Последовательности Сомоса

И. И. Богданов, Г. А. Голованов, К. Г. Куюмжиян,
А. В. Мирошников, А. В. Устинов, Б. Р. Френкин

Введение

Первый нетривиальный пример *последовательности Сомоса* — это последовательность Сомос-4. Она задаётся рекуррентным соотношением

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \tag{1}$$

где α и β — произвольные константы. Четвёрка в названии — это порядок рекуррентного соотношения (1). Он показывает, сколько надо задать начальных членов последовательности (s_n), чтобы можно было вычислить все остальные. Для последовательности Сомос-4 обычно считаются заданными s_0, s_1, s_2 и s_3.

Если взять коэффициенты $\alpha = \beta = 1$ и начальные условия $s_0 = s_1 = s_2 = s_3 = 1$, то получится последовательность Сомос-(4)

$$s_0, s_1, \ldots = 1, 1, 1, 1, 2, 3, 7, 23, 59, 314, 1529, 8209, 83313, \ldots, \tag{2}$$

которая удивительным образом оказывается целочисленной. Другим её неожиданным свойством является периодичность по произвольному модулю.

Определение 1. В общем случае последовательность $(s_n)_{n=-\infty}^{\infty}$ называется *последовательностью Сомос-k*, если она удовлетворяет квадратичному рекуррентному соотношению k-го порядка ($k \geq 2$)

$$s_{n+k}s_n = \sum_{1\leq j\leq k/2} \alpha_j s_{n+k-j}s_{n+j}, \tag{3}$$

где α_j ($1 \leq j \leq k/2$) — некоторые константы.

Мы считаем, что все члены последовательностей, а также параметры — комплексные числа. (Желающие могут ограничиться вещественными числами.)

Определение 2. Через *Сомос-(k)* обозначается последовательность Сомос-k, где все параметры и начальные условия равны 1, то есть эта последовательность задаётся начальными членами $s_0 = s_1 = \cdots = s_{k-1} = 1$ и соотношением

$$s_{n+k}s_n = \sum_{1\leq j\leq k/2} s_{n+k-j}s_{n+j}.$$

Целочисленной оказывается не только последовательность Сомос-(4), но и последовательности Сомос-(k) при $k = 5, 6, 7$. При бо́льших k это свойство теряется. Тем не менее, при каждом $k \geq 4$ среди всех последовательностей Сомос-k можно выделить большой класс последовательностей, которые являются целочисленными.

Целочисленность — это верный признак того, что мы имеем дело с объектом, который обладает богатыми арифметическими, алгебраическими, комбинаторными и аналитическими свойствами. Например, целочисленность и периодичность последовательности Сомос-(4) — это лишь вершина айсберга. За ними кроются не видимые на первый взгляд инварианты, скрытые теоремы сложения, тропическая арифметика, совершенные паросочетания и т. п. В случае последовательностей Сомос-4 и Сомос-5 всё объясняется тем, что за ними стоят эллиптические кривые. Начиная с последовательностей Сомос-6 всё становится сложней и интересней.

Проект в первую очередь направлен на то, чтобы познакомиться с теми идеями, которые стоят за последовательностями Сомос-4. Затем мы попробуем применить эти идеи к последовательностям Сомоса более высокого порядка, в надежде получить продвижения в нерешённых задачах.

1 Первое знакомство

Начальные условия $s_0, \ldots, s_{k-1}$ однозначно определяют всю последовательность (s_n), если её элементы не обращаются в нуль. В противном случае для нахождения элементов последовательности требуется накладывать дополнительные условия. За исключением специально оговорённых случаев при решении задач можно считать, что в последовательностях Сомос-k нулевых членов нет. Для последовательности Сомос-(k) это гарантируется задачей 1(а).

Задача 1.
(а) Последовательности Сомос-(k) определены корректно: ни один элемент в них не равен нулю.
(б) Последовательности Сомос-(2) и Сомос-(3) тривиальны: они состоят только из единиц.
(в) Последовательности Сомос-(k), $k \geq 4$, нетривиальны: предъявите элемент, не равный единице.
(г) Последовательности Сомос-(k) симметричны: для любого натурального n выполнено $s_{-n} = s_{n+k-1}$.

Задача 2. Для элементов последовательности Сомос-2, задаваемой уравнением $s_{n+2}s_n = \alpha s_{n+1}^2$, получите формулу, выражающую s_n через α и начальные условия s_0, s_1.

Задача 3. Пусть последовательность Сомос-3 задана уравнением $s_{n+3}s_n = \alpha s_{n+2}s_{n+1}$. Выразите s_n через s_{-1}, s_0, s_1 и α.

Задача 4.
(а) Пусть $k \geq 2$, $a, b, c, q \in \mathbb{R}$, $q > 0$ и (s_n) — последовательность Сомос-k. Тогда $(q^{an^2+bn+c}s_n)$ — также последовательность Сомос-k. Предполагая, что $k = 4$, выпишите рекуррентное соотношение на новую последовательность, если известно соотношение для исходной.
(б) Пусть $k \geq 2$ нечетно, $\gamma \in \mathbb{C}$ и (s_n) — последовательность Сомос-k. Тогда последовательности (a_n) и (b_n), задаваемые как

$$a_n = \begin{cases} s_n, & \text{если } n \text{ четно,} \\ \gamma s_n, & \text{если } n \text{ нечетно} \end{cases} \quad \text{и} \quad b_n = \begin{cases} \gamma s_n, & \text{если } n \text{ четно,} \\ s_n, & \text{если } n \text{ нечетно,} \end{cases}$$

также суть последовательности Сомос-k, удовлетворяющие тому же самому рекуррентному соотношению.
(в) Пусть (s_n) — последовательность Сомос-3. Тогда существуют (a_n) и (b_n) — последовательности Сомос-2, такие, что $s_n = \begin{cases} a_n, & \text{если } n \text{ четно,} \\ b_n, & \text{если } n \text{ нечетно.} \end{cases}$.

2 Простейшие свойства последовательностей Сомос-4

Напомним, что Сомос-4 — это последовательность, удовлетворяющая соотношению

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \qquad \alpha, \beta \in \mathbb{C}. \tag{4}$$

Задача 5. Пусть последовательность (s_n) удовлетворяет линейному уравнению второго порядка $s_{n+2} = us_{n+1} + vs_n$, $u, v \in \mathbb{C}$. Докажите, что (s_n) — последовательность Сомос-4. Выразите через u и v константы α и β в уравнении (4).

Задача 6. Докажите, что последовательность

$$s_n = (An + B)q^{an^2+bn+c} \tag{5}$$

является последовательностью Сомос-4. Выразите через A, B, a, b, c, q константы α и β в уравнении (4).

Задача 7. Докажите, что последовательность Сомос-(4) не является последовательностью вида (5).

Задача 8. Про последовательности (n^2), (2^{n^3}) выясните, являются ли они последовательностями (а) Сомос-4, (б) Сомос-6.

Задача 9*. Рассмотрим (s_n) — последовательность Сомос-4, удовлетворяющую уравнению (4) при $\alpha = \beta = 1$. Пусть $s_0 = 0$, $s_1 = s_2 = s_4 = 1$, $s_3 = -1$. (Для отрицательных номеров эту последовательность естественно доопределить по нечётности: $s_{-n} = -s_n$.) Тогда последовательность определена однозначно, и её элементы с нечётным индексом образуют знакопеременную последовательность Сомос-(4). [1]

3 Сомос-(4)

Задача 10. Пусть в последовательности Сомос-(4) элементы $s_0, \dots, s_n$ — целые числа. Тогда в любой четверке $(s_{k-3}, s_{k-2}, s_{k-1}, s_k)$, где $3 \le k \le n$, все числа попарно взаимно просты.

Задача 11. (а) Пусть в последовательности Сомос-(4) $s_{n-3} = a$, $s_{n-2} = b$, $s_{n-1} = c$ и s_n — целые числа. Используя задачу 10, выразите по модулю числа s_n значения s_{n+1}, s_{n+2}, s_{n+3}.
(б) Докажите, что все элементы последовательности Сомос-(4) — целые числа.

Замечание: Как отмечалось выше, целочисленными также являются последовательности Сомос-(k), при $k = 5, 6, 7$. При $k \ge 8$ последовательности Сомос-(k) перестают быть целочисленными. Например, начало последовательности Сомос-(8) выглядит следующим образом:

$$\dots, 1, 1, 1, 1, 1, 1, 1, 1, 4, 7, 13, 25, 61, 187, 775, 5827, 14815, \frac{420514}{7}, \dots$$

В проекте мы рассмотрим разные подходы к доказательству целочисленности последовательностей Сомос-(4) и Сомос-(5), которые в перспективе будут полезны и для последовательностей Сомоса более высокого порядка.

Задача 12. Последовательность $a_1, a_2, a_3, \dots$ задается начальными условиями $a_1 = 1, a_2 = 1$ и рекуррентным соотношением

$$a_n = \frac{a_{n-1}^2 + 2}{a_{n-2}} \qquad (n \ge 3).$$

Докажите, что все элементы этой последовательности — целые числа.

4 Скрытый инвариант последовательности Сомос-4

Как показывает задача 4а, последовательность Сомос-k допускает замены, после которых она удовлетворяет тому же самому уравнению. Этим обстоятельством можно воспользоваться для того, чтобы понизить порядок рекурренты.

Именно, пусть (s_n) — последовательность Сомос-k. Введём соответствующую ей *однородную последовательность* (f_n) формулой

$$f_n = \frac{s_{n-1}s_{n+1}}{s_n^2}.$$

Отметим, что при замене $(s_n) \mapsto (q^{bn+c}s_n)$ последовательность (f_n) не меняется.

Задача 13. (а) Пусть (s_n) — последовательность Сомос-4. Найдите рекуррентное соотношение порядка 2 для однородной последовательности (f_n).
(б) Пусть (s_n) — последовательность Сомос-5. Найдите рекуррентное соотношение порядка 3 для однородной последовательности (f_n).

Задача 14. Пусть (s_n) — последовательность Сомос-4, которой соответствует однородная последовательность (f_n).
(а) Докажите, что значение

$$T_n = f_{n-1}f_n + f_nf_{n+1} + \frac{\alpha}{f_n} \tag{6}$$

[1]Если эта задача кажется вам трудной, то её решение можно отложить до тех времён, когда появится больше сведений о последовательностях Сомос-4.

не зависит от n.
(б) Найдите выражение $T(x,y)$ такое, что $T_n = T(f_n, f_{n+1})$.

Замечание. Рекомендуем желающим подумать о том, из каких соображений можно *придумать* выражение (6)! Это может помочь в дальнейшем.

Таким образом, для данной последовательности (s_n) все выражения вида $T(f_n, f_{n+1})$ принимают одно и то же значение T.

Определение 3. Полученное значение T называется *инвариантом* данной последовательности Сомос-4.

Задача 15. Пусть (s_n) — последовательность Сомос-4 с соотношением (4); пусть T — её инвариант. Докажите, что тогда (s_n) также является последовательностью Сомос-5, то есть она удовлетворяет уравнению

$$s_{n+3}s_{n-2} = \mu s_{n+2}s_{n-1} + \nu s_{n+1}s_n$$

при некоторых константах μ и ν. Выразите эти константы через α, β и T.

Замечание. Верен более общий факт: любая последовательность Сомос-4 является последовательностью Сомос-k, $k \geq 4$. Доказательству этого факта будет посвящена отдельная серия задач.

Задача 16. Используя задачу 14 (и задачу 10), получите другое доказательство целочисленности последовательности Сомос-(4).

Задача 17. Используя задачу 15 (и задачу 10), получите ещё одно доказательство целочисленности последовательности Сомос-(4).

Задача 18. (а) Для каких последовательностей Сомос-4 можно доказать их целочисленность, используя те же идеи, что в задачах 16 и 17?
(б) Подумайте над тем, как получить критерий целочисленности последовательности Сомос-4.

Задача 19*. Пусть (s_n) — последовательность Сомос-4. Докажите, что подпоследовательности её элементов с чётными и нечётными номерами (s_{2n}) и (s_{2n+1}) также являются последовательностями Сомос-4.

5 Периодичность последовательности Сомос-4 по произвольному модулю

Задача 20. Докажите, что в последовательности Сомос-(4) нет чисел, делящихся на 5.

Определение 4. Будем называть последовательность (s_n) *примитивной*, если все её элементы — целые числа и не имеют общего для всех делителя, большего 1.

