, Kol, Ler, T, Sk11, Sk15] and this text. Exposition in [Al] is closer to this 'direct' style. Large part of [Al] contains theory not required to prove the weak version of Abel theorem announced as the main result, see [Sk15, end of remark 7]. However, the author of [Al] succeeded in avoiding unmotivated exposition of the most complicated part of the theory. The proof from [Al] is exposed a shorter and easier way in [FT, Lecture 5], [Sk11].
Note that proofs in many of these sources are incomplete. See [ZSS, footnote 12 in p. 113 and end of §5.5.4], [Sk15, Discussion]. In spite of these drawbacks the above elementary expositions were more useful to us than formal expositions (in standard textbooks intended for the theory) which start with several hundreds pages of definitions and results whose role in the proof of the insolvability theorem is not clear at the moment of their statements.

1.2 Insolvability in real radicals

A real number is called **expressible by real radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number, and taking the n-th root of a positive number, where n is a positive integer. In other words, a real number a is expressible by real radicals if some set containing this number can be obtained starting from the set $\{1\}$ and using the following operations. To a given set $M \subset \mathbb{R}$ containing numbers $x, y \in M$ one can add

$$\text{numbers} \quad x+y, x-y, xy, \quad \text{number } x/y \text{ when } y \neq 0,$$

$$\text{and number } \sqrt[n]{x} \text{ for } x > 0 \text{ and integer } n > 0.$$

A number a is expressible by real radicals if and only if there exist

- positive integers $s, k_1, \ldots, k_s$,
- real numbers $f_1, \ldots, f_s$ and polynomials $p_0, p_1, \ldots, p_s$ with rational coefficients of $0, 1, \ldots, s$ variables respectively such that

$$\begin{cases} f_1^{k_1} = p_0 \\ f_2^{k_2} = p_1(f_1) \\ \ldots \\ f_s^{k_s} = p_{s-1}(f_1, \ldots, f_{s-1}) \\ a = p_s(f_1, \ldots, f_s) \end{cases}.$$

Remark 1.1. (a) Any real root of a quadratic equation with rational coefficients is expressible by real radicals.

(b) The equation $x^3 + x + 1 = 0$ has exactly one real root which is expressible by real radicals [ZSS, §4.2], see also Problem 2.8 (c).

(c) The equation $x^4 + 4x - 1 = 0$ has two real roots; both of them are expressible by real radicals [ZSS, §4.2], see also Problem 2.10 (d).

(d) Any real constructible number [ZSS, §5.1.2] is expressible by real radicals.

(e) There exists a cubic polynomial with rational coefficients such that none of its roots is expressible by real radicals (for example, $x^3 - 3x + 1$). (This statement is proven in Remark (f).)

(f) The number $\cos(2\pi/9)$ is not expressible by real radicals.

Let us apply the triple-angle formula for cosine. Then the numbers $\cos(2\pi/9)$, $\cos(8\pi/9)$, $\cos(14\pi/9)$ are the roots of the polynomial $8y^3 - 6y + 1 = 0$. By Theorem 1.2 none of these numbers is expressible by real radicals.

(g) The trisection of an angle is impossible in real radicals. That is, there exists a number α (for example, $\alpha = 2\pi/3$) such that the number $\cos\alpha$ is expressible by real radicals and the number $\cos(\alpha/3)$ is not expressible by real radicals. (This statement follows from Remark (f).)

Theorem 1.2 (solvability in real radicals)**.** For a cubic polynomial with rational coefficients the following conditions are equivalent:

(i) the polynomial has either at least one rational root or exactly one real root;

(ii) the polynomial has a root which is expressible by real radicals;

(iii) all the real roots of the polynomial are expressible by real radicals.

The uniqueness of the real root of the 'shortened' equation $x^3 + px + q = 0$ is equivalent to the following condition: '$p = q = 0$ or $(p/3)^3 + (q/2)^2 > 0$' [ZSS, Problem 8.1.5.d].

Obviously, $(ii) \Leftrightarrow (iii)$. This follows from Remark 1.1.a. The solvability in Theorem 1.2 (that is $(i) \Rightarrow (ii)$) can be proved by *del Ferro method* [ZSS, §4.2]; see another proof in §2.3. The insolvability in Theorem 1.2 (that is $(ii) \Rightarrow (i)$) has more complicated proof. It is easier to prove the similar result on *insolvability in polynomials*, see § 2.5.

1.3 Insolvability in complex radicals

Now consider formulae which involve complex numbers. It turns out that a cubic equation (for example, $x^3 - 3x + 1$) that is not solvable in real radicals can be solved in complex radicals.

A complex number is called **expressible by radicals** if it can be obtained using number 1 and operations of addition, subtraction, multiplication, division by a non-zero number and taking the n-th root, where n is a positive integer.

In other words, a complex number a is expressible by radicals if some set containing this number can be obtained starting from the set $\{1\}$ and using the following operations. To a given set $M \subset \mathbb{C}$

containing numbers $x, y \in M$ one can add

$$\text{numbers} \quad x+y, x-y, xy, \quad \text{number } x/y \text{ when } y \neq 0,$$

and any number $r \in \mathbb{C}$ such that $r^n = x$ for some integer $n > 0$.

For example, any (complex) root of a quadratic equation with rational coefficients is expressible by radicals. Similar assertions hold for equations of 3-rd and 4-th degree. These assertions can be proved by *del Ferro and Ferrari methods* [ZSS, §4.2]; see another proof in §2.3. However, analogous assertions for equations of higher degrees do not hold.

Theorem 1.3 (Galois)**.** There exists an equation of 5-th degree with rational coefficients (for example, $x^5 - 4x + 2 = 0$) neither of whose roots are expressible by radicals.

The famous problem of solvability in radicals was solved by weaker Ruffini-Abel theorems proved a little earlier. The Ruffini Theorem 2.7 has more complicated statement. But it leads us to the proof of Galois theorem. The precise statement of Abel theorem is even more complicated. It is not presented here, see [Sk15, Remark 7]. An easier way to solve the solvability problem is to prove the following Galois Theorem 1.4. This theorem is weaker than Galois Theorem 1.3 and has an easier proof. For $X \subset \mathbb{C}$, a complex number a is called *X-expressible by radicals* if a can be expressed using the set $X \cup \{1\}$ and the operations from the definition of the expressibility by radicals.

Theorem 1.4 (Galois)**.** There are $a_0, a_1, a_2, a_3, a_4 \in \mathbb{C}$ such that no root of the equation $x^5 + a_4x^4 + \ldots + a_1x + a_0 = 0$ is $\{a_0, a_1, \ldots, a_4\}$-expressible by radicals.

Theorem 1.5. There is an algorithm to recognize whether all the roots of the equation $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ are expressible by radicals (if $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ are known).

Theorem 1.5 is proved using Galois Solvability Criterion 2.13.b and an estimation of the number of operations.

1.4 Plan

This project consists of three formally independent parts. In the first two parts the definition of 'expressibility by radicals' from §2.2 is used.

(1) In §2.3 we discuss Lagrange's resolvent method used to solve equations. Formally this method is not used to prove insolvability. However, familiarity with this method is useful because

• proofs of insolvability were invented during the analysis of this method,

• this familiarity helps to check intermediate conjectures (which occur in attempts to prove insolvability), and

• this method is required to prove Theorem 1.5.

(2) The proof of the Ruffini theorem 2.7 is based on the idea of symmetry and is sketched in §3.1. This proof is prepared by §2.5. Subsection 2.4 prepares to §2.5 and to the proof of Galois Theorem 1.4.

(3) The proof of Theorem 1.2 on solvability in real radicals is based on the idea of conjugation (or of algebraic symmetry). This proof is prepared by §2.1, §3.2 and §3.3.

Theorems 1.3 and 1.5 are not proved here. See the proof of Theorem 1.3 in [ZSS, §5], [Sk19, §9]. Galois Theorem 1.4 is proved in additional problems, cf. [Sk15], [Sk19, §5]. The proof is based on reduction to Ruffini Theorem 2.7 using the idea of conjugation (§2.1, §3.2 and §3.3).

1.5 Recommendations for participants

For every solution which has been written down and marked with either '+' or '+.' a student (or a group of students) get a 'bean'. The jury may also award extra bean for beautiful solutions, solutions of hard problems, or solutions typeset in TEX. The jury has infinitely many beans. One may submit a solution in oral form, but one loses a bean with each 5 attempts (successful or not).

If a problem is marked by bold and named 'theorem' ('lemma', 'corollary', etc.), then this statement is important. Usually we provide (as a problem) the *formulation* of beautiful or important statement *before* its *proof*. In this case to prove this statement one possibly needs to solve next problems. If you are stuck on a certain problem, try looking at the next ones. They may turn out to be helpful. We suggest to all the students working on the project to *consult* the jury on any questions on the project. Students who successfully work on the project will get interesting *extra problems*.

Please notify us if you already know solutions of several problems. If you confirm your knowledge by presenting some of them, you will be allowed not to receive plus-marks for their solutions, but to use them in solutions of other problems.

2 Problems before the semifinal

In this text equality signs involving polynomial f (or f_j) mean equality of polynomials (i.e. componentwise equality). In §§2.1, 3.2 and 3.3 'polynomial with rational coefficients' is called a 'polynomial'. Denote

$$\varepsilon_q := \cos(2\pi/q) + i\sin(2\pi/q).$$

2.1 Representability using only one square root

2.1. Can the following number be represented as $a+\sqrt{b}$ with $a, b \in \mathbb{Q}$:

(a) $\sqrt{3+2\sqrt{2}}$; (b) $\frac{1}{7+5\sqrt{2}}$; (c) $\sqrt[3]{7+5\sqrt{2}}$; (d) $\cos(2\pi/5)$;

(e) $\sqrt[3]{2}$; (f) $\sqrt{2}+\sqrt[3]{2}$; (g) $\cos(2\pi/9)$;

(h)* $\sqrt{2+\sqrt{2}}$; (i)* $\cos(2\pi/7)$; (j) $\sqrt{2}+\sqrt{3}+\sqrt{5}$?

Lemma 2.2. Assume that $r \in \mathbb{R}-\mathbb{Q}$ and $r^2 \in \mathbb{Q}$.