Задача 21. (а) Пусть p — простое число и (s_n) — примитивная последовательность Сомос-4, удовлетворяющая рекуррентному соотношению (4) с целыми коэффициентами α и β такими, что $(\alpha\beta, p) = 1$. Тогда в этой последовательности всегда можно выбрать три подряд идущих элемента, взаимно простых с p.
(б) В условиях пункта (а) для последовательности (s_n) корректно определен её инвариант $T \pmod{p^\gamma}$, где γ — натуральное число.

Задача 22. Пусть p — простое число, γ — натуральное число и (s_n) — примитивная последовательность Сомос-4, удовлетворяющая рекуррентному соотношению (4) с целыми коэффициентами α и β такими, что $(\alpha\beta, p) = 1$. Тогда остатки элементов последовательности (s_n) дают при делении на p^γ периодически повторяются.

Задача 23. (а) Пусть $m = p_1^{\gamma_1} \dots p_l^{\gamma_l}$ — каноническое разложение числа m на простые множители. Последовательность (a_n) периодична по каждому из модулей $p_i^{\gamma_i}$, $1 \leq i \leq l$. Докажите, что последовательность (a_n) будет периодической и по модулю m.
(б) Пусть m — натуральное число и (s_n) — примитивная последовательность Сомос-4, удовлетворяющая рекуррентному соотношению (4) с целыми коэффициентами α и β такими, что $(\alpha\beta, m) = 1$. Тогда остатки, которые элементы последовательности (s_n) дают при делении на m, периодически

повторяются.
(в) Остатки, которые элементы последовательности Сомос-(4) дают при делении на произвольное натуральное число m, периодически повторяются.

Задача 24. Докажите, что в условиях задачи 22 нельзя отбросить условие $(\alpha\beta, p) = 1$.

6 Последовательности Сомос-5

Задача 25. Пусть в последовательности Сомос-(5) элементы $s_0, \ldots, s_n$ — целые числа. Тогда в любой пятерке $(s_{k-4}, s_{k-3}, s_{k-2}, s_{k-1}, s_k)$, где $4 \leq k \leq n$, все числа попарно взаимно просты.

Пусть (s_n) — последовательность Сомос-5, заданная рекуррентным соотношением

$$s_{n+3}s_{n-2} = \mu s_{n+2}s_{n-1} + \nu s_{n+1}s_n. \tag{7}$$

Опять же обозначим через (f_n) соответствующую однородную последовательность.

Следующие две задачи посвящены поиску двух *независимых* инвариантов последовательности Сомос-(5), аналогичных инварианту T последовательности Сомос-4.

Задача 26. (а) Покажите, что в уравнении, полученном в задаче 13б, можно сделать ещё одну замену переменных, понижающую порядок уравнения (и упрощающую его).
(б) Найдите выражение $J_n = J_n(f_{n-1}, f_n, f_{n+1}, f_{n+2})$, обладающее такими же свойствами, как и выражение T_n в задаче 14а. Иначе говоря, значение J_n должно быть постоянным на любой однородной последовательности (f_n), но эти значения не должны совпадать для *всех* последовательностей, удовлетворяющих данному соотношению (7).
(в) Найдите нетривиальную функцию $J(x, y, z)$, являющуюся инвариантом данной однородной последовательности (то есть такую, что значение выражения $J = J(f_n, f_{n+1}, f_{n+2})$ не зависит от n).

Задача 27. (а) Преобразовав соотношение на (f_n) по-другому, найдите существенно другой *почти-инвариант*: выражение $K(x, y, z)$ такое, что значения $K(f_{n-1}, f_n, f_{n+1})$ совпадают при всех *чётных* n.
(б) Найдите ещё одно (существенно другое, чем в задаче 26!) выражение $I_n = I_n(f_{n-1}, f_n, f_{n+1}, f_{n+2})$, обладающее теми же свойствами, что и выражение в задаче 26б,
(в) ...и получите из него ещё один инвариант $I(x, y, z)$ последовательности (f_n).

Замечание. Если вам непонятны условия двух задач выше, обратитесь за разъяснениями!

Задача 28. С помощью каждой из задач 26, 27 докажите, что все элементы последовательности Сомос-(5) — целые числа.

Задача 29. Пусть m — натуральное число, и (s_n) — это последовательность Сомос-(5). С помощью инвариантов из задач 26, 27 докажите, что остатки элементов последовательности (s_n) при делении на m периодически повторяются.

Задача 30*. Докажите, что для любой последовательности (s_n), удовлетворяющей рекуррентному соотношению (7), каждая из подпоследовательностей $(s_n^*) = (s_{2n})$ и $(s_n^*) = (s_{2n+1})$ её элементов с чётными и нечётными номерами удовлетворяет уравнению Сомос-4

$$s_{n+2}^* s_{n-2}^* = \alpha^* s_{n+1}^* s_{n-1}^* + \beta^* (s_n^*)^2.$$

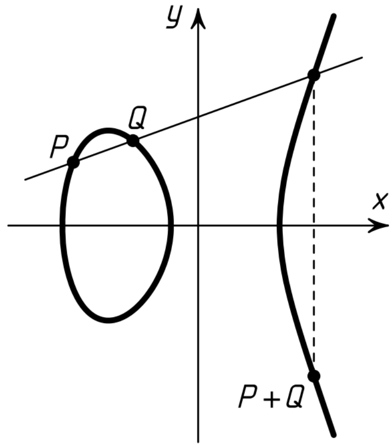
Как можно выразить коэффициенты α^* и β^*?

Задача 31*. Пусть (s_n) — последовательность Сомос-5, удовлетворяющая уравнению (7). Найдите условия на значения её инвариантов I и J, равносильные тому, что (s_n) является последовательностью Сомос-4.

Задача 32. Докажите, что умножив элементы последовательности Сомос-5 с чётными номерами на некоторое комплексное число, можно получить последовательность Сомос-4.

7 Связь с эллиптическими кривыми

В данном проекте под *эллиптической кривой* E мы будем понимать кривую на плоскости, заданную уравнением $y^2 = x^3 + ax + b$, с условием $4a^3 + 27b^2 \neq 0$. Прежде всего нас будут интересовать рациональные точки (точки с рациональными координатами) на таких кривых. Однако основные свойства (в первую очередь — возможность ввести на кривой структуру группы) будут справедливы для точек с вещественными и комплексными координатами.



Достаточно общая прямая пересекает эллиптическую кривую в трёх точках. Давайте договоримся, что сумма этих трёх точек будет равна нулю. Строго это формулируется так.

Определение 5. Рассмотрим две точки P и Q на эллиптической кривой, не симметричные друг другу относительно оси абсцисс. Определим сумму $P + Q$ следующим образом: проведём через P и Q прямую, рассмотрим третью точку R' пересечения этой прямой с нашей эллиптической кривой (она может совпадать с P или Q), отразим R' симметрично относительно оси абсцисс (отметим, что наша кривая симметрична относительно оси абсцисс). Полученную точку R назовём *суммой* точек P и Q, записывая это как $R = P + Q$.

Задача 33. Докажите, что это определение корректно, выпишите координаты R. Докажите, что $P + Q = Q + P$.

Добавим к нашей эллиптической кривой ещё одну точку: бесконечно удалённую. Будем считать, что это точка пересечения всех вертикальных прямых.

Задача 34. Как складывать обычную точку и бесконечно удалённую? В каком случае сумма двух обычных точек на эллиптической кривой даст бесконечно удалённую?

Задача 35*. Рассмотрим две тройки прямых на плоскости l_1, l_2, l_3 и m_1, m_2, m_3. Если из девяти (различных!) точек пересечения $l_i \cap m_j$ восемь лежат на эллиптической кривой E, то девятая точка пересечения тоже лежит на E.

Далее задачей 35 можно пользоваться без доказательства.

Задача 36*. Проверить тождество $(P+Q)+R = P+(Q+R)$ для точек на эллиптической кривой (ассоциативность сложения).

Задача 37. Пусть коэффициенты a и b рациональны. Если обе координаты P и Q рациональны, то координаты $P + Q$ также рациональны.

Замечание для участников, знакомых с понятием группы. Мы только что доказали, что точки эллиптической кривой образуют абелеву группу по сложению. Рациональные точки образуют подгруппу в этой группе.

Задача 38. Как определить $P + P$? Выпишите формулы для координат. Как определить $3P$, $4P$?

Пусть теперь (s_n) — последовательность Сомос-4, а (f_n) — соответствующая однородная последовательность. Инвариант T сообщает, что все точки вида (f_n, f_{n+1}) лежат на кривой четвёртого порядка

$$X^2Y^2 + \alpha(X + Y) + \beta - TXY = 0. \tag{8}$$

Оказывается, порядок этого уравнения может быть понижен.

Задача 39. (а) Сделайте в (8) замену переменных $x = -4\alpha X$. $y = 4\alpha(TX - \alpha - 2X^2 Y)$. Какое уравнение получилось?
(б) Как привести полученное уравнение к стандартному уравнению эллиптической кривой?

Задача 40. (а) Рассмотрим последовательность, определённую в задаче 9, и соответствующую ей однородную последовательность (f_n) (что такое f_0?). Пусть P_n — соответствующая ей последовательность точек на кубической кривой, построенной в предыдущей задаче. Докажите, что $P_n = nP_1$.
(б) Решите задачу 9.

Задача 41. (а) Докажите, что последовательность точек, соответствующих произвольной последовательности Сомос-4, является арифметической прогрессией, то есть $P_n = P_{n-1} + P$, где P — постоянная точка.
(б) Что означает, что полученная прогрессия имеет вид (nP)?

Предположим, что есть эллиптическая кривая E заданная уравнением $y^2 = x^3 + ax + b$ и точка $P = (x, y)$ на ней. Если посчитать первые точки вида nP, то окажется, что их координаты имеют специальный вид. Всегда найдётся такой многочлен $\psi_n = \psi_n(x, y) \in \mathbb{Z}[x, y, a, b]$, что $nP = \left(\frac{\dots}{\psi_n^2}, \frac{\dots}{\psi_n^3}\right)$. Вот первые элементы этой последовательности:

$$\begin{gathered}\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3).\end{gathered} \tag{9}$$

Кроме того, оказывается, что значения $\psi_5, \psi_6, \dots$ можно находить с помощью рекуррентного соотношения

$$\psi_1^2\psi_{n+2}\psi_{n-2} = \psi_2^2\psi_{n+1}\psi_{n-1} - \psi_1\psi_3\psi_n^2 \qquad (n \geq 3)$$

или с помощью пары соотношений

$$\begin{aligned}\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad (n \geq 2), \\ \psi_{2n} &= \frac{\psi_n}{2y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \qquad (n \geq 3).\end{aligned}$$

Многочлены $\psi_n(x, y)$ связанные с эллиптической кривой E называются *полиномами деления* (division polynomials). Для конкретной кривой с выбранной на ней точкой последовательность $\psi_n(x, y)$ становится числовой последовательностью.

Задача 42. Пусть дана эллиптическая кривая $y^2 = x^3 - x + \frac{1}{4}$ и точка $P = (0, \frac{1}{2})$ на ней. Проверьте, что им соответствует последовательность

$$\psi_0, \psi_1, \ldots = 0, \mathbf{1}, 1, -\mathbf{1}, 1, \mathbf{2}, -1, -\mathbf{3}, -5, \mathbf{7}, -4, -\mathbf{23}, 29, \mathbf{59}, 129, \ldots, \tag{10}$$

задаваемая начальными условиями $\psi_1 = \psi_2 = 1$, $\psi_3 = -1$, $\psi_4 = 1$ и рекуррентным соотношением

$$\psi_{n+2}\psi_{n-2} = \psi_{n+1}\psi_{n-1} + \psi_n^2 \qquad (n \geq 3).$$

Докажите, что в терминах переменных $f_n = \psi_{n+1}\psi_{n-1}/\psi_n^2$ координаты точки nP при $n \geq 2$ имеют вид

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1})\right).$$

Задача 43. Докажите, что в случае произвольной кривой $y^2 = x^3 + ax + b$ и точки $P = (x, y)$ на ней координаты точки nP при $n \geq 2$ имеют вид

$$nP = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right) = \left(x - f_n, \frac{f_n^2}{4y}(f_{n+1} - f_{n-1})\right), \tag{11}$$

где $\varphi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}$, $\omega_n = \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$.

Для этого установите, что последовательность (ψ_n) имеет инвариант $T = 2(a+3x^2)$, и коэффициент углового наклона секущей, проходящей через точки nP и P есть $k_n = -\frac{1}{4y}(2f_nf_{n+1} - T)$.

8 Сомос-4 есть Сомос-m

Одним из свойств последовательностей Сомоса малого порядка является то, что они удовлетворяют рекуррентным соотношениям более высоких порядков.

Задача 44. Докажите, что произвольная последовательность Сомос-2 является последовательностью Сомос-m при любом $m \geq 3$.

Задача 45. Докажите, что произвольная последовательность Сомос-3 является последовательностью Сомос-m при любом $m \geq 4$.

Аналогичное свойство выполняется и для произвольной последовательности Сомос-4: она является и последовательностью Сомос-m для любого $m \geq 5$. Более того, верно более сильное утверждение: существуют последовательности $(c_k)_{k=1}^{\infty}$ и $(d_k)_{k=1}^{\infty}$, для которых

$$s_{n+k}s_{n-k} = c_k s_{n+1}s_{n-1} - d_k s_n^2, \tag{12}$$

и последовательности $(u_k)_{k=-\infty}^{\infty}$ и $(v_k)_{k=-\infty}^{\infty}$ такие, что

$$s_{n+k+1}s_{n-k} = u_k s_{n+2}s_{n-1} - v_k s_n s_{n+1}. \tag{13}$$

Следующие задачи посвящены доказательству этого факта и его следствиям.

Задача 46. При $k \geq 2$ найдите формулы, позволяющие вычислить коэффициенты c_{k+1}, d_{k+1} через c_{k-1}, d_{k-1}, c_k, d_k.

Задача 47. Найдите значения c_k, d_k при $k = 1, 2, 3$.

Задача 48. Выпишите соотношение, которому при $k \geq 3$ должны удовлетворять параметры c_{k-1}, d_{k-1}, c_k, d_k для того, чтобы значения c_{k+1}, d_{k+1} можно было найти по рекуррентным формулам из задачи 46. Докажите, что это соотношение действительно является верным.

Задача 49. Докажите, что на самом деле формула (12) может быть записана в виде

$$w_1^2 s_{n+k}s_{n-k} = w_k^2 s_{n+1}s_{n-1} - w_{k+1}w_{k-1}s_n^2, \tag{14}$$

где (w_n) — некоторая последовательность Сомос-4. Как в этой последовательности удобней всего выбрать начальные значения?

Задача 50. Докажите, что элементы последовательности (w_n) из предыдущей задачи удовлетворяют уравнению

$$w_1^2 w_{n+k}w_{n-k} = w_k^2 w_{n+1}w_{n-1} - w_{k+1}w_{k-1}w_n^2. \tag{15}$$

Задача 51. При $k \geq 2$ найдите формулы, позволяющие вычислить коэффициенты u_{k+1}, v_{k+1} рекуррентного соотношения (13) через u_{k-1}, v_{k-1}, u_k, v_k.

Задача 52. Выпишите соотношение, которому при $k \geq 3$ должны удовлетворять параметры u_{k-1}, v_{k-1}, u_k, v_k для того, чтобы значения u_{k+1}, v_{k+1} можно было найти по рекуррентным формулам из задачи 51. Докажите, что это соотношение действительно является верным.

Задача 53. Выразите u_k, v_k через элементы последовательности (w_n) из задачи 49.

Задача 54. Пусть числа k, l, m, n одновременно целые или полуцелые. Докажите, что

$$s_{k+l}s_{m+n}w_{k-l}w_{m-n} + s_{k+n}s_{l+m}w_{k-n}w_{l-m} - s_{k+m}s_{l+n}w_{k-m}w_{l-n} = 0, \tag{16}$$

и в частности,

$$w_{k+l}w_{m+n}w_{k-l}w_{m-n} + w_{k+n}w_{l+m}w_{k-n}w_{l-m} - w_{k+m}w_{l+n}w_{k-m}w_{l-n} = 0. \tag{17}$$

Задача 55. С помощью формул предыдущей задачи дайте ещё одно решение задачи 9: докажите, что элементы последовательности (10) связаны с элементами последовательности Сомос-(4) равенством $s_n = (-1)^n \psi_{2n-3}$ (выделены жирным в (10)).

Задача 56. Пусть (s_n) — последовательность Сомос-4. Докажите, что для любых a и b последовательность $(\tau_n) = (s_{an+b})$ также будет последовательностью Сомос-4.

9 Сложные задачи

Задача 57*. Найдите инварианты последовательности Сомос-6, удовлетворяющей уравнению

$$s_{n+3}s_{n-3} = \alpha s_{n+2}s_{n-2} + \beta s_{n+1}s_{n-1} + \gamma s_n^2, \qquad \alpha, \beta, \gamma \in \mathbb{C}. \tag{18}$$

Задача 58*. Докажите, что Сомос-(6) — целочисленная последовательность.

Задача 59*. Докажите, что последовательность Сомос-(6) по модулю произвольного натурального числа представляет собой периодическую последовательность.

Задача 60*. Найдите инварианты последовательности Сомос-7, удовлетворяющей уравнению

$$s_{n+4}s_{n-3} = \alpha s_{n+3}s_{n-2} + \beta s_{n+2}s_{n-1} + \gamma s_{n+1}s_n, \qquad \alpha, \beta, \gamma \in \mathbb{C}. \tag{19}$$

10 Нерешённые проблемы

Задача 61*. Для последовательности Сомос-6 докажите «теорему сложения», аналогичную формуле (14).

Задача 62*. Для последовательности Сомос-7 докажите «теорему сложения», аналогичную формуле (14).

Задача 63*. Можно ли элементы последовательности Сомос-7 с нечётными номерами умножить на константу так, чтобы получилась последовательность Сомос-6?

Задача 64*. Докажите, что последовательность Сомос-(7) по модулю произвольного натурального числа представляет собой периодическую последовательность.

Задача 65*. Докажите, что последовательность Сомос-(8) не является последовательностью Сомос-k при $k \neq 8$.

Задача 66*. Нетрудно видеть, что последовательности Сомос-k при $k = 4, 5, 6, 7$ являются частными случаями *последовательностей Гейла — Робинсона*, которые задаются рекуррентными соотношениями двух типов, двучленным

$$s_n s_{n-k} = \alpha s_{n-l}s_{n-k+l} + \beta s_{n-m}s_{n-k+m},$$

где $0 < l < m < k$, или трёхчленным

$$s_n s_{n-k} = \alpha s_{n-p}s_{n-k+p} + \beta s_{n-q}s_{n-k+q} + \gamma s_{n-r}s_{n-k+r},$$

где $0 < p < q < r < k$, и $p + q + r = k$. Придумайте подход, который позволял бы для таких последовательностей, находить инварианты, доказывать периодичность по модулю, теоремы сложения, …

Решения задач

Первое знакомство

Решение задачи 1. Все утверждения доказываются по индукции.
Сперва удобно доказать пункт (г). База $n = 0$ верна по условию. Пусть для $m < n$ верно $s_{-m} = s_{m+k-1}$. Тогда по рекуррентной формуле

$$s_{-n} = \frac{1}{s_{k-n}} \sum_{1\le j\le k/2} s_{-n+k-j}s_{-n+j} = \frac{1}{s_{n-1}} \sum_{1\le j\le k/2} s_{n+j-1}s_{n-j+k-1} = s_{n+k-1}.$$

Теперь, имея пункт (г), можно доказывать утверждения для последовательностей Сомос-(k) только для натуральных чисел. Пункт (а) верен, так как числитель строго положителен.

Пункт (б) верен по индукции. База верна по условию. Переход: $s_{n+2} = \frac{s_{n+1}^2}{s_n} = \frac{1}{1} = 1$ для Сомос-2 и $s_{n+3} = \frac{s_{n+2}s_{n+1}}{s_n} = \frac{1}{1} = 1$ для Сомос-3.

Для решения пункта (в) достаточно рассмотреть элемент $s_k = [k/2]$.

Решение задачи 2. Формула:

$$s_n = \alpha^{n(n-1)/2} s_0^{1-n} s_1^n. \tag{20}$$

Докажем её по индукции. Она даёт нужные значения при $n = 0$ и $n = 1$. Если предположить, что формула верна для $n = k - 1$ и $n = k$ ($k \geq 1$), то для s_{k+1} с помощью рекуррентного соотношения получаем нужное представление:

$$s_{k+1} = \alpha s_k^2 s_{k-1}^{-1} = \alpha \cdot \alpha^{k(k-1)} s_0^{2(1-k)} s_1^{2k} \alpha^{-(k-1)(k-2)/2} s_0^{2k} s_1^{1-k} = \alpha^{k(k+1)/2} s_0^{-k} s_1^{k+1}.$$

Решение задачи 3. Формула

$$s_n = \begin{cases} \alpha^{n^2/4} s_{-1}^{-n/2} s_0 s_1^{n/2}, & \text{если } n \text{ чётное;} \\ \alpha^{(n^2-1)/4} s_{-1}^{(1-n)/2} s_1^{(n+1)/2}, & \text{если } n \text{ нечётное.} \end{cases} \tag{21}$$

Доказывается по индукции аналогично.

Решение задачи 4.

(а) Достаточно доказать по отдельности, что если домножить элементы последовательности (s_n) на $q \in \mathbb{C}$, q^n или q^{n^2}, она останется последовательностью Сомос-k.

Для (qs_n) надо проверить равенство

$$(qs_{n+k})(qs_n) = \sum_{1 \leq j \leq k/2} \alpha_j (qs_{n+k-j})(qs_{n+j}), \quad \text{или} \quad q^2 s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \alpha_j q^2 s_{n+k-j} s_{n+j}.$$

Оно получается из исходного умножением на q^2.

Для $(q^n s_n)$ нужное равенство имеет вид

$$(q^{n+k} s_{n+k})(q^n s_n) = \sum_{1 \leq j \leq k/2} \alpha_j (q^{n+k-j} s_{n+k-j})(q^{n+j} s_{n+j}), \quad \text{или} \quad q^{2n+k} s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \alpha_j q^{2n+k} s_{n+k-j} s_{n+j}.$$

Оно получается из исходного умножением на q^{2n+k}.

Для $(q^{n^2} s_n)$ уравнение изменится. Нам нужно получить равенство вида

$$(q^{(n+k)^2} s_{n+k})(q^{n^2} s_n) = \sum_{1 \leq j \leq k/2} \beta_j (q^{(n+k-j)^2} s_{n+k-j})(q^{(n+j)^2} s_{n+j}),$$

которое преобразуется к виду

$$s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \left(\beta_j q^{2j^2 - 2kj}\right) s_{n+k-j} s_{n+j}.$$

Значит, достаточно выбрать $\beta_j = \alpha_j q^{2kj - 2j^2}$.

(б) Заметим, что если k нечетно, то для любого целого j числа $n + k - j$ и $n + j$ имеют разную четность, а потому $a_{n+k-j} a_{n+j} = b_{n+k-j} b_{n+j} = \gamma s_{n+k-j} s_{n+j}$, и на $\gamma \neq 0$ можно сократить в каждом слагаемом рекуррентного соотношения.

(в) Из задачи 3 получаем, что в последовательности (a_n) при чётных n мы должны иметь $a_n = \alpha^{n^2/4} s_{-1}^{-n/2} s_0 s_1^{n/2}$; теперь из результата задачи 2 нетрудно получить, что подойдёт последовательность вида

$$a_n = (\alpha^{1/2})^{n(n-1)/2} (\alpha^{1/4} (s_1/s_{-1})^{1/2})^n s_0,$$

где, например, через $\alpha^{1/4}$ обозначено такое комплексное число β, что $\beta^4 = \alpha$. Полученная последовательность удовлетворяет соотношению $a_{n+2} a_n = \alpha^{1/2} a_{n+1}^2$.

Последовательность (b_n) строится аналогично и удовлетворяет тому же соотношению.