(a) **Irreducibility.** The polynomial x^2-r^2 is irreducible over $\mathbb{Q}$.

(b) **Linear independence.** If $a, b \in \mathbb{Q}$ and $a+br=0$, then $a=b=0$.

(c) If r is a root of a polynomial, then this polynomial is divisible by x^2-r^2.

(d) **Conjugation.** If r is a root of a polynomial, then $-r$ is also its root.

(e) **Conjugation.** If $a, b \in \mathbb{Q}$ and a polynomial has a root $a+br$, then $a-br$ is also a root of this polynomial.

(f) If $a, b \in \mathbb{Q}$ and a cubic polynomial has a root $a+br$, then this polynomial has a rational root.

Theorem 2.3. If a polynomial of degree at least 3 is irreducible over $\mathbb{Q}$, then none of its roots equals to $a \pm \sqrt{b}$ for some $a, b \in \mathbb{Q}$.

Lemma 2.4 (Extension)**.** Suppose we can obtain a number using number 1, several operations of addition, subtraction, multiplication,

division by a non-zero number and exactly one operation of taking the square root of a positive number. Then the number can be represented as $a \pm \sqrt{b}$, where $a, b \in \mathbb{Q}$ and $b > 0$.

2.5.* Find all n such that the number $\cos(2\pi/n)$ can be represented as $a + \sqrt{b}$, where $a, b \in \mathbb{Q}$.

Hints to §2.1

2.2. (a) If the polynomial $x^2 - r^2$ is reducible over $\mathbb{Q}$, then it has a rational root. This is a contradiction.

(b) If $b \neq 0$, then $r = -a/b \in \mathbb{Q}$, which is impossible. Hence $b = 0$, thus $a = 0$.

(c) Divide our polynomial with a remainder[3] by $x^2 - r^2$:

$$P(x) = (x^2 - r^2)Q(x) + mx + n.$$

Substitute $x = r$. By the Linear independence lemma (see (b)) the reminder is equal to zero.

(d) By (c) if $R^2 = r^2$, then R is a root of the polynomial.

(e) Let P be given polynomial, and set $G(t) := P(a + bt)$. Then $G(r) = 0$. Hence by (d) we obtain $G(-r) = 0$.

(f) If $b = 0$ the assertion is proved. Otherwise by (e) the polynomial has the roots $a \pm br$. These roots are distinct. Hence the third root is rational by the Vieta theorem.

2.4. It would suffice to prove that the set of all numbers of the form $a \pm \sqrt{b}$ is closed under operations of addition, subtraction, multiplication and division. This is obviously false: $(1 + \sqrt{2}) + (1 + \sqrt{3})$ cannot be represented as $a \pm \sqrt{b}$, where $a, b \in \mathbb{Q}$ (prove this!).

2.2 Definition of the expressibility by radicals for polynomials

The solution of quadratic equation can be expressed by the following formulae:

$$(x - y)^2 = (x + y)^2 - 4xy \quad \text{and} \quad x = \frac{x + y + (x - y)}{2}.$$

[3]The division with a reminder is equivalent to 'replacing' x^2 by r^2.

These formulae show that *the root x of a quadratic equation is expressible by radicals* using the coefficients $x+y, xy$ of the equation. The rigorous definition of expressibility by radicals is given below.

Denote the elementary symmetric polynomials by

$$\sigma_1(x_1,\dots,x_n) := x_1+\dots+x_n, \quad \dots, \quad \sigma_n(x_1,\dots,x_n) = x_1\cdot\dots\cdot x_n.$$

If the number n and the arguments $x_1,\dots,x_n$ are clear from the context, we omit them from the notation.

A polynomial $p\in\mathbb{C}[x_1,\dots,x_n]$ is called **expressible by (complex) radicals**, if one can add p to the collection $\{\sigma_1,\dots,\sigma_n\}\cup\mathbb{C}$ of polynomials by a sequence of the following operations:

• if the polynomials f and g are already contained in the collection one can add their sum $f+g$ and their product fg;

• if the polynomial g is already contained in the collection and $g=f^k$ for some $f\in\mathbb{C}[x_1,\dots,x_n]$ and integer $k>1$ one can add f to the collection.

Remark 2.6. (a) E.g. if a collection contains x^2+2y and $x-y^3$, then one may apply the first operations and add the polynomial

$$-5(x^2+2y)^2+3(x^2+2y)(x-y^3)^6$$

to the collection; moreover, if a collection already contains $x^2-2xy+y^2$, then one may apply the second operation and add $x-y$ (or $y-x$).

(b) If we use only first operations we can add a polynomial with complex coefficients of polynomials which are already available.

(c) By Vieta theorem $\sigma_1,\dots,\sigma_n$ are the coefficients of the polynomial

$$t^n-\sigma_1t^{n-1}+\dots+(-1)^{n-1}\sigma_{n-1}t+(-1)^n\sigma_n\in\mathbb{C}[x_1,\dots,x_n][t]$$

with roots $x_1,\dots,x_n$. Therefore, the expressibility by radicals of the polynomial x_1 is equivalent to the expressibility (in the above sense) of its root x_1 in terms of the coefficients of this polynomial.

(d) The polynomial x_1 is expressible by radicals if and only if there exist:

• positive integers $s,k_1,\dots,k_s$,

• polynomials $f_1, \dots, f_s$ and $p_0, p_1, \dots, p_s$ with complex coefficients of n and of $n, n+1, \dots, n+s$ variables respectively, such that

$$\begin{cases} f_1^{k_1} = p_0(\sigma_1, \dots, \sigma_n) \\ f_2^{k_2} = p_1(\sigma_1, \dots, \sigma_n, f_1) \\ \dots \\ f_s^{k_s} = p_{s-1}(\sigma_1, \dots, \sigma_n, f_1, \dots, f_{s-1}) \\ x_1 = p_s(\sigma_1, \dots, \sigma_n, f_1, \dots, f_s) \end{cases} .$$

Here we omit the variables $(x_1, \dots, x_n)$ of the polynomials $\sigma_1, \dots, \sigma_n, f_1, \dots, f_s$.

(e) Given $x + y$ and xy, is it always possible to find x?

A simple formalization of this question is the following: *does there exist a map* $f : \mathbb{R}^2 \to \mathbb{R}$ *such that* $f(x + y, xy) = x$ *for any* $x, y \in \mathbb{R}$*?* The answer is no. Indeed, consider the pairs $x = 1, y = 2$ and $x = 2, y = 1$. Therefore, the expressibility by radicals does not allow 'to find x' in the sense described above.

Analogously, given $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$ and $\sigma_3 = xyz$ is it not always possible to find $(x - y)(y - z)(z - x)$. Indeed, consider the triples $x = 0, y = 1, z = -1$ and $x = 0, y = -1, z = 1$.

Theorem 2.7 (Ruffini)**.** For every positive integer $n \geqslant 5$ the polynomial x_1 is not expressible by radicals.

The proof shows that even the polynomial $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$ is not expressible by radicals for $n = 5$.

2.3 Solution of equations of low degrees

2.8. Which of the following polynomials are expressible by radicals for $n = 3$?

(a) $(x - y)(y - z)(z - x)$; (b) $x^9y + y^9z + z^9x$; (c) x.

To solve Problem 2.8 and the following problems, one can use the fundamental theorem on symmetric polynomials,see for example [Sk19, 4.6.3c]. Hints for part (c) are Problems 2.9.a and 2.11.c.

2.9. A polynomial $f \in \mathbb{C}[u_1, u_2, \dots, u_n]$ is called **cyclic symmetric** if $f(u_1, u_2, \dots, u_n) = f(u_2, u_3, \dots, u_{n-1}, u_n, u_1)$.

(a) Find at least one pair $\alpha, \beta \in \mathbb{C}$ such that the polynomial $(u + v\alpha + w\beta)^3$ is cyclic symmetric, but the polynomial $u + v\alpha + w\beta$ is not.

(b) Express $x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1$ by operations from the definition of expressibility by radicals starting with some *cyclic symmetric* polynomials in $x_1, x_2, \dots, x_{10}$.

2.10. Which of the following polynomials are expressible by radicals for $n = 4$?

(a) $(x-y)(x-z)(x-t)(y-z)(y-t)(z-t)$;

(b) $xy + zt$; (c) $x + y - z - t$; (d) x.

2.11. Solve the following systems of equations (x, y, z, t are unknowns, a, b, c, d are known):

$$\text{(a)} \quad \begin{cases} x+y+z+t=a, \\ x+y-z-t=b, \\ x-y+z-t=c, \\ x-y-z+t=d; \end{cases} \qquad \text{(b)} \quad \begin{cases} x+y+z+t=a, \\ x+iy-z-it=b, \\ x-y+z-t=c, \\ x-iy-z+it=d; \end{cases}$$

$$\text{(c)} \quad \begin{cases} x+y+z=a, \\ x+\varepsilon_3 y+\varepsilon_3^2 z=b, \\ x+\varepsilon_3^2 y+\varepsilon_3 z=c. \end{cases}$$

Expressions from Problem 2.11 are called *Lagrange resolvents*. They are 'better' than roots because they are 'more symmetric' in the following sense.

Solution of cubic equation using Lagrange resolvents (solution of Problem 2.8 (c)). To find the roots x, y, z of a cubic equation, it suffices to find the expressions a, b, c from Problem 2.11 (c). Notice that the del Ferro method from [Sk19, 4.2.2] leads us to the same expressions. By Vieta theorem, $a = a(x, y, z)$ is the coefficient of the equation. Under the substitution $x \leftrightarrow y$, polynomial $b = b(x, y, z)$ goes to $\varepsilon_3 c$, and $c = c(x, y, z)$ goes to $\varepsilon_3^2 b$ (check this!). Therefore, the polynomials bc and $b^3 + c^3$ do not change under this substitution. Analogously, they do not change under substitution $z \leftrightarrow y$. Therefore the polynomials bc and $b^3 + c^3$ are *symmetric*, i.e., they do not change under any permutation of variables. From the theorem on representability of a symmetric polynomial as a polynomial in elementary symmetric polynomials (see e.g. [Sk19, 4.6.3c]) and Vieta theorem it follows that the bc and $b^3 + c^3$ polynomials in x, y, z can be represented as polynomials in the coefficients of the equation. Hence we can obtain b^3 and c^3 by

solving certain quadratic equation. Now, by solving certain quadratic equation we can obtain b^3 and c^3.

By Ruffini Theorem 2.7, Lagrange resolvent method demonstrated by solving equations of degrees 3 and 4 (Problems 2.8 (c) and 2.10 (d)) does not work for degree 5. Guess why!

Denote by Σ_q the set of permutations of the set $\{1, 2, \ldots, q\}$. For a permutation $\alpha \in \Sigma_q$ denote

$$\vec{u}_\alpha := (u_{\alpha(1)}, \ldots, u_{\alpha(q)}).$$

Define the *Lagrange resolvent* by

$$t(u_1, \ldots, u_q) := \varepsilon_q u_1 + \varepsilon_q^2 u_2 + \ldots + \varepsilon_q^q u_q.$$

Define *Galois resolvent* by

$$Q(u_1, \ldots, u_q, y) := \prod_{\alpha \in \Sigma_q} (y - t(\vec{u}_\alpha)) \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, y].$$

2.12. (a) We have $Q(\varepsilon_q u_1, \ldots, \varepsilon_q u_q, y) = Q(u_1, \ldots, u_q, y)$.

(b) For some $R_Q \in \mathbb{Q}[\varepsilon_q][u_1, \ldots, u_q, z]$ we have $Q(u_1, \ldots, u_q, y) = R_Q(u_1, \ldots, u_q, y^q)$.

(c) If $x_1, \ldots, x_q \in \mathbb{C}$ are the roots of a polynomial $f \in \mathbb{Q}[x]$ of degree q, then $Q(x_1, \ldots, x_q, y) \in \mathbb{Q}[\varepsilon_q][y]$ and even $Q(x_1, \ldots, x_q, y) \in \mathbb{Q}[y]$.

The polynomial $R_Q(x_1, \ldots, x_q, z) \in \mathbb{Q}[z]$ is called *the resolvent polynomial* for f.

(d)* All the roots of the resolvent polynomial for $f(x) = x^5 + 15x + 11$ (and therefore, all the roots of f) are expressible by radicals.

Theorem 2.13.* (a) For $a, b \in \mathbb{R}$ all the roots of the equation $x^5 + ax + b = 0$ are expressible by radicals if and only if $a = \dfrac{15 \pm 20c}{c^2 + 1}$ and $b = \dfrac{44 \mp 8c}{c^2 + 1}$ for some $c \in \mathbb{Q}$, $c \geqslant 0$.

(b) (**Galois Solvability Criterion**) For each $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$ all the roots of the equation $A(x) := x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0$ are expressible by radicals if and only if a set of degree 1 polynomials over $\mathbb{Q}$ can be obtained from $\{A\}$ using the following operations:

• (factorization) if one of our polynomials equals to $P_1 P_2$ for some non-constant $P_1, P_2 \in \mathbb{Q}[x]$, then replace $P_1 P_2$ by P_1 and P_2;

• (extracting a root) if one of our polynomials equals to $P(x^q)$ for some $P \in \mathbb{Q}[x]$, then replace $P(x^q)$ by $P(x)$;

• (taking Galois resolvent) replace one of our polynomials P by the polynomial $Q(y_1, \dots, y_q, y)$, where $y_1, \dots, y_q$ are all the roots of P. (Analogously to Problem 2.12.c $Q(y_1, \dots, y_q, y) \in \mathbb{Q}[y]$.)

Part (a) is derived from (b) [PSo]. Part 'if' in (b) is easier. This part can be proved using Lagrange resolvent method which is considered in this subsection. Part 'only if' in (b) is more complicated. This can be proved similarly to Galois Theorems 1.3, 1.4.

2.4 There is only one way to solve quadratic equation

Systems of equations studied here and in the following subsection arise when solving equations by radicals ('using one radical'), see Remark 2.6.d.

2.14. (a,b) Solve the system of equations in polynomials $f(x, y)$, $p(u, v)$ and $q(u, v, w)$ with real coefficients:

(a) $\begin{cases} f^2(x, y) = p(x + y, xy) \\ x = q\,(x + y, xy, f(x, y)) \end{cases}$.

(b) $\begin{cases} f^k(x, y) = p(x + y, xy) \\ x = q\,(x + y, xy, f(x, y)) \end{cases}$, where $k > 0$ is an integer.

(c,d*) Solve the analogues of (a,b) where the polynomial f is replaced by a function $f : \mathbb{R}^2 \to \mathbb{R}$ (which is not assumed to be continuous).

The system of equations from 2.14.a is satisfied, for example, by the polynomials

$$f(x, y) = x - y, \quad p(u, v) = u^2 - 4v \quad \text{and} \quad q(u, v, w) = \frac{u + w}{2}.$$

2.15. Assume that $f, g \in \mathbb{R}[x, y]$.

(a) **Lemma.** If $fg = 0$, then $f = 0$ or $g = 0$.

Warnings. There exist functions $F, G : \mathbb{R} \to \mathbb{R}$ such that $FG = 0$, $F \neq 0$ and $G \neq 0$. There exist two different polynomials in two variables which are equal at an infinite set of points. Do not use without proof the fact that if the values of polynomials in two variables are equal in any point, then the polynomials are equal.

(b) If $f^2 = g^2$, then $f = g$ or $f = -g$.
(c) If $f^2 + fg + g^2 = 0$, then $f = 0$ or $g = 0$.
(d) If $f^3 = g^3$, then $f = g$.
(e) If $f^5 = g^5$, then $f = g$.
(f) $f^5 - g^5 = (f - g)(f - \varepsilon_5 g)(f - \varepsilon_5^2 g)(f - \varepsilon_5^3 g)(f - \varepsilon_5^4 g)$.

To prove the assertions 2.14.bd, the following notions and lemma are useful.

A polynomial f in two variables x, y is called *symmetric*, if $f(x, y) = f(y, x)$. A polynomial f is called *antisymmetric*, if $f(x, y) = -f(y, x)$.

2.16. (a) **Lemma.** If $f \in \mathbb{R}[x, y]$ is a polynomial with real coefficients in two variables such that f^2 is symmetric, then f is either symmetric or antisymmetric.

(b) **Lemma.** If $f \in \mathbb{R}[x, y]$ is such that f^{2k+1} is symmetric, then f is symmetric.

(c) If $f \in \mathbb{R}[x, y]$ is antisymmetric, then there exists a symmetric polynomial $a \in \mathbb{R}[x, y]$ such that $f = (x - y)a$.

To prove the assertions above and to solve other problems, Lemma 2.15.a would be useful.

2.17. For which of the statements 2.15 and 2.16 their analogues for polynomials with complex coefficients hold?

Now we give a generalized form of assertion 2.14 for an arbitrary number of steps in the definition of the expressibility by radicals.

2.18. A *rational fraction* is a 'formal ratio of polynomials', i.e. a pair $f/g := (f, g)$ of polynomials with $g \neq 0$. We define $f/g \sim f'/g'$ if and only if $fg' = f'g$. The polynomial f is identified with the pair $(f, 1)$. Denote by $\mathbb{R}(u_1, \ldots, u_n)$ the set of all rational fractions with real coefficients in variables $u_1, \ldots, u_n$.

(a) Define the sum and the product of rational fractions. Are they well-defined? Check this!

(b) Consider the system of Remark 2.6.(d) for $n = 2$, where f_j and p_j are rational functions (not necessarily polynomials). Assume that the system is *minimal*. This means that there is no system with a smaller s, and that f_j^k is not a rational fraction of $x+y, xy, f_1, \ldots, f_{j-1}$ for any $j = 1, \ldots, s$ and $k < k_j$. Then $s = 1$, $k_1 = 2$, and there exists

a rational fraction $a \in \mathbb{R}(u, v)$ such that

$$f_1(x, y) = (x - y)a(x + y, xy).$$

(c)* State and prove the analogue of (a), where rational fractions $f_1, \dots, f_s$ are replaced by functions $\mathbb{R}^2 \to \mathbb{R}$ (while $p_0, \dots, p_s$ are still rational fractions) and equalities for rational fractions are replaced by equalities for functions defined for all $(x, y) \in \mathbb{R}^2$.

2.5 Insolvability 'in real polynomials'

In this subsection we often omit the arguments (x, y, z) of polynomials in formulae.

2.19. There are no polynomials $f(x, y, z)$, $p(u, v, w)$ and $q(u, v, w, \tau)$ with real coefficients such that

$$\begin{cases} f(x, y, z)^k = p\big(\sigma_1(x, y, z), \sigma_2(x, y, z), \sigma_3(x, y, z)\big) \\ x = q\big(\sigma_1(x, y, z), \sigma_2(x, y, z), \sigma_3(x, y, z), f(x, y, z)\big) \end{cases}.$$

(a) for $k = 1$; (b) for $k = 3$; (c) for $k = 2$;
(d) for any integer $k > 0$.

For the proof the following definition and statement are useful. A polynomial $f \in \mathbb{R}[x, y, z]$ is called **cyclic symmetric** if $f(x, y, z) = f(y, z, x)$.

2.20. If $f \in \mathbb{R}[x, y, z]$ and the polynomial
(a) f^3; (b) f^2
is cyclic symmetric, then f is cyclic symmetric.

Remark 2.21 (cf. solution of Problem 2.8.c)**.** There are no polynomials

$$f_1(x, y, z), \quad f_2(x, y, z), \quad p_0(u, v, w), \quad p_1(u, v, w, \tau_1), \quad p_2(u, v, w, \tau_1, \tau_2)$$

with real coefficients such that

$$\begin{cases} f_1^2 = p_0(\sigma_1, \sigma_2, \sigma_3) \\ f_2^3 = p_1(\sigma_1, \sigma_2, \sigma_3, f_1) \\ x = p_2(\sigma_1, \sigma_2, \sigma_3, f_1, f_2) \end{cases}.$$

A generalization of Remark 2.21 to an arbitrary number of steps can be formalized by the definition of *expressibility by real radicals*which is obtained from its complex analogue (§2.3) by replacing complex coefficients by real coefficients.