Простейшие свойства последовательностей Сомос-4

Решение задачи 5. Пусть $v \neq 0$. Если $s_{n+2} = us_{n+1} + vs_n$, то $s_{n-2} = -\frac{u}{v}s_{n-1} + \frac{1}{v}s_n$. Значит,

$$s_{n+2}s_{n-2} = (us_{n+1} + vs_n)\left(-\frac{u}{v}s_{n-1} + \frac{1}{v}s_n\right) =$$
$$= s_n^2 - \frac{u^2}{v}s_{n-1}s_{n+1} + s_n\left(\frac{u}{v}s_{n+1} - us_{n-1}\right) = s_n^2\left(1 + \frac{u^2}{v}\right) - \frac{u^2}{v}s_{n-1}s_{n+1}.$$

Таким образом, $\alpha = -u^2/v$ и $\beta = 1 + u^2/v$.
Случай $v = 0$ дает рекуррентную формулу $s_n = us_{n-1}$, откуда $s_n = u^n s_0$. Тогда $s_{n+2}s_{n-2} = u^{2n}s_0^2 = s_n^2 = s_{n+1}s_{n-1}$. Таким образом, s_n будет последовательностью Сомос-4 для любых α, β с условием $\alpha + \beta = 1$.

Решение задачи 6. Подставляя $s_n = (An + B)q^{an^2+bn+c}$ в уравнение (1), приходим к равенству

$$(A^2(n^2-4) + 2ABn + B^2)q^{8a} = \alpha(A^2(n^2-1) + 2ABn + B^2)q^{2a} + \beta(A^2n^2 + 2ABn + B^2),$$

которое должно выполняться для всех целых n. Это означает, что коэффициенты при всех степенях n в левой и правой частях должны совпадать. Сравнивая коэффициенты при n^2 и при n^0, приходим к системе уравнений

$$q^{8a} = \alpha q^{2a} + \beta, \qquad (-4A^2 + B^2)q^{8a} = \alpha(-A^2 + B^2)q^{2a} + \beta B^2.$$

Равенство коэффициентов при n^1 также сводится к первому уравнению. Решая систему, находим единственное решение $\alpha = 4q^{6a}$, $\beta = -3q^{8a}$.

Решение задачи 7. Если бы последовательность Сомос-(4) имела вид $s_n = (An+B)q^{an^2+bn+c}$, то, согласно задаче 6, выполнялись бы равенства $q^{6a} = 1/4$, $q^{8a} = -1/3$. Но эти два равенства не могут выполняться одновременно, т. к. из них следовало бы, что $4^{-4} = q^{24a} = -3^{-3}$.

Решение задачи 8. С одной стороны, если предположить, что $s_n = n^2$ — это последовательность Сомос-4, то для некоторых α, β и всех целых n должно выполняться равенство

$$n^4 - 8n^2 + 16 = \alpha(n^4 - 2n^2 + 1) + \beta n^4.$$

Сравнение коэффициентов при различных степенях n приводит к несовместной системе уравнений на α и β. Поэтому $s_n = n^2$ — это не последовательность Сомос-4. С другой стороны, это будет последовательность Сомос-6, поскольку возможно подобрать коэффициенты α, β, γ так, чтобы для всех целых n выполнялось равенство

$$n^4 - 18n^2 + 81 = \alpha(n^4 - 8n^2 + 16) + \beta(n^4 - 2n^2 + 1) + \gamma n^4.$$

Сравнение коэффициентов при различных степенях n приводит к системе

$$1 + \alpha + \beta + \gamma, \quad -18 = -8\alpha - 2\beta, \quad 81 = 16\alpha + \beta,$$

единственным решением которой является тройка $(\alpha, \beta, \gamma) = (6, -15, 10)$.

Подстановка $s_n = 2^{n^3}$ в уравнение (1) приводит к равенству $2^{24n} = \alpha 2^{6n} + \beta$. Такое равенство не может выполняться при всех целых n, так как левая часть при $n \to \infty$ растёт быстрее правой. Аналогично проверяется, что последовательность $s_n = 2^{n^3}$ не может быть последовательностью Сомос-k для любого $k \geq 2$. В частности, это не может быть последовательность Сомос-6.

Решение задачи 9. См. решения задач 30, 40 и 55 ниже.

Сомос-(4)

Решение задачи 10. Решим задачу по индукции. При $n = 0$ мы имеем четверку $(s_0, s_1, s_2, s_3) = (1, 1, 1, 1)$, в которой все числа попарно взаимно просты. Пусть $(s_{n+3}, s_{n+2}, s_{n+1}, s_n)$ — это первая четверка, в которой нашлись не взаимно простые числа. Тогда есть простое p, которое делит s_{n+3} и одно из чисел s_{n+2}, s_{n+1}, s_n. Пользуясь рекуррентным соотношением $s_{n+3}s_{n-1} = s_{n+2}s_n + s_{n+1}^2$, находим, что если $p \mid s_{n+2}$ или $p \mid s_n$, то $p \mid s_{n+1}$. Если $p \mid s_{n+1}$, то $p \mid s_{n+2}s_n$. В любом случае $p \mid (s_n, s_{n+2}s_{n+1})$, что противоречит сделанному предположению.

Решение задачи 11.
(а) В введенных обозначениях $s_{n-3} = a$, $s_{n-2} = b$, $s_{n-1} = c$. Тогда $s_n s_{n-4} = ac + b^2$, и s_n делит $ac + b^2$. Согласно задаче 10, $(abc, s_n) = 1$. Поэтому мы можем несколько раз применить рекуррентное соотношение $s_{k+1}s_{k-3} = s_k s_{k-2} + s_{k-1}^2$ по модулю числа s_n для $k = n,\ n+1,\ n+2$:

$$s_{n+1}a = s_n b + c^2 \equiv c^2 \pmod{s_n},\ \text{т. е. } s_{n+1} \equiv c^2 a^{-1} \pmod{s_n};$$
$$s_{n+2}b = s_{n+1}c + s_n^2 \equiv s_{n+1}c \pmod{s_n},\ \text{т. е. } s_{n+2} \equiv c^3 a^{-1} b^{-1} \pmod{s_n};$$
$$s_{n+3}c = s_{n+2}s_n + s_{n+1}^2 \equiv s_{n+1}^2 \pmod{s_n},\ \text{т. е. } s_{n+3} \equiv c^3 a^{-2} \pmod{s_n}.$$

Здесь везде подразумевается, что обратный элемент вычисляется по модулю s_n. [2]
(б) Проверим, что если числа $s_{n-4}, \ldots, s_n, \ldots, s_{n+3}$ — целые (очевидно, это утверждение верно при $n = 4$), то число s_{n+4} также будет целым. Тогда по индукции получим, что все числа s_n — целые. Из формул выше, наш фрагмент последовательности по модулю s_n выглядит как

$$a, \quad b, \quad c, \quad 0, \quad c^2a^{-1}, \quad c^3a^{-1}b^{-1}, \quad c^3a^{-2}.$$

Следующий элемент s_{n+4} мы должны находить из равенства $s_n s_{n+4} = s_{n+1}s_{n+3} + s_{n+2}^2$. Но теперь мы можем проверить делимость правой части на s_n, заменив все числа их остатками от деления на s_n:

$$s_{n+1}s_{n+3} + s_{n+2}^2 \equiv c^5(ac + b^2)a^{-3}b^{-2} \equiv 0 \pmod{s_n}.$$

Таким образом s_n делит $s_{n+1}s_{n+3} + s_{n+2}^2$, и s_{n+4} — целое число.

Решение задачи 12. Будем доказывать целочисленность последовательности (a_n) по индукции. Предположим, что $n \geq 3$, и числа $a_1, a_2, \ldots, a_n$ — целые. Проверим, что a_{n+1} также будет целым числом.

Из начальных условий и рекуррентного соотношения следует, что все числа $a_1, a_2, \ldots, a_n$ — нечётные. Это в свою очередь влечёт за собой то, что при $k = 2, \ldots, n-1$ числа a_{k-1} и a_k взаимно просты. (Если это не так, и k — наименьший номер, для которого $d = (a_{k-1}, a_k) > 1$, то из равенства $a_{k-1}a_{k+1} = a_k^2 + 2$ получаем, что $d = 2$. Но это невозможно, поскольку d — нечётное число.)

Значение a_{n+1} находится из равенства $a_{n+1}a_{n-1} = a_n^2 + 2$, и для доказательства целочисленности a_{n+1} достаточно проверить, что $a_n^2 + 2 \equiv 0 \pmod{a_{n-1}}$. Из рекуррентного соотношения находим, что

$$a_n^2 + 2 = \left(\frac{a_{n-1}^2 + 2}{a_{n-2}}\right)^2 + 2 = \frac{a_{n-1}^2(a_{n-1}^2 + 4) + 2a_{n-1}a_{n+1}}{a_{n-2}^2}.$$

Поскольку $(a_{n-1}, a_{n-2}) = 1$, то после сокращения числителя и знаменателя на a_{n-2}^2 числитель будет по-прежнему делиться на a_{n-1}, а значит число $(a_n^2 + 2)/a_{n-1}$ будет целым.

[2]Обратным к a по модулю m называется такое число a^{-1}, что $aa^{-1} \equiv 1 \pmod{m}$. Обратный элемент существует тогда и только тогда, когда $(a, m) = 1$. Далее во всех сравнениях обратные элементы будут пониматься именно в таком смысле.

Скрытый инвариант последовательности Сомос-4

Решение задачи 13. (а) $f_{n-1}f_n^2f_{n+1} = \alpha f_n + \beta$, (б) $f_{n-1}f_n^2f_{n+1}^2f_{n+2} = \mu f_nf_{n+1} + \nu$.

Решение задачи 14.
(а) Перепишем соотношения из задачи 13(а) в двух видах:

$$f_nf_{n+1} = \frac{\alpha}{f_{n-1}} + \frac{\beta}{f_{n-1}f_n} \quad \text{и} \quad f_{n-2}f_{n-1} = \frac{\alpha}{f_n} + \frac{\beta}{f_{n-1}f_n} \tag{22}$$

(для второго равенства мы сдвинули индекс на 1). Вычитая одно равенство из другого, получаем

$$f_nf_{n+1} + \frac{\alpha}{f_n} = f_{n-2}f_{n-1} + \frac{\alpha}{f_{n-1}}.$$

Прибавив к обеим частям $f_{n-1}f_n$, получаем $T_n = T_{n-1}$, что и надо было доказать.
(б) Выражая $f_{n-1}f_n$ через f_n и f_{n+1}, получаем, что годится функция

$$T(x,y) = xy + \alpha\left(\frac{1}{x} + \frac{1}{y}\right) + \frac{\beta}{xy}.$$

Решение задачи 15. Перейдем к однородной последовательности (f_n). По задаче 13(б) уравнение (7) примет вид

$$f_{n+2}f_{n+1}^2f_n^2f_{n-1} = \mu f_nf_{n+1} + \nu.$$

Попробуем подобрать коэффициенты μ и ν так, чтобы это равенство действительно выполнялось. Из рекуррентного соотношения 13(а) следует, что

$$f_{n+2}f_{n+1}f_n = \alpha + \frac{\beta}{f_{n+1}}, \qquad f_{n+1}f_nf_{n-1} = \alpha + \frac{\beta}{f_n}.$$

Перемножая эти равенства, получаем, что μ и ν при любом n должны удовлетворять соотношению

$$\left(\alpha + \frac{\beta}{f_{n+1}}\right)\left(\alpha + \frac{\beta}{f_n}\right) = \mu f_nf_{n+1} + \nu,$$

которое можно переписать в виде

$$\nu - \alpha^2 = -\mu f_nf_{n+1} + \alpha\beta\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) + \frac{\beta^2}{f_nf_{n+1}}. \tag{23}$$

Правая часть этого равенства оказывается похожа на формулу (6) для инварианта T. С учётом этой формулы получаем, что μ и ν должны удовлетворять соотношению

$$\nu - \alpha^2 = \beta T - (\beta + \mu)f_nf_{n+1}.$$

Так как произведение f_nf_{n+1} может принимать разные значения, для выполнения последнего равенства необходимо, чтобы $\mu = -\beta$. После этого находим, что $\nu = \alpha^2 + \beta T$. Полученные необходимые условия на μ и ν являются и достаточными для того, чтобы выполнялась формула (23), равносильная уравнению (7).