The formulae at the beginning of §2.2 show that x is expressible by real radicals for $n = 2$. The solution of Problem 2.8.ab shows that both polynomials

$$(x - y)(y - z)(z - x) \quad \text{and} \quad x^9y + y^9z + z^9x$$

are expressible by real radicals for $n = 3$.

Theorem 2.22. The polynomial x is not expressible by real radicals for $n = 3$.

Theorem 2.22 is yet another formalization of the fact that *a root of a cubic equation is not expressible by real radicals via its coefficients,* see Remark 1.1.e. Theorem 2.22 is implied by the following lemma.

Lemma 2.23 (keeping cyclic symmetry)**.** If $q > 0$ is an integer, $f \in \mathbb{R}[x, y, z]$ and the polynomial f^q is cyclic symmetric, then f is cyclic symmetric.

2.24. For which of the statements from this subsection their analogues for polynomials with complex coefficients hold?

Toward algorithms of solving algebraic equations

presented by A. Enne, A. Skopenkov,
A. Glebov, A. Chilikov, B. Vukorepa

3 Problems after the semifinal

3.1 Insolvability 'in polynomials'

The definition of expressibility by radicals for a polynomial is given in §2.2. Formally, the Ruffini Theorem 2.7 follows from Lemma 3.4. The most difficult and interesting task is to invent the statement of this lemma. In order to do that we prove the following simple facts. Explain why the polynomial x is not a polynomial of $x+y$ and xy.

3.1. The polynomial x_1 is not expressible by radicals in such a way that the second operation in the definition of expressibility is applied only for

(a) $k=2$ (*hint:* see Problem 2.24); (b) $k=3$.

3.2. Which of the following assertions are true for every $f \in \mathbb{C}[x_1,\dots,x_5]$?

(a) If f^3 is cyclic symmetric, then f is cyclic symmetric.

(b) If f^5 is cyclic symmetric, then f is cyclic symmetric.

(c) If f^3 is symmetric, then f is symmetric.

(d) If f^2 is symmetric, then f is symmetric.

A cycle of length 3 is a permutation of an n-element set which moves some 3 elements cyclically and does not change positions of any other elements. A polynomial $f \in \mathbb{C}[x_1,\dots,x_n]$ is **even symmetric** if for any cycle α of length 3 the polynomials $f(x_1,x_2,\dots,x_n)$ and $f(x_{\alpha(1)},x_{\alpha(2)},\dots,x_{\alpha(n)})$ are equal.

3.3. (a) Find a cyclic symmetric polynomial that is not even symmetric.

(b) If a permutation does not change the polynomial from your solution of Problem 3.2.d, then it can be represented as a composition of cycles of length 3.

Lemma 3.4 (keeping even symmetry)**.** If $q>0$ is an integer, $f \in \mathbb{C}[x_1,\dots,x_5]$, and the polynomial f^q is even symmetric, then f is even symmetric.

3.5. Suppose $f \in \mathbb{C}[x_1, \dots, x_n]$ is a polynomial.

(a) If the polynomial f^7 is even symmetric, then f is even symmetric.

(b) If $n \geqslant 5$ and the polynomial f^3 is even symmetric, then f is even symmetric.

(c) If $n \geqslant 5$, then any cycle of length 3 on an n-element set can be written as a product of permutations of the form $(ab)(cd)$, where a, b, c, d are pairwise distinct (i.e. as a product of compositions of transpositions with disjoint supports).

3.6. The definition of *rational* expressibility by real (complex) radicals is analogous to the definition of expressibility by radicals. Polynomials are replaced by rational fractions (with appropriate coefficients; see the definition in Problem 2.18). Is the polynomial x_1 rationally expressible by

(a) real radicals for $n = 3$?

(b) (complex) radicals for $n = 5$?

3.2 Representability using only one cubic root

Here we develop the ideas from § 2.1.

3.7. Can the following number be represented as $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ with $a, b, c \in \mathbb{Q}$:

(a) $\sqrt{3}$; (b) $\frac{1}{1+5\sqrt[3]{2}+\sqrt[3]{4}}$; (c) $\cos(2\pi/9)$; (d) $\sqrt[5]{3}$; (e) $\sqrt[3]{3}$;

(f) the maximal real root of $x^3 - 4x + 2 = 0$;

(g)* the unique real root of $x^3 - 6x - 6 = 0$;

(h)* the unique real root of $x^3 - 9x - 12 = 0$?

Lemma 3.8. Assume that $r \in \mathbb{R} - \mathbb{Q}$ and $r^3 \in \mathbb{Q}$.

(a) **Irreducibility.** The polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$.

(b) **Linear independence.** If $a + br + cr^2 = 0$ with $a, b, c \in \mathbb{Q}$, then $a = b = c = 0$.

(b′) **Linear independence over $\mathbb{Q}[\varepsilon_3]$.** If

$$k, \ell, m \in \mathbb{Q}[\varepsilon_3] := \{u + v\varepsilon_3 \colon u, v \in \mathbb{Q}\}$$

and $k + \ell r + mr^2 = 0$, then $k = \ell = m = 0$.

(c) If r is a root of a polynomial, then this polynomial is divisible by $x^3 - r^3$.

(d) **Conjugation.** If r is a root of a polynomial, then the numbers $\varepsilon_3 r$ and $\varepsilon_3^2 r$ are also its roots.

(e) **Conjugation.** If $a, b, c \in \mathbb{Q}$ and a polynomial has root $x_0 := a + br + cr^2$, then the numbers

$$x_1 := a + b\varepsilon_3 r + c\varepsilon_3^2 r^2 \quad \text{and} \quad x_2 := a + b\varepsilon_3^2 r + c\varepsilon_3 r^2$$

are also its roots.

(f) **Rationality.** If $a, b, c \in \mathbb{Q}$, then the number $a + br + cr^2$ is a root of some cubic polynomial.

Theorem 3.9. If a polynomial is irreducible over $\mathbb{Q}$ and has a root $a+br+cr^2$ for some $r \in \mathbb{R}-\mathbb{Q}$ and $a, b, c, r^3 \in \mathbb{Q}$, then this polynomial is cubic and it has exactly one real root.

Lemma 3.10 (Extension)**.** A number expressible by real radicals with only one extraction of a cubic root can be represented as $a+br+cr^2$, where $r \in \mathbb{R}$ and $a, b, c, r^3 \in \mathbb{Q}$.

3.3 Representability using only one root of prime order

3.11. Can the following number be represented in the form

$$a_0 + a_1\sqrt[7]{2} + a_2\sqrt[7]{2^2} + \cdots + a_6\sqrt[7]{2^6}$$

with $a_0, a_1, a_2, \ldots, a_6 \in \mathbb{Q}$:

(a) $\sqrt{3}$; (b) $\cos\frac{2\pi}{21}$; (c) $\sqrt[11]{3}$; (d) $\sqrt[7]{3}$;

(e) some root of the polynomial $x^7 - 4x + 2$?

Answers: no. The arguments are similar to those in the solutions of problems 3.7. Use lemmas stated below.

Lemma 3.12. Let q be a prime number, $r \in \mathbb{R} - \mathbb{Q}$ and $r^q \in \mathbb{Q}$.

(a) **Irreducibility.** The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}$.

(b) **Linear independence.** If r is a root of a polynomial A which degree is less than q, then $A = 0$.

(c) **Conjugation.** If r is a root of a polynomial, then all the numbers $r\varepsilon_q^k$, $k = 1, 2, 3, \ldots, q-1$, are also roots of this polynomial.

(d) **Rationality.** If A is a polynomial, then the number $A(r)$ is a root of some nonzero polynomial which degree is at most q.

Denote

$$\mathbb{Q}[\varepsilon_q] := \{a_0 + a_1\varepsilon_q + a_2\varepsilon_q^2 + \ldots + a_{q-2}\varepsilon_q^{q-2} \ : \ a_0, \ldots, a_{q-2} \in \mathbb{Q}\}.$$

3.13. Let q be a prime number, $r \in \mathbb{C} - \mathbb{Q}[\varepsilon_q]$ and $r^q \in \mathbb{Q}[\varepsilon_q]$.

(a) The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b), (c) Prove the analogues of parts (b,c) of the previous problem for a polynomial with coefficients in $\mathbb{Q}[\varepsilon_q]$.

Lemma 3.14.* Let q be a prime number, $r \in \mathbb{R} - \mathbb{Q}$ and $r^q \in \mathbb{Q}$.

(a) **Irreducibility over $\mathbb{Q}[\varepsilon_q]$.** The polynomial $x^q - r^q$ is irreducible over $\mathbb{Q}[\varepsilon_q]$.

(b) **Linear independence over $\mathbb{Q}[\varepsilon_q]$.** If A is a polynomial of degree less than q with coefficients in $\mathbb{Q}[\varepsilon_q]$ and $A(r) = 0$, then $A = 0$.

Theorem 3.15. Assume that a polynomial is irreducible over $\mathbb{Q}$ and has an irrational root $A(r)$, where A is a polynomial and $r \in \mathbb{R}$ is such that $r^q \in \mathbb{Q}$ for some prime q. Then the polynomial has degree q and, if $q \neq 2$, has no other real roots.

The proof is analogous to the proofs of Theorems 2.3, 3.9 and to the solutions of 3.11 (abc). Apply the Conjugation Lemma 3.12.c, the Rationality Lemma 3.12.d, and the Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b.

Lemma 3.16 (Extension)**.** The number expressible by real radicals with only one root extraction is equal to $A(r)$ for some $r \in \mathbb{R}$, $q \in \mathbb{Z}$ and $A \in \mathbb{Q}[x]$, with $r^q \in \mathbb{Q}$.

The proof is similar to the proof of the Extension Lemma 3.10.

3.17. (a–d) Prove the assertions analogous to Problem 3.12 with $\mathbb{Q}$ replaced by any set $F \subset \mathbb{R}$ which is closed under operations of addition, subtraction, multiplication and division by a non-zero number (and with polynomials over $\mathbb{Q}$ replaced by polynomials over F).

Solutions for problems before the semifinal

2.1. *Answers:* (a), (b), (c), (d) "— yes, (e), (f), (g), (h), (i) "— no.

(a), (c) We have $\sqrt{3+2\sqrt{2}} = \sqrt[3]{7+5\sqrt{2}} = 1+\sqrt{2}$.

(b) We have $\dfrac{1}{7+5\sqrt{2}} = \dfrac{7-5\sqrt{2}}{7^2-2\cdot 5^2} = -7+5\sqrt{2}$.

(d) We have $\cos(2\pi/5) = (\sqrt{5}-1)/4$.

(e) Assume that $\sqrt[3]{2}$ is representable in this form. Then

$$2 = (\sqrt[3]{2})^3 = (a^3+3ab)+(3a^2+b)\sqrt{b}.$$

Since $3a^2+b \neq 0$, we have $\sqrt{b} \in \mathbb{Q}$. Thus $\sqrt[3]{2} \in \mathbb{Q}$, which is a contradiction.

Other proofs are similar to the proof of Theorem 2.3.

(f) *A sketch for the first solution.* It is easier to prove right away that

$$\sqrt[3]{2} \neq a+p\sqrt{b}+q\sqrt{c}+r\sqrt{bc}, \quad \text{for any} \quad a,b,c,p,q,r \in \mathbb{Q}.$$

It sufficies to show that $\sqrt[3]{2} \neq u+v\sqrt{c}$ for any $u,v,c \in \mathbb{Q}[\sqrt{b}] := \{x+y\sqrt{b}\colon x,y \in \mathbb{Q}\}$. The idea of our proof is that numbers from $\mathbb{Q}[\sqrt{b}]$ (with b fixed) are ¡¡as good as¿¿ rational numbers, that is the sum, the difference, the product and the quotient of the numbers from $\mathbb{Q}[\sqrt{b}]$ are also the numbers from $\mathbb{Q}[\sqrt{b}]$ (or, scientifically speaking, $\mathbb{Q}[\sqrt{b}]$ — is a *number field*). Therefore we can prove the assertion simillary to (e).

A sketch for the second solution. Assume that $\sqrt{2}+\sqrt[3]{2} = a+\sqrt{b}$ for some $a,b \in \mathbb{Q}$. This number is a root of the polynomial $P(x) = ((x-\sqrt{2})^3-2)((x+\sqrt{2})^3-2)$ having rational coefficients. From (e) it follows that $\sqrt{2}+\sqrt[3]{2} \notin \mathbb{Q}$. Hence, $\sqrt{b} \notin \mathbb{Q}$. By the Conjugation Lemma 2.2 (e) for $r = \sqrt{b}$ we have $P(a-\sqrt{b}) = 0$. Since $\sqrt{b} \notin \mathbb{Q}$, then roots $a \pm \sqrt{b}$ are different. The polynomial P has only two real roots, namely $\sqrt{2}+\sqrt[3]{2}$ and $-\sqrt{2}+\sqrt[3]{2}$. Thus $a+\sqrt{b} = \sqrt{2}+\sqrt[3]{2}$ and $a-\sqrt{b} = -\sqrt{2}+\sqrt[3]{2}$. Therefore $\sqrt[3]{2} = a \in \mathbb{Q}$. This is a contradiction.

(g) Assume that $\cos(2\pi/9)$ is representable in this form. By the formula for the cosine of a triple angle $\cos(2\pi/9)$ is a root of the equation $4x^3-3x = -\frac{1}{2}$. By Lemma 2.2 (f) this equation has a rational root, which is a contradiction.

Another proof is analogous to Theorem 2.3.

(h) The roots of the polynomial $P(x) = (x^2-2)^2 - 2$ are four numbers of the form $\pm\sqrt{2 \pm \sqrt{2}}$, where the signs need not agree. All these numbers are irrational. From Theorem 2.3 it follows that it is sufficient to prove that the polynomial P cannot be written as a product of two quadratic trinomials with rational coefficients. This irreducibility follows from the fact that the product of any two roots of P is irrational.

(i) (Here we use the text by I. Braude-Zolotarev.) The equality

$$\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) + \ldots + \cos(14\pi/7) = 0$$

implies that $\cos(2\pi/7) + \cos(4\pi/7) + \cos(6\pi/7) = -1/2$. Applying the formulas $\cos 2\alpha = 2\cos^2\alpha - 1$ and $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, we find that $\cos(2\pi/7)$ is a root of the equation $8t^3 + 4t^2 - 4t - 1 = 0$.

Substituting $u = 2t$ we get $u^3 + u^2 - 2u - 1 = 0$. This equation has no rational roots. Hence the same holds for $8t^3 + 4t^2 - 4t - 1 = 0$. Thus the polynomial $8t^3 + 4t^2 - 4t - 1 = 0$ is irreducible over $\mathbb{Q}$. Now the negative answer to the question follows from Lemma 2.2.f.

(j) is similar to (f).

2.3. Suppose on the contrary that the given polynomial $P(x)$ has a root $x_0 = a \pm \sqrt{b}$. By the Conjugation Lemma 2.2.e and analogously to it, the number $x_1 = a \mp \sqrt{b}$ is also a root of P. If $b = 0$, then the statement is obvious. So assume that $b \neq 0$. Then $x_0 \neq x_1$. Therefore, P is divisible by $(x-a)^2 - b$. Since $\deg P > 2$ then P is reducible. This is a contradiction.

2.4. Let $\sqrt{c}$ be a number we get with only one extraction of the root, where $c \in \mathbb{Q}$. Prove that all the obtained numbers have the form $a + b\sqrt{c}$ with $a, b \in \mathbb{Q}$.

2.5. Answer: The number is representable if and only if $n \in \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Or, equivalently, $\varphi(n) \in \{1, 2, 4\}$.

2.8. (a) The polynomial $(x-y)^2(y-z)^2(z-x)^2$ is symmetric.

(One may also reduce (a) to (b).)

(b) Set

$$M = x^9y + y^9z + z^9x \quad \text{and} \quad N = y^9x + x^9z + z^9y.$$

Then $M+N$ and MN are symmetric polynomials. Therefore they are polynomials in elementary symmetric polynomials $\sigma_1, \sigma_2, \sigma_3$. Finally, M itself now can be expressed via $M+N$ and MN by the 'formula for the roots of a quadratic equation', see beginning of §2.3.

2.9. (a) One possible answer is $u + v\varepsilon_3 + w\varepsilon_3^2$.

(b) Set

$$M = x_1x_3 + x_3x_5 + x_5x_7 + x_7x_9 + x_9x_1 \quad \text{and}$$

$$N = x_2x_4 + x_4x_6 + x_6x_8 + x_8x_{10} + x_{10}x_2.$$

Now one can argue as in 2.8.b.

2.10. (a) The square $(x-y)^2(x-z)^2(x-t)^2(y-z)^2(y-t)^2(z-t)^2$ is symmetric, cf. 2.8.a.

(b) Set

$$M = xy + zt, \quad N = xz + yt, \quad K = xt + yz.$$

By 2.8.c, M can be expressed by radicals using the polynomials

$$M + N + K, \quad MN + MK + NK, \quad MNK.$$

Analogously to the solutions of Problems 2.8 c above and 2.10 (d) below, these polynomials are symmetric. Thus $M = xy + zt$ is expressible by radicals.

(c) Set

$$M = (x+y-z-t)^2, \quad N = (x+z-y-t)^2, \quad K = (x+t-y-z)^2.$$

Then repeat the solution of part (b) to obtain $M = (x+y-z-t)^2$. Then it is easy to obtain $x+y-z-t$.

Alternative solution. We have

$$(x+y-z-t)^2 = (x^2+y^2+z^2+t^2)+2(xy+tz)-2(xt+yz)-2(xz+yt).$$

The first summand is symmetric and the other summands are expressible by radicals due to part (b). Thus $x+y-z-t$ is expressible by radicals.

Solution of the equation of fourth degree using Lagrange resolvent method (solution of the problem 2.10 (d)). To find the roots x, y, z, t of the fourth degree equation it is enough to find the expressions for a, b, c, d from Problem 2.11 (a). By Vieta theorem, a is the coefficient of the equation. Under substitution $x \leftrightarrow y$, polynomials c^2 and d^2 are interchanged, and b^2 goes to itself. After cyclic permutation $x \to y \to z \to t \to x$, polynomials b^2 and d^2 are interchanged, and c^2 goes to itself. Therefore polynomials b^2, c^2, d^2 are permuted for every permutation of variables x, y, z, t. Hence their Vieta polynomials, i.e.

$$b^2+c^2+d^2, \quad b^2c^2+b^2d^2+c^2d^2, \quad b^2c^2d^2,$$

are symmetric. Then these polynomials in x, y, z can be represented as polynomials in the coefficients of the equation. Now by solving the cubic equation we can get b^2, c^2, d^2. Then it is easy to obtain b, c, d.

2.11. Repeatedly use the identities $1+\varepsilon+\varepsilon^2=0$ and $1+i+i^2+i^3=0$.

2.12. Here we show the solution for $q=5$.

(a) We have

$$t(\varepsilon_5\vec{u}_\alpha) = t(u_{\alpha(5)}, u_{\alpha(1)}, u_{\alpha(2)}, u_{\alpha(3)}, u_{\alpha(4)}) = t(\vec{u}_{\alpha\circ(54321)}).$$

Hence

$$Q(\varepsilon_5 u_1, \dots, \varepsilon_5 u_5, y) = \prod_{\alpha\in\Sigma_5} (y - t(\varepsilon_5\vec{u}_\alpha)) =$$

$$= \prod_{\alpha\in\Sigma_5} (y - t(\vec{u}_{\alpha\circ(54321)}) = Q(u_1, \dots, u_5, y).$$

Here

• $(54321) \in \Sigma_5$ is the cycle that sends 5 to 4, 4 to 3, ..., 1 to 5.

• the last equality holds because when α ranges through Σ_5, so does $\alpha \circ (54321)$.

(b) There is a homogeneous polynomial $P_k \in \mathbb{Q}[\varepsilon_5][u_1, \dots, u_5]$ (of 'degree' $120-k$) such that the coefficient of y^k in Q is $P(u_1, \dots, u_5)$,

i.e.

$$Q(u_1, \dots, u_5, y) = \sum_{k=0}^{120} P_k(u_1, \dots, u_5) y^k.$$

By (a) and by homogeneity we have

$$P_k(u_1, \dots, u_5) = P_k(\varepsilon_5 u_1, \dots \varepsilon_5 u_5) = \varepsilon_5^{-k} P_k(u_1, \dots, u_5).$$

If k is not divisible by 5, we obtain $P_k(u_1, \dots, u_5) = 0$ as required.