Решение задачи 16. Переписав выражение (6) в терминах последовательности (s_n), получаем

$$T = \frac{s_{n-2}s_{n+1}}{s_{n-1}s_n} + \frac{s_{n-1}s_{n+2}}{s_ns_{n+1}} + \frac{\alpha s_n^2}{s_{n-1}s_{n+1}}, \tag{24}$$

откуда выражаем

$$s_{n+2} = \frac{Ts_{n+1}s_ns_{n-1} - s_{n+1}^2s_{n-2} - \alpha s_n^3}{s_{n-1}^2}. \tag{25}$$

Для последовательности Сомос-(4) значение инварианта T равно 4. Будем предполагать, что $n \geq 3$, и целочисленность элементов $s_0, \ldots, s_{n+1}$ уже доказана. Тогда из рекуррентного соотношения следует, что $s_{n-2}s_{n+2}$ — целое число, а из соотношения выше — что $s_{n-1}^2 s_{n+2}$ тоже целое. Значит, знаменатель числа s_{n+2} в несократимой записи является делителем чисел s_{n-2} и s_{n-1}^2. Поскольку они взаимно просты, отсюда вытекает, что s_{n+2} целое. По индукции получаем, что вся последовательность Сомос-(4) целочисленна.

Решение задачи 17. Для последовательности Сомос-(4) значение инварианта T равно 4. По задаче 15 эта последовательность удовлетворяет уравнению

$$s_{n+2}s_{n-3} = -s_{n+1}s_{n-2} + 5s_n s_{n-1}. \tag{26}$$

Теперь можно провести такую же индукцию, как и выше: поскольку $s_{n+2}s_{n-2}$ и $s_{n+2}s_{n-3}$ целые, причём $(s_{n-2}, s_{n-3}) = 1$, то и само s_{n+2} целое.

Решение задачи 18. (а) Найдём несколько достаточных условий целочисленности, используя идею из задачи 15 (наличие двух рекуррентных соотношений). Предположим, что целыми числами являются коэффициенты α и β, инвариант T и первые пять членов $s_0, s_1, \ldots, s_4$. Тогда каждое новое число в последовательности можно находить с помощью формул

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \quad s_{n+2}s_{n-3} = \mu s_{n+1}s_{n-2} + \nu s_n s_{n-1},$$

где $\mu = -\beta$ и $\nu = \alpha^2 + \beta T$ — целые числа.

Если s_0, s_1, $\ldots$, s_{n+1} — целые числа, то для целочисленности s_{n+2} достаточно, чтобы $(s_{n-2}, s_{n-3}) = 1$; если это не так, то каждый простой делитель p, делящий (s_{n-2}, s_{n+3}) может оказаться в знаменателе s_{n+2} и всех последующих чисел. Условие $(s_{n-2}, s_{n-3}) = 1$ будет выполняться при всех $n \geq 3$, если потребовать, чтобы $(s_0, s_1) = 1$ и $\beta = \pm 1$.

Если $\beta \neq \pm 1$, то последовательность будет целочисленной, если для любого простого p, делящего β, в последовательности не будет элементов, делящихся на p. Для этого нужно требовать, чтобы $(\alpha, p) = 1$. И тогда по модулю p мы будем иметь сравнение $s_{n+2}s_{n-2} \equiv \alpha s_{n+1}s_{n-1} \pmod{p}$. Из него следует, что элементы последовательности не делятся на p при условии, что этому условию удовлетворяют s_0, s_1, s_2, s_3.

(б) Окончательный критерий целочисленности элементов последовательности Сомос-4 неизвестен. Один из полезных инструментов у нас появится чуть позже, см. раздел «Сомос-4 есть Сомос-m».

Решение задачи 19. Найдём константы α' и β', для которых будет выполняться равенство

$$s_{n+4}s_{n-4} = \alpha' s_{n+2}s_{n-2} + \beta' s_n^2. \tag{27}$$

В терминах переменных f_n оно становится рекуррентным соотношением шестого порядка

$$f_{n+3}f_{n+2}^2 f_{n+1}^3 f_n^4 f_{n-1}^3 f_{n-2}^2 f_{n-3} = \alpha' f_{n+1} f_n^2 f_{n-1} + \beta'.$$

Если воспользоваться равенствами

$$f_{n+3}f_{n+2}^2 f_{n+1} = \alpha f_{n+2} + \beta, \quad f_{n-3}f_{n-2}^2 f_{n-1} = \alpha f_{n-2} + \beta, \quad f_{n+1}f_n^2 f_{n-1} = \alpha f_n + \beta,$$

то порядок можно понизить до четвёртого:

$$(\alpha f_{n+2} + \beta)(\alpha f_{n-2} + \beta)(\alpha f_n + \beta)^2 = \alpha'(\alpha f_n + \beta) + \beta'. \tag{28}$$

Избавимся теперь от переменных f_{n+2} и f_{n-2}. Они входят в формулу симметрично. Поэтому всё можно свести к переменным f_{n+1}, f_n и f_{n-1}, если выразить через них произведение $f_{n+2}f_{n-2}$ и сумму $f_{n+2} + f_{n-2}$. Точно так же любой симметрический многочлен от f_{n+1} и f_{n-1} мы можем выразить через f_n, поскольку

$$f_{n+1}f_{n-1} = \frac{\alpha f_n + \beta}{f_n^2} \quad \text{и} \quad f_{n+1} + f_{n-1} = \frac{T f_n - \alpha}{f_n^2}. \tag{29}$$

Упростим сначала произведение:

$$f_{n+2}f_{n-2} = \frac{f_{n+2}f_{n+1}^2 f_n \cdot f_n f_{n-1}^2 f_{n-2}}{f_{n+1}^2 f_n^4 f_{n-1}^2} f_n^2 = \frac{(\alpha f_{n+1} + \beta)(\alpha f_{n-1} + \beta)}{(\alpha f_n + \beta)^2} f_n^2 = \frac{\alpha(\alpha^2 + \beta T) f_n + \beta^2 f_n^2}{(\alpha f_n + \beta)^2}.$$

Последний переход здесь был сделан с помощью равенств (29).

Упростим теперь сумму:

$$f_{n+2}+f_{n-2}=\frac{\alpha f_{n+1}+\beta}{f_{n+1}^2 f_n}+\frac{\alpha f_{n-1}+\beta}{f_{n-1}^2 f_n}=\frac{\alpha f_{n+1}f_{n-1}(f_{n+1}+f_{n-1})+\beta(f_{n+1}^2+f_{n-1}^2)}{(\alpha f_n+\beta)^2}f_n^3.$$

Снова избавляясь от f_{n+1}, f_{n-1} с помощью равенств (29), находим, что

$$f_{n+2}+f_{n-2}=\frac{-2\alpha\beta f_n^2+(\alpha^2 T+\beta T^2-2\beta^2)f_n-\alpha(\alpha^2+\beta T)}{(\alpha f_n+\beta)^2}.$$

Подставляя найденные представления для $f_{n+2}f_{n-2}$ и $f_{n+2}+f_{n-2}$ в формулу (28), получаем уравнение с одной переменной f_n:

$$\alpha^2(\alpha^3 f_n+\alpha\beta T f_n+\beta^2 f_n^2)+\alpha\beta(-2\alpha\beta f_n^2+(\alpha^2 T+\beta T^2-2\beta^2)f_n-\\ -\alpha(\alpha^2+\beta T))+\beta^2(\alpha f_n+\beta)^2=\alpha'(\alpha f_n+\beta)+\beta'.$$

Коэффициенты при f_n^2 в этом уравнении сокращаются. Равенство коэффициентов при f_n^1 и f_n^0 приводит к системе из двух уравнений с двумя неизвестными α' и β'. Решая систему, находим единственно возможные значения $\alpha'=(\alpha^2+\beta T)^2$, $\beta'=\beta^4-\beta(\alpha^2+\beta T)(2\alpha^2+\beta T)$. Поскольку все переходы были эквивалентными, при таких α' и β' будет выполняться рекуррентное соотношение (27).

Данное утверждение допускает более простое доказательство, см. комментарий к задаче 30.

Отметим, что эта задача позволяет решить задачу 9. Но мы получим несколько более концептуальных решений позже.

Периодичность последовательности Сомос-4 по произвольному модулю

Решение задачи 20.
Остатки, которые числа s_n дают при делении на 5, имеют вид

$$1,1,1,1,2,3,2,3,4,4,4,4,3,2,3,2,1,1,1,1,\ldots$$

Таким образом, $s_n\equiv s_{n+16} \pmod 5$ при $n=0,1,2,3$. Между четвёрками последовательных единиц не появилось нулевых остатков. Значит, и каждый следующий остаток можно было вычислять с помощью рекуррентного соотношения

$$s_{n+2}s_{n-2}\equiv s_{n+1}s_{n-1}+s_n^2 \pmod 5.$$

В частности, это означает, что остатки повторяются с периодом 16, и нулевой остаток при этом никогда не возникает.

Ещё одно решение получается, если воспользоваться рекуррентным соотношением (26). По модулю 5 оно превращается в сравнение

$$s_{n+2}s_{n-3}\equiv -s_{n+1}s_{n-2} \pmod 5.$$

Если предположить, что s_{n+2} — это первое число, делящееся на 5, то из этого сравнения следует, что $s_{n+1}s_{n-2}\equiv 0 \pmod 5$. Таким образом на 5 должно делиться и одно из чисел s_{n+1}, s_{n-2}, что противоречит сделанному предположению.

Решение задачи 21.
(a) Решение аналогично решению задачи 10.

Отметим сначала, что в последовательности (s_n) не может быть двух подряд идущих элементов, кратных p. Действительно, если $p\mid s_{n-2}$ и $p\mid s_{n-1}$, то из уравнения (1) и условия $(\beta,p)=1$ следует, что $p\mid s_n$. Повторяя это рассуждение, мы получаем, что все элементы последовательности (s_n) делятся на p. Таким образом, сделанное предположение противоречит условию примитивности последовательности (s_n).

Если найдутся два числа, кратные p, у которых номера отличаются на три, то снова приходим к противоречию. Действительно, если $p \mid s_{n-2}$ и $p \mid s_{n+1}$, то из уравнения (1) и условия $(\beta, p) = 1$ следует, что $p \mid s_n$. Значит, два подряд идущих элемента s_n и s_{n+1} делятся на p, что, как мы уже доказали, невозможно.

Предположим, что в последовательности (s_n) найдутся два элемента, кратных p и идущих через один. Если $p \mid s_{n-2}$ и $p \mid s_n$, то из уравнения (1) и условия $(\alpha, p) = 1$ следует, что $p \mid s_{n-1}s_{n+1}$. Тогда p делит s_n и один из соседних элементов, что снова приводит к противоречию: на p делятся либо два соседних элемента последовательности, либо два элемента, номера которых отличаются на три.

Из доказанных утверждений следует, что номера двух элементов последовательности, делящихся на p, отличаются по крайней мере на 4. Значит, всегда можно выбрать три подряд идущих элемента, взаимно простых с p.

(б) Выбрав три подряд идущих элемента, взаимно простых с p, можно найти значение $T \pmod{p^\gamma}$ по формуле (24). Иначе говоря, значение T — постоянное рациональное число, знаменатель которого не кратен p.

Решение задачи 22. Проверим, что значение $s_{n+2} \bmod p^\gamma$ однозначно определяется остатками, которые при делении на p^γ дают s_{n+1}, s_n, s_{n-1}, s_{n-2}, s_{n-3}. Действительно, для нахождения $s_{n+2} \bmod p^\gamma$ будем применять рекуррентные соотношения (1) и (7), записанные в виде

$$\begin{aligned} s_{n+2} &\equiv (\alpha s_{n+1}s_{n-1} + \beta s_n^2)s_{n-2}^{-1} \pmod{p^\gamma}, \\ s_{n+2} &\equiv (\mu s_{n+1}s_{n-2} + \nu s_n s_{n-1})s_{n-3}^{-1} \pmod{p^\gamma}. \end{aligned} \tag{30}$$

Первое из них имеет смысл, если $(s_{n-2}, p) = 1$. Второе, — если $(s_{n-3}, p) = 1$. Но хотя бы одно из этих условий всегда выполнено, т. к. два соседних элемента последовательности (s_n) не могут делиться на одно и то же простое число p одновременно (см. решение задачи 21).

Если мы рассмотрим первые $p^{5\gamma}$ пятёрок вида $(s_{n-3}, s_{n-2}, s_{n-1}, s_n, s_{n+1})$, то среди них найдутся по крайней мере две, в которых все соответственные числа дают одни и те же остатки от деления на p^γ. Из доказанного выше следует, что последовательность по модулю p^γ зациклится.