(c) The polynomial $Q(u_1, \dots, u_5, y)$ is symmetric in $u_1, \dots, u_5$. So all the coefficients (P_k from (b)) of the corresponding polynomial from $\mathbb{Q}[\varepsilon_5, u_1, \dots, u_5][y]$ are symmetric in $u_1, \dots, u_5$. Now the statement follows from the fundamental theorem on symmetric polynomials, Vieta theorem and the fact that the coefficients of f are rational.

2.14. (a) We will prove that there exists $\alpha \in \mathbb{R}$ such that $f(x, y) = \alpha(x - y)$.

Since the polynomial $f^2 = p$ is symmetric, we can assume that the polynomial q is linear in third variable, i.e. $q(u, v, w) = a(u, v) + b(u, v)w$ for some $a, b \in \mathbb{R}[u, v]$ (otherwise we can change q while preserving f, p). Then we have $x = a(x + y, xy) + b(x + y, xy) f(x, y)$.

Now we get $pb^2 = f^2 b^2 = (x - a)^2 = (y - a)^2$. By Lemma 2.15.b we get $x - a = a - y$, since the case $x - a = y - a$ is impossible. Hence $a = (x + y)/2$. Then $(x - y)^2 = 4f^2 b^2 = 4pb^2$. If the polynomial $p = f^2$ is constant, the polynomial $b = \pm(x - y)/2\sqrt{p}$ is not symmetric. Therefore p is not constant. Thus b is constant. Hence $2x = 2q = x + y + 2bf$, from which $b \neq 0$ and $f = \alpha(x - y)$ for $\alpha = 1/2b$.

(b) We will prove that k is even and that there exists $\alpha \in \mathbb{R}$ such that $f(x, y) = \alpha(x - y)$. We can use induction on k with the application of part (a) and the generalization of Lemmas 2.15.be, 2.16. If k is odd, from Lemma 2.16.b we get that f is symmetric. That contradicts the equality $x = q(x + y, xy, f(x, y))$. If $k = 4$, then f^2 is either symmetric or antisymmetric. The first case reduces to part (a). The second one gives us $f^2(x, y) + f^2(y, x) = 0$. We solve the case of arbitrary even k analogously.

(c) Analogously to part (a) we get $x = a + bf$. Therefore, f is a rational fraction. Now the solution is analogous to part (a).

2.15. (a) Define the *leading term* of a polynomial so that the leading term of the product is equal to the product of the leading terms of the factors.

(b) This follows from part (a).

(c) We have $f^2 + fg + g^2 = \left(f + \frac{g}{2}\right)^2 + \frac{3}{4}g^2 = (f - \varepsilon_3 g)(f - \varepsilon_3^2 g)$.

(d) This follows from part (c).

(e) This follows from part (f).

(f) Prove and apply the Bezout theorem for polynomials in u with coefficients in $\mathbb{R}[v]$.

2.16. (a) Since f^2 is symmetric, we have $f(x,y)^2 = f(y,x)^2$. Now by the statement 2.15.b we have $f(x,y) = \pm f(y,x)$.

(b) Use the analogues of statements 2.15.ce.

(c) See the hint for 2.15.f.

2.17. *Answer:* 2.15.abf, 2.16.abc.

2.22. For $n = 3$, the set of polynomials expressible by real radicals is contained in the set of cyclic symmetric polynomials. This statement can be proved by induction on the number of operations from the definition of expressibility in radicals. The induction step follows from Lemma 2.23 on the preservation of cyclic symmetry.

Since the polynomial x is not cyclic symmetric, it is also not expressible in real radicals.

2.23. The proof can be found in [Sk19, p. 9.4.2].

2.24. *Answer:* 2.19.abcd, 2.20.b, 2.23 for all q which are not divisible by 3.

Toward algorithms of solving algebraic equations

presented by A. Enne, A. Skopenkov,
A. Glebov, A. Chilikov, B. Vukorepa

Solutions for problems after the semifinal

3.1. (b) Use the analog of Problem 3.2.c for $n = 3$.

3.2. *Answer:* (c) — true, (a), (b), (d) — not true.

(a) See 2.9.a.

(b) Consider the polynomial $x_1 + \varepsilon_5 x_2 + \varepsilon_5^2 x_3 + \varepsilon_5^3 x_4 + \varepsilon_5^4 x_5$.

(d) Consider the polynomial $\prod\limits_{i<j}(x_i - x_j)$.

(c) Since f^3 is symmetric, we have

$$f^3(x_1, x_2, x_3, x_4, x_5) = f^3(x_2, x_1, x_3, x_4, x_5).$$

Extracting the third root, we have

$$f(x_1, x_2, x_3, x_4, x_5) = \varepsilon_3^q f(x_2, x_1, x_3, x_4, x_5) = \varepsilon_3^{2q} f(x_1, x_2, x_3, x_4, x_5).$$

Thus, $\varepsilon_3^{2q} = 1$, and so $\varepsilon_3^q = 1$. Similarly, $f(\vec{x}) = f(\vec{x}_\alpha)$ for any permutation α exchanging two elements from the set $\{x_1, x_2, x_3, x_4, x_5\}$. Therefore, f is symmetric.

3.3. (a) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_5 + x_5x_1$.

(b) First prove that if a permutation maps the polynomial of Problem 3.2.d to itself, then the permutation is even. This implies that the permutation can be represented as a composition of cycles of length 3, see [ZSS, p. 23.2.4].

3.4. The proof can be found in [Sk15].

3.5. (c) $(abc) = (ac)(de)(ab)(de)$.

3.6. *Answer:* (a), (b) — no.

Lemmas 2.23 on keeping cyclic symmetry and 3.4 on keeping even symmetry also hold for rational fractions, see [Sk15], [Sk19, p. 9.4.2]. After that, we can proceed analogously to the solution of Problem 2.22.

3.7. *Answers*: (a), (c), (d), (e), (f), (h) "— no, (b), (g) "— yes.

Denote $r := \sqrt[3]{2}$.

(a) Assume that $\sqrt{3}$ is representable in this form.

First solution. Then

$$3 = (a^2 + 4bc) + (2ab + 2c^2)\sqrt[3]{2} + (2ac + b^2)\sqrt[3]{4}.$$

Since the polynomial $x^3 - 2$ has no rational roots, it is irreducible over $\mathbb{Q}$. Thus, $2ab + 2c^2 = 2ac + b^2 = 0$ (cf. 3.8.b). So we have $b^3 = -2abc = 2c^3$. Hence either $b = c = 0$ or $\sqrt[3]{2} = b/c$. Both cases are impossible.

Second solution. Denote $P(x) := x^2 - 3$. By the Conjugation Lemma 3.8 (e), P has three roots x_0, x_1, x_2 defined in the statement of the lemma. Since none of them is rational, the equality $b = c = 0$ does not hold. So by the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′) the three roots are distinct. This is a contradiction.

(b) We have $(1 + 5\sqrt[3]{2} + \sqrt[3]{4})(3 + \sqrt[3]{2} - 8\sqrt[3]{4}) = -75$. (This equality can be easily obtained by the undetermined coefficients method or applying Euclid algorithm to $x^3 - 2$ and $x^2 + 5x + 1$, see solution of 3.10.) Therefore,

$$\frac{1}{1 + 5\sqrt[3]{2} + \sqrt[3]{4}} = -\frac{1}{25} - \frac{1}{75} \cdot \sqrt[3]{2} + \frac{8}{75} \cdot (\sqrt[3]{2})^2.$$

(c) Assume that $\cos(2\pi/9)$ is representable in this form. This number is a root of the equation $4x^3 - 3x = -\frac{1}{2}$. Its other two real roots are $\cos(8\pi/9)$ and $\cos(4\pi/9)$.

Repeat the second solution of (a) for $P(x) := 8x^3 - 6x - 1$. We obtain that the roots x_0, x_1, x_2 are distinct. Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_1$. Thus, x_1 and x_2 can not be both real and distinct. This is a contradiction.

(d) Assume that $\sqrt[5]{3}$ is representable in this form. By the Rationality Lemma 3.8 (f), $\sqrt[5]{3}$ is a root of a cubic polynomial. This contradicts to the irreducibility of the polynomial $x^5 - 3$ over $\mathbb{Q}$.

(e) Analogously to (a) and (c), by the Conjugation Lemma 3.8 (e) it follows that the polynomial $x^3 - 3$ has three roots x_0, x_1, x_2 defined in the statement of the lemma. Thus, $(a + br + cr^2)\varepsilon_3^s = a + br\varepsilon_3 + cr^2\varepsilon_3^2$ for some $s \in \{1, 2\}$. By the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$

3.8 (b′) we have $a = 0$ and $bc = 0$. Hence either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$. This is a contradiction.

(f) The proof is analogous to (c).

(g) This equation has a root $\sqrt[3]{2} + \sqrt[3]{4}$.

(h) The only real root of this equation is $\sqrt[3]{3} + \sqrt[3]{9}$. Assume that this number is representable in the required form. Repeat the second solution of (a) for $P(x) := x^3 - 9x - 12$. We obtain that x_0, x_1, x_2 are all roots of P.

On the other hand, all roots of the equation are

$$y_0 := \sqrt[3]{3} + \sqrt[3]{9}, \quad y_1 := \sqrt[3]{3}\varepsilon_3 + \sqrt[3]{9}\varepsilon_3^2, \quad y_2 := \sqrt[3]{3}\varepsilon_3^2 + \sqrt[3]{9}\varepsilon_3.$$

Since the equation has exactly one real root, we have $x_0 = y_0$. Then either $x_1 = y_1$, $x_2 = y_2$, or $x_2 = y_1$, $x_1 = y_2$.

Denote $R(x) := \sqrt[3]{3}x + \sqrt[3]{9}x^2$ and let $S(x) := a + brx + cr^2x^2$ or $S(x) := a + brx^2 + cr^2x$ in the first and second case, respectively. Then the polynomial $R(x) - S(x)$ has three distinct roots 1, ε_3, and ε_3^2. But the degree of this polynomial is at most 2. Thus, $R = S$. Hence either $\sqrt[3]{3} = br$ or $\sqrt[3]{3} = cr^2$. A contradiction.