Решение задачи 23.
(а) Пусть T_i — период последовательности (a_n) по модулю $p_i^{\gamma_i}$ $(i = 1, 2, \ldots, l)$. Тогда для любого $i = 1, 2, \ldots, l$ и любого целого n будет выполняться сравнение $a_{n+T} \equiv a_n \pmod{p_i^{\gamma_i}}$, где $T = [T_1, T_2, \ldots, T_l]$ — наименьшее общее кратное всех периодов. Поскольку все числа $p_i^{\gamma_i}$ попарно взаимно просты, то из полученных сравнений следует, что $a_{n+T} \equiv a_n \pmod{m}$ $(n \in \mathbb{Z})$.
(б) Пусть $m = p_1^{\gamma_1} \ldots p_l^{\gamma_l}$ — каноническое разложение числа m. Из условия $(\alpha\beta, m) = 1$ следует $(\alpha\beta, p_i) = 1$ для $1 \le i \le l$. Потому выполнены условия задачи 22 и по каждому модулю $p_i^{\gamma_i}, 1 \le i \le l$ последовательность (s_n) периодична. Тогда по пункту (а) она периодична и по модулю m.
(в) Последовательность Сомос-(4) удовлетворяет условиям пункта (б), а потому является периодической по любому модулю.

Решение задачи 24. При простом p последовательность $s_n = p^{n^2}$ удовлетворяет уравнению (1) с $\alpha = 0$, $\beta = p^8$, но не является периодической по модулю p^γ для любого $\gamma > 0$.

Последовательности Сомос-5

Решение задачи 25. Докажем утверждение по индукции. При $n = 0$ мы имеем пятёрку $(s_0, s_1, s_2, s_3, s_4) = (1, 1, 1, 1, 1)$, в которой все числа попарно взаимно просты. Пусть $(s_{n+4}, s_{n+3}, s_{n+2}, s_{n+1}, s_n)$ — это первая пятёрка, в которой нашлись не взаимно простые числа. Тогда есть простое p, которое делит s_{n+4} и одно из чисел s_{n+3}, s_{n+2}, s_{n+1}, s_n. Пользуясь рекуррентным соотношением $s_{n+4}s_{n-1} = s_{n+3}s_n + s_{n+2}s_{n+1}$, находим, что если $p \mid s_{n+3}$ или $p \mid s_n$, то $p \mid s_{n+2}s_{n+1}$. Если $p \mid s_{n+2}$ или $p \mid s_{n+1}$, то $p \mid s_{n+3}s_n$. В любом случае $p \mid (s_{n+3}s_n, s_{n+2}s_{n+1})$, что противоречит сделанному предположению.

Решение задачи 26.
(а) Полагая $h_n = f_n f_{n+1}$, имеем

$$h_{n-1}h_n h_{n+1} = \mu h_n + \nu.$$

(б) Из предыдущего пункта получаем

$$h_{n+1}=\frac{\mu}{h_{n-1}}+\frac{\nu}{h_{n-1}h_n},\quad h_{n-2}=\frac{\mu}{h_n}+\frac{\nu}{h_{n-1}h_n}. \tag{31}$$

Значит,

$$\mu\left(\frac{1}{h_{n-1}}+\frac{1}{h_n}\right)+\frac{\nu}{h_{n-1}h_n}=h_{n-2}+\frac{\mu}{h_{n-1}}=h_{n+1}+\frac{\mu}{h_n}.$$

Поэтому

$$J=h_{n-2}+h_{n-1}+h_n+\frac{\mu}{h_{n-1}}=h_{n-1}+h_n+h_{n+1}+\frac{\mu}{h_n}. \tag{32}$$

Это и есть требуемый инвариант.

(в)

$$J(x,y,z)=xy+yz+\mu\left(\frac{1}{xy}+\frac{1}{yz}\right)+\frac{\nu}{xy^2z}.$$

Решение задачи 27.

(а) Положим $x_n=f_{n-1}f_nf_{n+1}$. Тогда рекуррентное соотношение из задачи 13(б) переписывается в виде

$$x_nx_{n+1}=\mu f_nf_{n+1}+\nu,$$

откуда

$$x_{n+1}=\frac{\mu}{f_{n-1}}+\frac{\nu}{x_n}.\quad x_{n-1}=\frac{\mu}{f_{n+1}}+\frac{\nu}{x_n},$$

Значит,

$$\mu\left(\frac{1}{f_{n+1}}+\frac{1}{f_{n-1}}\right)+\frac{\nu}{x_n}=x_{n-1}+\frac{\mu}{f_{n-1}}=x_{n+1}+\frac{\mu}{f_{n+1}}.$$

Это даёт даже два (дополняющих друг друга) почти-инварианта:

$$K_1(x,y,z)=\mu\left(\frac{1}{x}+\frac{1}{z}\right)+\frac{\nu}{xyz}\quad \text{и}\quad K_2(x,y,z)=xyz+\frac{\mu}{y}, \tag{33}$$

поскольку $K_1(f_{n-1},f_n,f_{n+1})=K_2(f_{n-2},f_{n-1},f_n)$ и наоборот.

(б,в) Из доказанного следует, что в качестве I годится сумма двух почти-инвариантов выше:

$$I(x,y,z)=K_1(x,y,z)+K_2(x,y,z)=xyz+\mu\left(\frac{1}{x}+\frac{1}{y}+\frac{1}{z}\right)+\frac{\nu}{xyz}. \tag{34}$$

При этом можно также записать другие выражения для значения этого инварианта, расписав

$$\begin{aligned}I_n=I(f_{n-1},f_n,f_{n+1})&=K_1(f_{n-1},f_n,f_{n+1})+K_1(f_n,f_{n+1},f_{n+2})=K_2(f_{n-1},f_n,f_{n+1})+K_2(f_n,f_{n+1},f_{n+2})=\\&=\mu\left(\frac{1}{f_{n-1}}+\frac{1}{f_n}+\frac{1}{f_{n+1}}+\frac{1}{f_{n+2}}\right)+\nu\left(\frac{1}{f_{n-1}f_nf_{n+1}}+\frac{1}{f_nf_{n+1}f_{n+2}}\right)=\\&=f_{n-1}f_nf_{n+1}+f_nf_{n+1}f_{n+2}+\mu\left(\frac{1}{f_n}+\frac{1}{f_{n+1}}\right).\end{aligned} \tag{35}$$

Решение задачи 28. Докажем это утверждение индукцией по n. База индукции: $s_0=\ldots=s_4=1$. Пусть s_k - целое для любого $k\le n+2$. Обозначим $s_{n-2}=a$, $s_{n-1}=b$, $s_n=c$, $s_{n+1}=d$, $s_{n+2}=e$. Тогда из соотношения 7: s_{n+3} целое, если $be+cd\equiv 0 \pmod a$.

Оба инварианта J и I последовательности Сомос-(5) по задачам 26 и 27 равны 5 и их можно записать в виде:

$$J=\frac{ad}{bc}+\frac{be}{cd}+\frac{bc}{ad}+\frac{cd}{be}+\frac{c^2}{ae} \tag{36}$$

$$I=\frac{b^2}{ac}+\frac{c^2}{bd}+\frac{d^2}{ce}+\frac{ae}{bd}+\frac{bd}{ae} \tag{37}$$

Тогда домножив (36) и (37) на $abcde$ по модулю a получим $bc^2(be+cd) \equiv 0 \pmod a$ и $b^2d(be+cd) \equiv 0 \pmod a$ соответственно. Так как b, c и d по задаче 25 взаимно просты с a, то $be + cd$ делится на a в обоих случаях.

Решение задачи 29. Зафиксируем простое p, натуральное γ. Докажем индукцией по n, что s_n корректно определено по модулю p^γ. База индукции: $s_0 = \ldots = s_4 = 1$. Пусть s_k (целое для любого k по задаче 28)- корректно определено по модулю p^γ для любого $k \le n+2$. Обозначим $s_{n-2} = a$, $s_{n-1} = b$, $s_n = c$, $s_{n+1} = d$, $s_{n+2} = e$.

Если a не делится на p, то $s_{n+3} = \frac{be+cd}{a}$ корректно определено по модулю p^γ. Если же делится, то по 25 на p не делятся b, c, d, e.

Тогда определены $f_{n-1}, f_n, f_{n+1} \pmod{p^\gamma}$. Преобразуем многочлен (34) и подставим $y = f_n, z = f_{n+1}$:

$$f_n^2 f_{n+1}^2 x^2 + (f_n + f_{n+1} - I f_n f_{n+1})x + f_n f_{n+1} = 0$$

Этот многочлен имеет два корня f_{n-1} и f_{n+2}. По теореме Виета $f_{n+2} = \frac{I f_n f_{n+1} - (f_n + f_{n+1})}{f_n^2 f_{n+1}^2} - f_{n-1}$, откуда f_{n+2} определено корректно по модулю p^γ, а потому и $s_{n+3} = \frac{f_{n+2} s_{n+2}^2}{s_{n+1}}$ определено корректно по модулю p^γ. Таким образом, вся последовательность корректно определена по модулю p^γ и по принципу Дирихле найдутся две пятёрки подряд идущих элементов, одинаковые по модулю p^γ. Они и составят период последовательности Сомос-(5) по модулю p^γ.

Для перехода к произвольному натуральному m осталось воспользоваться задачей 23(а).

Решение задачи 30. Воспользуемся результатами задач 26(а) и 26(в). Введем последовательность $h_n = f_n f_{n+1}$, для которой выполнены соотношения

$$h_{n-1} h_n h_{n+1} = \mu h_n + \nu, \tag{38}$$

$$J = h_{n-1} + h_n + \mu\left(\frac{1}{h_{n-1}} + \frac{1}{h_n}\right) + \frac{\nu}{h_{n-1}h_n}. \tag{39}$$

Преобразуем величину

$$\frac{s_{n-4}s_{n+4}}{s_n^2} = h_{n-3}h_{n-2}h_{n-1}^2 h_n^2 h_{n+1} h_{n+2} = h_{n-1}h_n(\mu h_{n-2} + \nu)(\mu h_{n+1} + \nu).$$

Исключая h_{n-2} и h_{n+1} с помощью равенств (31), раскрывая скобки и учитывая (39), получаем уравнение, эквивалентное (1):

$$\frac{s_{n-4}s_{n+4}}{s_n^2} = \nu^2 h_{n-1}h_n + \mu(\mu^3 + 2\nu^2 + \mu\nu J) = \alpha^* \frac{s_{n-2}s_{n+2}}{s_n^2} + \beta^*,$$

где $\alpha^* = \nu^2$ и $\beta^* = \mu(\mu^3 + 2\nu^2 + \mu\nu J)$.

Полученное уравнение позволяет, в частности, решить и задачу 9. Для последовательности (ψ_n) параметры устроены следующим образом: $\alpha = \beta = 1$, $T = -2$, $\mu = -\beta = -1$, $\nu = \alpha^2 + \beta T = -1$, $J = -1$. Значит, $\alpha^* = \beta^* = 1$, т. е. последовательность $s_n = (\psi_{2n-3})$ удовлетворяет уравнению $s_{n+2}s_{n-2} = s_{n+1}s_{n-1} + s_n^2$. А так как первые четыре элемента этой последовательности — единицы, то это последовательность Сомос-(4).

Доказанное утверждение позволяет получить более простое решение задачи 19 . Согласно задаче 15, последовательность Сомос-4 удовлетворяет уравнению Сомос-5 с коэффициентами $\tilde{\alpha} = -\beta$ и $\tilde{\beta} = \alpha^2 + \beta T$. Применяя задачу 30, находим, что последовательность Сомос-4 удовлетворяет уравнению (27) с коэффициентами $\alpha' = \alpha^* = \tilde{\beta}^2 = (\alpha^2 + \beta T)^2$ и $\beta' = \beta^* = \tilde{\alpha}^4 + \tilde{\alpha}\tilde{\beta}(2\tilde{\beta} + \tilde{\alpha}J) = \beta^4 - \beta(\alpha^2 + \beta T)(2\alpha^2 + \beta T)$.

Решение задачи 31. Необходимым и достаточным является соотношение $I^2 = 4(\nu + \mu J)$.