3.8. (a) Suppose that $x^3 - r^3$ is reducible over $\mathbb{Q}$. Then it has a rational root. This is a contradiction.

(b) Assume the contrary. Divide $x^3 - r^3$ by $a + bx + cx^2$ with a remainder. By (a), the remainder is nonzero. Both polynomials $x^3 - r^3$ and $a + bx + cx^2$ have a root $x = r$. Hence the remainder has the root $x = r$. Thus, the remainder has an irrational root. This is impossible because the remainder has degree 1.

(b′) Consider the real and the imaginary parts separately.

(c) Divide our polynomial by $x^3 - r^3$ with a remainder. Taking $x = r$ and applying Linear Independence Lemma (b), we get that the remainder is zero.

(d) By (c), if $R^3 = r^3$, then R is a root of our polynomial.

(e) Let P be the given polynomial, and set $G(t) := P(a + bt + ct^2)$. Then $G(r) = 0$. Hence by (d) we have $G(r\varepsilon_3) = 0 = G(r\varepsilon_3^2)$.

(f) *First solution.* Taking $x = y + a$ we see that it suffices to prove the assertion for $a = 0$. The number $t = br + cr^2$ satisfies $t^3 = b^3r^3 + c^3r^6 + 3bcr^3t$.

In other words, since $u^3+v^3+w^3-3uvw$ is divisible by $u+v+w$, the number $a+br+cr^2$ is a root of the polynomial

$$(x-a)^3-3bcr^3(x-a)-b^3r^3-c^3r^6.$$

Second solution. Denote $x_0 := a+br+cr^2$. Expand the numbers x_0^k, $k=0,1,2,3$, as polynomials in r:

$$x_0^k = a_k + b_k r + c_k r^2.$$

It suffices to find numbers $\lambda_0,\lambda_1,\lambda_2,\lambda_3 \in \mathbb{Q}$, not all zeros, such that $\lambda_0+\lambda_1 x_0+\lambda_2 x_0^2+\lambda_3 x_0^3=0$. So, these numbers must satisfy the system of equations

$$\begin{cases} \lambda_0 a_0 + \ldots + \lambda_3 a_3 = 0, \\ \lambda_0 b_0 + \ldots + \lambda_3 b_3 = 0, \\ \lambda_0 c_0 + \ldots + \lambda_3 c_3 = 0. \end{cases}$$

It is known that a homogeneous (i.e. with zero right-hand parts) system of linear equations with rational coefficients, where the number of equations is smaller than the number of variables, has a nontrivial rational solution. Hence, the required numbers exist.

The obtained polynomial has degree exactly 3 by lemmas 3.8 (e, b′).

Third solution. Denote $A(x) := a+bx+cx^2$. The product $(x-A(t_0))(x-A(t_1))(x-A(t_2))$ is a symmetric polynomial in t_0,t_1,t_2. Hence this product is a polynomial in x and the elementary symmetric polynomials in t_0,t_1,t_2. The values of these elementary symmetric polynomials at $t_k = r\varepsilon_3^k$ $(k=0,1,2)$ are the coefficients of the polynomial x^3-r^3, and hence are rational. So the considered product is the required polynomial.

3.9. By the Rationality Lemma 3.8 (f) there exists a cubic polynomial having $a+br+cr^2$ as a root. Since the given polynomial P is irreducible over $\mathbb{Q}$ and has the same root, we conclude that $\deg P \leqslant 3$. By the Conjugation Lemma 3.8 (e), P has three roots x_0,x_1,x_2 defined in the statement of the lemma. Since P is irreducible over $\mathbb{Q}$, none of its roots is rational. So the equality $b=c=0$ is impossible. By the

Linear Independence Lemma over $\mathbb{Q}[\varepsilon_3]$ 3.8 (b′), x_0, x_1, x_2 are distinct. Hence $\deg P = 3$.

Since $\overline{\varepsilon_3^k} = \varepsilon_3^{-k}$, we have $\overline{x_2} = x_1$. Hence x_2 and x_1 cannot be real and distinct. So $x_2, x_1 \in \mathbb{C} - \mathbb{R}$. Then P has a unique real root.

3.10. Assume that after extracting the third root we get number r. If $|r| \in \mathbb{Q}$, the statement is trivial. If $|r| \notin \mathbb{Q}$, then the polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$.

It suffices to prove that $\frac{1}{a+br+cr^2} = h(r)$ for some polynomial h. By the Irreducibility Lemma, the polynomial $x^3 - r^3$ is irreducible over $\mathbb{Q}$. Hence it is coprime with $a + bx + cx^2$. Therefore, there exist polynomials g and h such that $h(x)(a + bx + cx^2) + g(x)(x^3 - r^3) = 1$. Then h is the required polynomial.

3.11. Denote $r := \sqrt[7]{2}$ and $A(x) := a_0 + a_1x + a_2x^2 + \ldots + a_6x^6$.

(a) Assume that $\sqrt{3}$ is representable in this form. By the Conjugation Lemma 3.12 (c), the polynomial $x^2 - 3$ has roots $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Since this polynomial has no rational roots, the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) yields that these roots are distinct. This is a contradiction.

(b) Assume that $\cos\frac{2\pi}{21}$ is representable in this form.

First solution. Analogously to part (a), the given polynomial P has pairwise distinct roots $x_k := A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k different from x_0. We have $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$. Hence $x_k = \overline{x_k} = x_{7-k}$. A contradiction.

Second solution. Denote by P the polynomial such that $\cos 7x = P(\cos x)$ (prove that it exists!). The roots of the polynomial $2P(x) + 1$ are real numbers $y_k = \cos\dfrac{2(3k+1)\pi}{21}$ with $k = 0, \ldots, 6$. One of them, namely $y_2 = -1/2$, is rational.

In the following paragraph we prove that y_0 is irrational.

(Otherwise, the equality $\varepsilon_{21}^2 - 2y_0\varepsilon_{21} + 1 = 0$ implies that $\varepsilon_{21} = a + i\sqrt{b}$ for some $a, b \in \mathbb{Q}$. Then the number $\varepsilon_7 = \varepsilon_{21}^3$ also has this form. But ε_7 is a root of the irreducible[4] polynomial $1 + x + \cdots + x^6$,

[4]The irreducibility of the polynomial $g(x) = 1 + x + \ldots + x^6$ can be proved, e.g.,

which contradicts to the analogue of Theorem 2.3 for numbers of the form $a + i\sqrt{b}$.)

Thus the number y_0 is an irrational root of the polynomial $\frac{2P(x)+1}{2x+1}$ which has degree 6. Then Conjugation Lemma 3.12.c and Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b show that this polynomial has seven distinct roots, which is impossible.

(c) Assume that $\sqrt[11]{3}$ is representable in this form. Then by the Rationality Lemma 3.12 (d), there exists a nonzero polynomial of degree at most 7 having $\sqrt[11]{3}$ as a root. This contradicts the irreducibility of the polynomial $x^{11} - 3$ over $\mathbb{Q}$.

(d) Assume that $\sqrt[7]{3}$ is representable in this form. Analogously to (a), all the complex roots of the polynomial $x^7 - 3$ are $A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Therefore, $A(r)\varepsilon_7^s = A(r\varepsilon_7)$ for some $s \in \{1, 2, 3, 4, 5, 6\}$. Hence by the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b) we have $a_k = 0$ for each $k \neq s$. Therefore, $\sqrt[7]{3} = a_s r^s$. This is a contradiction.

(e) Assume that one of the roots is representable in this form. The given polynomial P has no rational roots. Then Conjugation Lemma 3.12.c and Linear Independence over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.14.b yield that P has pairwise distinct roots $x_k := A(r\varepsilon_7^k)$ for $k = 0, 1, 2, \ldots, 6$. Since $P(0) > 0$, $P(1) < 0$, and $P(2) > 0$, the polynomial P has a real root x_k distinct from x_0. From the equality $\overline{\varepsilon_7^k} = \varepsilon_7^{-k}$ it follows that $x_k = \overline{x_k} = x_{7-k}$. This is a contradiction.

3.12. (a) All the roots of the polynomial $x^q - r^q$ are $r, r\varepsilon_q, r\varepsilon_q^2, \ldots, r\varepsilon_q^{q-1}$. Assume that $x^q - r^q$ is reducible over $\mathbb{Q}$. Then the absolute value of the constant term of one of its unitary irreducible factors is rational and equals to the product of absolute values of k of these roots, $0 < k < q$. Therefore, $r^k \in \mathbb{Q}$. Since q is prime, we have $kx + qy = 1$ for some integers x, y. Thus, $r = (r^k)^x (r^q)^y \in \mathbb{Q}$. This is a contradiction.

(b) Assume the contrary. Take the smallest degree polynomial $A(x)$ for which the statement is false. Let $R(x)$ be the remainder of $x^q - r^q$ divided by $A(x)$. Then $\deg R < \deg A$, $R(r) = 0$, and $R(x) \neq 0$ by (a). This contradicts the choice of A.

---

by applying the Eisenstein criterion to the polynomial $g(x + 1)$. However, in this particular case it suffices to prove that g has no divisors of degree 1 and 2 with rational coefficients.

(c) The solution is analogous to that of 2.2 (c, d), 3.8 (d). Use (b).

(d) The proofs repeat the second and the third proofs of the Rationality Lemma 3.8 (f). It is only necessary to replace 3 by q and 2 by $q-1$ throughout the proofs (for example, in the second line of the second proof put $k = 0, 1, 2, \dots, q$).

3.13. (a) Assume that our polynomial is reducible. The constant term of any its unitary factor lies in $\mathbb{Q}[\varepsilon_q]$ and equals to $\pm r^k \varepsilon_q^m$ for some m. Then $r^k \in \mathbb{Q}[\varepsilon_q]$. Now as in the proof of Lemma 3.12.a we obtain that $r \in \mathbb{Q}[\varepsilon_q]$. This is a contradiction.

Parts (b,c) are deduced from (a) analogously to the corresponding parts of 3.12.bc.