Проверим необходимость этого условия. Пусть последовательность является как Сомос-4 (с коэффициентами α и β), так и Сомос-5 (с коэффициентами μ и ν). В задаче 15 были найдены формулы $\mu = -\beta$, $\nu = \alpha^2 + \beta T$. Также можно найти связь между инвариантами: из формулы (35) вытекает представление

$$I = f_{n-1}f_nf_{n+1} + f_nf_{n+1}f_{n+2} + \mu\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) = \left(\alpha + \frac{\beta}{f_n}\right) + \left(\alpha + \frac{\beta}{f_{n+1}}\right) - \beta\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) = 2\alpha,$$

а из формулы (32) — представление

$$J = f_{n-1}f_n + f_nf_{n+1} + f_{n+1}f_{n+2} + \frac{\mu}{f_nf_{n+1}} = f_{n-1}f_n + f_nf_{n+1} + \left(\frac{\alpha}{f_n} + \frac{\beta}{f_nf_{n+1}}\right) - \frac{\beta}{f_nf_{n+1}} = T. \qquad (40)$$

Поэтому

$$I^2 = 4\alpha^2 = 4(\alpha^2 + \beta T - \beta T) = 4(\nu + \mu J).$$

Для доказательства достаточности условия $I^2 = 4(\nu + \mu J)$ заметим, используя обозначения из решений задач 26 и 27, что

$$4(\nu+\mu J) = 4\left(x_n + \frac{\mu}{f_n}\right)\left(\frac{\mu}{f_{n-1}} + \frac{\mu}{f_{n+1}} + \frac{\nu}{x_n}\right) = I^2 - \left(x_n + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{x_n}\right)^2,$$

так что

$$I^2 - 4(\nu+\mu J) = \left(f_{n-1}f_nf_{n+1} + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{f_{n-1}f_nf_{n+1}}\right)^2.$$

Поэтому равенство $I^2 = 4(\nu + \mu J)$ означает, что

$$f_{n-1}f_nf_{n+1} + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{f_{n-1}f_nf_{n+1}} = 0. \qquad (41)$$

Из (34) и (41) получаем уравнение $f_{n-1}f_nf_{n+1} + \frac{\mu}{f_n} = I/2$, совпадающее с 13(a) при $\mu = -\beta$ и $I = 2\alpha$, то есть последовательность есть Сомос-4 с параметрами $\beta = -\mu$ и $\alpha = I/2$.

Решение задачи 32. При замене $s_{2n} \mapsto ts_{2n}$ $(t \neq 0)$ переменные f_n меняются следующим образом: $f_{2n} \mapsto t^{-2}f_{2n}$, $f_{2n+1} \mapsto t^2f_{2n+1}$. Следовательно, значение инварианта J не изменится, а почти-инварианты K_1 и K_2 (вычисленные при чётном n) перейдут в $K_{n,1}(t)$ и $K_{n,2}(t)$, где

$$K_{n,1}(t) = \frac{\mu}{t^2}\left(\frac{1}{f_{n-1}} + \frac{1}{f_{b+1}}\right) + \frac{\nu}{t^2f_{n-1}f_nf_{n+1}} = \frac{K_{0,1}}{t^2},$$
$$K_{n,2}(t) = t^2f_{n-1}f_nf_{n+1} + \frac{\mu t^2}{f_n} = t^2K_{0,2}.$$

Значит, I заменяется на $I(t) = K_{0,1}/t^2 + K_{0,2}t^2$. Согласно задаче 31, для того, чтобы последовательность Сомос-5 была последовательностью Сомос-4, необходимо и достаточно, чтобы выполнялось условие $I(t)^2 = 4(\nu + \mu J)$. Это уравнение на t имеет комплексное решение всегда, кроме, возможно, случая, когда $K_{0,1} = K_{0,2} = 0$.

Этот последний случай означает, что

$$\mu(f_{-1}f_0 + f_0f_1) + \nu = f_{-1}f_0^2f_1 + \mu = 0.$$

В этом случае, обозначая $f_{-1} = a$, $f_0 = b$, $f_1 = c$, мы имеем $\mu = -ab^2c$, $\nu = -\mu(ab+bc) = ab^3c(a+c)$, $J = ab + bc - (ab+bc) + b(a+c) = ab + bc$. Тогда $I^2 - 4(\nu+\mu J) = -4ab^3c(a+c) + ab^2c\cdot(ab+bc) = 0$, то есть условие уже автоматически выполнено.

Связь с эллиптическими кривыми

Решение задачи 33. Пусть точки P и Q имеют координаты (x_P, y_P) и (x_Q, y_Q). По предположению задачи $x_P \neq x_Q$, поэтому прямая, проходящая через точки P и Q, задаётся уравнением

$$(y - y_P)(x_Q - x_P) = (x - x_P)(y_Q - y_P).$$

Выразим из него y:

$$y = y_P + (x - x_P)\frac{y_Q - y_P}{x_Q - x_P} = x\frac{y_Q - y_P}{x_Q - x_P} + \frac{y_Px_Q - x_Py_Q}{x_Q - x_P}.$$

Для того, чтобы найти точки пересечения данной прямой с эллиптической кривой, достаточно подставить y в уравнение $y^2 = x^3 + ax + b$.

$$\left(x\frac{y_Q - y_P}{x_Q - x_P} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P}\right)^2 = x^3 + ax + b.$$

Получится кубическое уравнение относительно x, у которого уже есть два корня x_P и x_Q. Отметим, что тогда у него есть и третий корень, по теореме Виета равный $\left(\frac{y_Q-y_P}{x_Q-x_P}\right)^2 - x_P - x_Q$. (возможно, он совпадёт с каким-то из первых двух корней). По предыдущему равенству, ему соответствует значение

$$\frac{\left(\left(\frac{y_Q-y_P}{x_Q-x_P}\right)^2 - x_P - x_Q\right)(y_Q - y_P)}{x_Q - x_P} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P} =$$
$$= \frac{\left((y_Q - y_P)^2 - (x_P + x_Q)(x_Q - x_P)^2\right)(y_Q - y_P)}{(x_Q - x_P)^3} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P}.$$

Это точка R'. В задаче требуется построить точку R, её координаты будут

$$\left(\left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q,\ \frac{((y_Q - y_P)^2 - (x_P + x_Q)(x_Q - x_P)^2)(y_Q - y_P)}{(x_P - x_Q)^3} + \frac{y_P x_Q - x_P y_Q}{x_P - x_Q}\right). \tag{42}$$

Случай совпадающих точек P и Q разбирается в задаче 38.

Полученная формула симметрична относительно P и Q, поэтому сложение коммутативно.

Решение задачи 34. Если P – обычная точка, Q – бесконечно удалённая, то прямая PQ будет вертикальной, R' совпадёт с точкой, симметричной P относительно оси абсцисс, и тогда R совпадёт с P.

Сумма двух обычных точек на эллиптической кривой даст бесконечно удалённую, если прямая PQ будет вертикальной. Это возможно в двух случаях: если P и Q симметричны друг другу относительно оси абсцисс и если $P = Q$ и касательная в этой точке вертикальна.

Решение задачи 35. Пусть прямые l_1, l_2, l_3, m_1, m_2, m_3 задаются уравнениями

$$L_1(x,y) = 0,\ L_2(x,y) = 0,\ L_3(x,y) = 0,$$
$$M_1(x,y) = 0,\ M_2(x,y) = 0,\ M_3(x,y) = 0,$$

соответственно. Обозначим уравнение, задающее эллиптическую кривую, через $F(x,y) = 0$. Докажем, что найдутся такие числа α, β, что

$$F(x,y) = \alpha L_1(x,y)L_2(x,y)L_3(x,y) + \beta M_1(x,y)M_2(x,y)M_3(x,y). \tag{43}$$

Обозначим также точки пересечения прямых l_1, l_2, l_3 с m_1: $l_1 \cap m_1 = A$, $l_2 \cap m_1 = B$, $l_3 \cap m_1 = C$. Выберем на m_1 ещё точку $D = (d_1, d_2)$, отличную от A, B, C. Поскольку она не лежит ни на одной из прямых l_1, l_2, l_3, имеем: $L_1(d_1,d_2) \neq 0$, $L_2(d_1,d_2) \neq 0$, $L_3(d_1,d_2) \neq 0$. Подставляя в равенство (43) координаты точки (d_1, d_2), получаем уравнение

$$F(d_1,d_2) = \alpha L_1(d_1,d_2)L_2(d_1,d_2)L_3(d_1,d_2),$$

из которого можно найти α. При этом значении α разность

$$F(x,y) - \alpha L_1(x,y)L_2(x,y)L_3(x,y) - \beta M_1(x,y)M_2(x,y)M_3(x,y) \tag{44}$$

обращается в ноль в четырёх точках прямой m_1. Поскольку рассматриваемая разность – многочлен степени не выше третьей, из этого следует, что выписанная разность делится на многочлен $M_1(x,y)$ (это не очевидно, но легко доказывается).

Рассматривая аналогичным образом четыре точки на прямой l_1 (три точки пересечения с прямыми m_i и одну дополнительную), подбираем параметр β, для которого по аналогичным рассуждениям

рассматриваемая разность будет делиться на $L_1(x,y)$. В итоге для данных α, β эта разность будет иметь вид
$$L_1(x,y)M_1(x,y)N(x,y),$$
где N – многочлен степени не выше первой.

Теперь подставим в это выражение ещё какую-то из заданных точек, пусть $G = (g_1, g_2) = l_2 \cap m_3$. Имеем

$$0 = F(g_1,g_2) - \alpha L_1(g_1,g_2)L_2(g_1,g_2)L_3(g_1,g_2) - \beta M_1(g_1,g_2)M_2(g_1,g_2)M_3(g_1,g_2) = \\ = L_1(g_1,g_2)M_1(g_1,g_2)N(g_1,g_2).$$

Поскольку по условию задачи предполагалось, что все девять точек пересечения прямых различны, мы имеем $L_1(g_1,g_2) \neq 0$, $M_1(g_1,g_2) \neq 0$, и тогда $N(g_1,g_2) = 0$. Аналогично для точек $H = (h_1,h_2) = l_3 \cap m_2$ и $I = (i_1,i_2) = l_2 \cap m_2$ (для всех, кроме точки $l_3 \cap m_3$, принадлежность которой к эллиптической кривой мы хотим доказать) получаем, что $N(h_1,h_2) = 0$ и $N(i_1,i_2) = 0$. Получаем, что прямая, задаваемая уравнением $N(x,y) = 0$, совпадает одновременно и с прямой l_2, и с прямой m_2, противоречие, значит, это уравнение имеет степень 0, а не 1, и тождественно нулевое, поскольку зануляется в точке $G = (g_1,g_2)$. Значит, разность (44) обращается в ноль, откуда и следует, что точка $l_3 \cap m_3$ лежит на эллиптической кривой.

Решение задачи 36. Назовём бесконечно удалённую точку O и определим $-P$ как точку, сумма которой с P даёт O. Для доказательства ассоциативности сложения P, Q, R рассмотрим следующие прямые:

l_1 через точки Q, $-Q-R$, R; l_2 через точки $-P-Q$, O, $P+Q$; l_3 через P, $Q+R$, $-P-(Q+R)$;

m_1 через точки Q, $-P-Q$, P; m_2 через точки $-Q-R$, O, $Q+R$; m_3 через точки R, $P+Q$, $-R-(P+Q)$.

Поскольку из выписанных точек все, кроме $-P-(Q+R)$ и $-R-(P+Q)$, уже лежат на эллиптической кривой, по предыдущей задаче $l_3 \cap m_3$ также лежит на эллиптической кривой. Значит, $l_3 \cap m_3 = -P-(Q+R) = -R-(P+Q)$, и сложение точек ассоциативно.

Решение задачи 37. Из формул следует, что для рациональных x_P, y_P, x_Q, y_Q координаты x_R, y_R также всегда будут рациональны. (В случае $P = Q$ надо воспользоваться следуюшей задачей и рациональностью коэффициентов a и b.)

Решение задачи 38. Продифференцировав функцию $x^3 + ax + b - y^2$ по x и по y, получим, что её градиент есть $(3x^2 + a, -2y)$. Значит, уравнение прямой, касающейся нашей эллиптической кривой в точке (x_P, y_P), имеет вид
$$(3x_P^2 + a)(x - x_P) - 2y_P(y - y_P) = 0. \tag{45}$$
Это уравнение задаёт прямую во всех случаях, кроме случая $3x_P^2 + a = -2y_P = 0$. Несложная проверка показывает, что выполнение условий $3x_P^2 + a = -2y_P = x_P^3 + ax_P + b - y_P^2 = 0$ влечёт $4a^3 + 27b^2 = 0$, что запрещено по условию.