3.14. (a) Suppose that the polynomial is reducible. Analogously to the proof of the Irreducibility over $\mathbb{Q}[\varepsilon_q]$ Lemma 3.13 (a) we have $r \in \mathbb{Q}[\varepsilon_q]$. Thus, $r^2, r^3, \dots, r^{q-1} \in \mathbb{Q}[\varepsilon_q]$.

In the following paragraph we prove that r is a root of some polynomial of degree at most $q-1$. This would contradict the irreducibility of $x^q - r^q$ over $\mathbb{Q}$.

Expand the numbers r^k as polynomials in ε_q for $k = 0, 1, \dots, q-1$:

$$r^k = a_{k,0} + a_{k,1}\varepsilon_q + \dots + a_{k,q-2}\varepsilon_q^{q-2}.$$

It suffices to find numbers $\lambda_0, \lambda_1, \dots, \lambda_{q-1} \in \mathbb{Q}$, not all of them zeros, such that

$$\lambda_0 a_{0,m} + \dots + \lambda_{q-1} a_{q-1,m} = 0 \quad \text{for every} \quad m = 0, 1, \dots, q-2$$

Such numbers exist analogously to the corresponding assertion in the second proof of the Rationality Lemma 3.8 (f).

Part (b) follows from (a).

3.15. Assume the contrary. Denote by P the given polynomial. The assumption $q < \deg P$ contradicts to the Rationality Lemma 3.12.d. If $q \geqslant \deg P$, then by the Conjugation Lemma 3.12.c and the Linear Independence Lemma over $\mathbb{Q}[\varepsilon_q]$ 3.14 (b), the polynomial P has pairwise distinct roots $x_k = A(r\varepsilon_q^k)$ for $k = 0, 1, 2, \dots, q-1$. For $q > \deg P$ we get a contradiction. When $q = \deg P$ the conditions $q \neq 2$ and $\overline{x_k} = x_{q-k} \neq x_k$ yield the uniqueness of the real root.

References

[Al] *Alekseev V. B.*, Abel's Theorem in Problems and Solutions. Springer Netherlands, 2004.

[AB] *Akhtyamov D.*, *Bogdanov I.*, Solvability of cubic and quartic equations using one radical. `http://arxiv.org/abs/1411.4990`.

[Dor] *Dörrie H.*, 100 Great Problems of Elementary Mathematics: Their History and Solution. New York: Dover Publ, 1965.

[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.

[Es] *Esterov A.*, Galois theory for general systems of polynomial equations, `https://arxiv.org/abs/1801.08260`

[FT] *Fuchs D., Tabachnikov S.*, Mathematical Omnibus. AMS, 2007.

[Had] *Hadlock Ch. R.*, Field Theory and its Classical Problems. The Mathematical Association of America, 1978. (Carus Mathematical Monographs, N 19.)

[Ka] *Kannunikov A. L.*, The beginning of Galois theory: solvability of algebraic equations by radicals (in Russian). `http://www.mathnet.ru/conf1015`.

[Ko17] *Kogan E.*, Set complexity of construction of a regular polygon, `https://arxiv.org/abs/1711.05807`.

[Kol] *Kolosov V. A.*, Theorems and problems in algebra, number theory and combinatorics (in Russian). M.: Helios, 2001.

[Ler] *Lerner L.*, Galois Theory without abstract algebra. `http://arxiv.org/abs/1108.4593`.

[Pr07-2] *Prasolov V. V.*, Problems in algebra, arithmetics and analysis, Moscow, MCCME, 2007.

[PSo] *Prasolov V. V.*, *Solovyev Y. P.*, Elliptic Functions and Elliptic Integrals. AMS, 1997.

[Saf] *Safin A.*, A program for construction of regular polygons by compass and ruler. `http://www.mccme.ru/mmks/dec08/Safin.pdf`.

[Sk10] *Skopenkov A.*, Basic embeddings and Hilbert's 13th problem (in Russian), Mat. Prosveschenie, 14 (2010) 143–174, `http://arxiv.org/abs/1001.4011`. Abridged English translation: `http://arxiv.org/abs/1003.1586`.

[Sk11] *Skopenkov A.*, A simple proof of the Abel-Ruffini theorem on insolvability of equations in radicals (in Russian), Mat. Prosveschenie, 15 (2011) 113-126. `http://arxiv.org/abs/1102.2100`.

[Sk15] *Skopenkov A.*, A short elementary proof of the Ruffini-Abel Theorem. `http://arxiv.org/abs/1508.03317`.

[Sk19] *Skopenkov A.*, Mathematics via problems: from olympiads and math circles to a profession. Algebra. AMS, Providence, to appear.

[St94] *Stillwell J.*, Galois theory for beginners, Amer. Math. Monthly, 101 (1994), 22-27.

[T] *Tikhomirov V. M.*, Abel and his great theorem, Kvant. 2003. N 1. P. 11–15.

[Vag] *Vaguten H.*, Conjugated numbers (in Russian), Kvant. 1980. N 2. P. 26–32.

[Vi] *Vinberg E. B.*, Algebra of polynomials (in Russian). M.: Prosveschenie, 1980.

[ZSS] Mathematics via problems: from olympiads and math circles to a profession (in Russian). Editors: A. Zaslavsky, A. Skopenkov and M. Skopenkov. MCCME, 2018. Abridged version: `http://www.mccme.ru/circles/oim/materials/sturm.pdf`.

[SZ19] Mathematics via problems: from olympiads and math circles to a profession. Geometry and Combinatorics. Editors: A. Zaslavsky, and M. Skopenkov. AMS, Providence, to appear.

[W] *Van der Waerden B. L.*, Algebra. Frederick Ungar Publishing, 1970.

4 Additional problems for successful teams

4.1. (a) Let $x, y, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$ and

$$\begin{cases} r^2 = p(x + y, xy) \\ g(x, y) = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.c). Then $r \in \mathbb{Q}(x, y)$.

(b) Let $x, y, r \in \mathbb{R}$, $p \in \mathbb{Q}[\sqrt{2}][u, v]$, $g \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ be such that $g(x, y) \notin \mathbb{Q}(x + y, xy, \sqrt{2})$ and the equations of (a) hold. Then there are $\rho \in \mathbb{Q}(x, y)$, $\pi \in \mathbb{Q}[\sqrt{2}][u, v]$ and $\pi_1 \in \mathbb{Q}[\sqrt{2}][u, v, w]$ such that the equations of (a) hold with r, p, p_1 replaced by ρ, π, π_1.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing $x + y, xy, r^2$ but not r. If $F(r) \cap \mathbb{Q}(x, y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x, y)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

4.2. Denote $a_j = \sigma_j(x_1, x_2, x_3)$, $j = 1, 2, 3$.

(a) Let $x_1, x_2, x_3, r \in \mathbb{R}$, $p, g \in \mathbb{Q}[u_1, u_2, u_3]$ and $p_1 \in \mathbb{Q}[u_1, u_2, u_3, v]$ be such that $g(x_1, x_2, x_3) \notin \mathbb{Q}(a_1, a_2, a_3)$ and

$$\begin{cases} r^2 = p(a_1, a_2, a_3) \\ g(x_1, x_2, x_3) = p_1(a_1, a_2, a_3, r) \end{cases}.$$

Then $r \in \mathbb{Q}(x_1, x_2, x_3)$.

(b) **Rationalization Lemma.** Let $x_1, x_2, x_3, r \in \mathbb{R}$ and $F \subset \mathbb{R}$ a field containing a_1, a_2, a_3, r^2 but not r. If $F(r) \cap \mathbb{Q}(x_1, x_2, x_3) \not\subset F$, then there is $\rho \in \mathbb{Q}(x_1, x_2, x_3)$ such that $\rho^2 \in F$ and $F(\rho) = F(r)$.

(c) **Proposition.** If $x_1, x_2, x_3 \in \mathbb{R}$ and x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals, then x_1 is $\{a_1, a_2, a_3\}$-expressible by quadratic real radicals so that every radical is in $\mathbb{Q}(x_1, x_2, x_3)$.

4.3. (a) Let $x, y, r \in \mathbb{C}$, $p \in \mathbb{Q}[u, v]$ and $p_1 \in \mathbb{Q}[u, v, w]$ be such that

$$\begin{cases} r^3 = p(x + y, xy) \\ x = p_1(x + y, xy, r) \end{cases}$$

(cf. Problem 2.14.d for $k = 3$). Then $r \in \mathbb{Q}[\varepsilon_3](x, y)$.

(b) Same as (a) with $x = p_1(x + y, xy, r)$ replaced by $g(x, y) = p_1(x + y, xy, r)$ for some $g \in \mathbb{Q}[u, v]$ such that $g(x, y) \notin \mathbb{Q}(x + y, xy)$.

(c) **Rationalization Lemma.** Let $x, y, r \in \mathbb{C}$ and $F \subset \mathbb{C}$ a field containing $x+y, xy, \varepsilon_3, r^3$ but not r. If $F(r) \cap \mathbb{Q}(x,y) \not\subset F$, then there is $\rho \in \mathbb{Q}(x,y)$ such that $\rho^3 \in F$ and $F(\rho) = F(r)$.

(d) **Rationalization Lemma.** Same as (c) with x, y replaced by $x_1, \ldots, x_n$ and $x+y, xy$ replaced by $\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)$.

(e) **Rationalization Lemma.** Same as (d) with r^3, ρ^3 replaced by r^q, ρ^q for a prime q and ε_3 replaced by ε_q.

(f) **Proposition.** If

$$x_1, \ldots, x_n \in \mathbb{C}, \quad M := \{\sigma_1(x_1, \ldots, x_n), \ldots, \sigma_n(x_1, \ldots, x_n)\}$$

and x_1 is M-expressible by radicals, then x_1 is M-expressible by radicals so that every radical is in $\bigcup_{q=3}^{\infty} \mathbb{Q}[\varepsilon_q](x_1, \ldots, x_n)$.

4.4. There are numbers $x, y \in \mathbb{R}$ such that if $p \in \mathbb{Q}[u, v]$ and $p(x, y) = 0$, then $p = 0$.

Such numbers are called *algebraically independent over* $\mathbb{Q}$.