Далее при $y_P \neq 0$ решение аналогично решению задачи 33. Выразим y из уравнения (45):

$$y = y_P + \frac{(x - x_P)(3x_P^2 + a)}{2y_P}.$$

Подставим в уравнение эллиптической кривой:

$$\left(y_P + \frac{(x - x_P)(3x_P^2 + a)}{2y_P}\right)^2 = x^3 + ax + b.$$

Мы знаем два корня этого уравнения, они равны x_P. Также по теореме Виета сумма корней этого уравнения равна минус коэффициенту при x^2, то есть

$$\left(\frac{3x_P^2 + a}{2y_P}\right)^2.$$

Отсюда третий корень (всегда существует и) равен

$$\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P.$$

Ордината этой точки будет равна

$$y = y_P + \frac{\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P - x_P\right)(3x_P^2+a)}{2y_P},$$

а после отражения относительно оси абсцисс получим точку с координатами

$$\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P,\ -y_P - \frac{\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 3x_P\right)(3x_P^2+a)}{2y_P}\right).$$

Разберём также случай $y_P = 0$. В этом случае касательная вертикальна, $x = x_P$, и в качестве третьей точки пересечения с нашей эллиптической кривой получим бесконечно удалённую точку O. Заметим, что таких точек $(x_P, 0)$ на нашей кривой максимум три, они соответствуют корням уравнения $x^3 + ax + b = 0$. На картинке из раздела 7 таких точек три.

Решение задачи 39. (а) Имеем

$$X = -\frac{x}{4\alpha}, \qquad Y = \frac{1}{2X^2}\left(TX - \alpha - \frac{y}{4\alpha}\right) = -\frac{2\alpha}{x^2}(Tx + 4\alpha^2 + y).$$

После подстановки получается уравнение

$$(Tx + 4\alpha^2 + y)^2 - (x^3 + 8\alpha^2 Tx + 32\alpha^4 + 8\alpha^2 y) + 4\beta x^2 - (2T^2x^2 + 8\alpha^2 Tx + 2Txy) = 0,$$

или

$$y^2 = x^3 + (T^2 - 4\beta)x^2 + 8\alpha^2 Tx + 16\alpha^4, \tag{46}$$

(б) Переименуем координату x из предыдущего пункта в x'. Чтобы привести к стандартному виду, достаточно сделать замену $x = x' + (T^2 - 4\beta)/3$. Получится уравнение

$$y^2 = x^3 + \left(8\alpha^2 T - \frac{(T^2-4\beta)^2}{3}\right)x + \left(\frac{2(T^2-4\beta)^3}{27} - \frac{8\alpha^2 T}{3}(T^2 - 4\beta) + 16\alpha^4\right). \tag{47}$$

Замечание 1. Чтобы складывать точки на эллиптической кривой, чаще всего достаточно знать их координаты, но не уравнение кривой. Поэтому непосредственный вид координат точек для нас представляет бóльшую ценность, нежели уравнение (47) (хотя и последнее пригодится).

Замечание 2. В условие закралась некоторая неточность. Именно, мы всегда получаем последовательность точек на кубической кривой требуемого вида — но не всегда эта кривая эллиптична. Однако в нетривиальных случаях это так!

Решение задачи 40. В этом решении мы будем пользоваться результатами следующей задачи.

(а) Имеем $\alpha = \beta = 1$ и $T = -2$, из предыдущей задачи получаем кривую $y^2 = x^3 - 16x + 16$ и точки $P_n(-4f_n, -4(1 + 2f_n + 2f_n^2 f_{n+1}))$. Теперь из следующей задачи получается, что $P_n = nP$ для точки $P(0, -4)$.

(б) Члены последовательности с нечётными номерами соответствуют теперь точкам $Q_n = (-3P) + n \cdot Q$, где $Q = 2P = P_2 = (4, -4)$ (мы сразу совершили нужный сдвиг индексов).

Пусть $t_n = (-1)^n s_{2n-3}$; пусть (g_n) — однородная последовательность, соответствующая последовательности (t_n). Обозначим через (t'_n) и (g'_n) последовательность Сомос-(4) и её однородную последовательность. Видим, что $t_n = t'_n$ при $n = 0, 1, 2, 3$ (и, следовательно, $g_n = g'_n$ при $n = 1, 2$).

Заметим, что параметры $\alpha = \beta = 1$, $T = 4$ задают именно кривую $y^2 = x^3 - 16x + 16$ и прогрессию с разностью $Q = (4, -4)$. При этом эта прогрессия для членов $g'_1 = g'_2 = 1$ стартует с точки $Q_1 = (0, 4) = P_{-1}$. Значит, последовательности (g'_n) соответствует именно последовательность точек (Q_n), откуда ясно, что $g'_n = g_n$ при всех n. Наконец, поскольку $t'_n = t_n$ при $n = 0, 1, 2, 3$, отсюда следует, что $t'_n = t_n$ при всех n.

Замечание. Может показаться, что это решение работает, только если мы знаем, к чему хотим прийти. Однако нетрудно показать, что *любая* арифметическая прогрессия на эллиптической кривой соответствует некоторой однородной последовательности, из которой уже можно найти и соответствующую последовательность Сомос-4. Так что все параметры можно было найти и по ходу.

Решение задачи 41.
(а) В общем случае на нашей кривой получаются точки

$$P_n = (x_n, y_n) = \left(-4\alpha f_n + \frac{T^2 - 4\beta}{3},\ 4\alpha(Tf_n - \alpha - 2f_n^2 f_{n+1})\right).$$

Найдём точку $P = P_{n+1} - P_n = P_{n+1} + (-P_n)$ с координатами (x, y); наша цель — показать, что она не зависит от n.

Для начала упростим формулу для углового коэффициента прямой $(-P_n)P_{n+1}$:

$$\begin{aligned} k = \frac{y_{n+1} + y_n}{x_{n+1} - x_n} &= \frac{-T(f_n + f_{n+1}) + 2\alpha + 2f_n^2 f_{n+1} + 2f_{n+1}f_{n+2}}{f_{n+1} - f_n} \\ &= T - 2f_n f_{n+1} + \frac{2f_{n+1}}{f_{n+1} - f_n}\left(-T + \frac{\alpha}{f_{n+1}} + f_n f_{n+1} + f_{n+1}f_{n+2}\right) = T - 2f_n f_{n+1}, \end{aligned}$$

и потому

$$k^2 = (T - 2f_n f_{n+1})^2 = T^2 + 4(f_n^2 f_{n+1}^2 - Tf_n f_{n+1}) = T^2 - 4\alpha(f_n + f_{n+1}) - 4\beta.$$

Значит, имеем

$$x = k^2 - x_{n+1} - x_n = T^2 - 4\alpha(f_n + f_{n+1}) - 4\beta + 4\alpha(f_n + f_{n+1}) - \frac{2(T^2 - 4\beta)}{3} = \frac{T^2 - 4\beta}{3}$$

и отсюда

$$-y = -y_n + (x - x_n)k = 4\alpha(-Tf_n + \alpha + 2f_n^2 f_{n+1}) + 4\alpha f_n(T - 2f_n f_{n+1}) = 4\alpha^2.$$

Итого, точка $P = \left(\frac{T^2-4\beta}{3}, -4\alpha^2\right)$ постоянна, что и требовалось доказать.

(б) Если $P_n = nP$, то $P_0 = 0$ — бесконечно удалённая точка. Значит, f_0 должно обращаться в бесконечность, то есть $s_0 = 0$.

Решение задачи 42. Рекуррентное соотношение для элементов последовательности (ψ_n) в однородных координатах $f_n = \psi_{n-1}\psi_{n+1}/\psi_n^2$ принимает вид

$$f_{n+1}f_n^2 f_{n-1} = f_n + 1. \tag{48}$$

По начальным значениям $f_2 = -1$, $f_3 = 1$ мы можем найти значение инварианта: $T = -2$. Поэтому в вычислениях мы можем пользоваться формулами

$$f_n f_{n-1} + f_n f_{n+1} + \frac{1}{f_n} = f_n f_{n-1} + \frac{1}{f_{n-1}} + \frac{1}{f_n} + \frac{1}{f_n f_{n-1}} = -2. \tag{49}$$

Докажем по индукции равенство

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1})\right). \tag{50}$$

Координаты точки $P_2 = 2P_1$ вычисляются непосредственно по формулам удвоения: $P_2 = (1, \frac{1}{2})$. Значит, равенство (50) выполняется при $n = 2$. Предположим, что равенство (50) верно для некоторого $n \geq 2$ и проверим его справедливость для $n + 1$. При сложении точек nP и P коэффициент углового наклона секущей имеет вид

$$k_n = \frac{y_n - y_1}{x_n - x_1} = \frac{1}{-f_n}\left(\frac{f_n^2}{2}(f_{n+1} - f_{n-1} - \frac{1}{2}\right) = -(f_n f_{n+1} + 1).$$

Значит,

$$x_{n+1} = k_n^2 - x_n - x_1 = (f_n f_{n+1} + 1)^2 + f_n = -f_{n+1}.$$

После этого остаётся найти ординату точки P_{n+1}:

$$y_{n+1} = -k_n(x_{n+1} - x_1) - y_1 = -(f_n f_{n+1} + 1) f_{n+1} - \frac{1}{2} = \frac{f_{n+1}^2}{2}(f_{n+2} - fn).$$

На последнем шаге преобразований было использовано рекуррентное соотношение (48) и формулы для инварианта T (49).

Решение задачи 43. Значение инварианта $T = 2(a+3x^2)$ для последовательности (ψ_n) находится по начальным условиям (9). Таким образом в вычислениях мы можем пользоваться формулами

$$f_n f_{n-1} + f_n f_{n+1} + \frac{\alpha}{f_n} = f_n f_{n-1} + \alpha \left(\frac{1}{f_{n-1}} + \frac{1}{f_n} \right) + \frac{\beta}{f_n f_{n-1}} = T = 2(a + 3x^2). \tag{51}$$

Докажем по индукции равенство

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1}) \right). \tag{52}$$

Координаты точки $2P$ находятся непосредственно по формулам удвоения. Значит, равенство (52) выполняется при $n = 2$. Предположим, что равенство (52) верно для некоторого $n \geq 2$ и проверим его справедливость для $n+1$. При сложении точек nP и P коэффициент углового наклона секущей имеет вид

$$k_n = \frac{y_n - y_1}{x_n - x_1} = \frac{1}{-f_n} \left(\frac{f_n^2}{4y}(f_{n+1} - f_{n-1} - y \right) = -\frac{1}{4y}(2 f_n f_{n+1} - T).$$

Значит,

$$x_{n+1} = k_n^2 - x_n - x_1 = \frac{1}{16y^2}(2 f_n f_{n+1} - T)^2 - 2x + f_n = x - f_{n+1}.$$

После этого остаётся найти ординату точки P_{n+1}:

$$y_{n+1} = -k_n(x_{n+1} - x_1) - y_1 = -\frac{1}{4y}(2 f_n f_{n+1} - T) f_{n+1} - y = \frac{f_{n+1}^2}{4y}(f_{n+2} - fn).$$

На последнем шаге преобразований было использовано рекуррентное соотношение (48) и формулы для инварианта T (51).

Сомос-4 есть Сомос-m

Решение задачи 44. Утверждение задачи вытекает из равенств

$$s_{n+l} s_{n-l} = \alpha^{l^2} s_n^2 \quad (l \geq 0), \qquad s_{n+l+1} s_{n-l} = \alpha^{l(l+1)} s_{n+1} s_n \quad (l \geq 0),$$

которые проверяются с помощью формулы (20).

Решение задачи 45. Как и в предыдущей задаче, утверждение следует из явных формул (21):

$$s_{n+l} s_{n-l} = \alpha^{2l-2} s_{n+l-2} s_{n-l+2} \quad (l \geq 2), \qquad s_{n+l+1} s_{n-l} = \alpha^{l(l+1)/2} s_{n+1} s_n \quad (l \geq 0).$$

Решение задачи 46. Введём новые переменные

$$F_k^{(n)} = \frac{s_{n+k} s_{n-k}}{s_n^2}. \tag{53}$$

В частности, $F_0^{(n)} = 1$, $F_1^{(n)} = f_n$, $F_2^{(n)} = \alpha f_n + \beta$. Тогда равенство (12) можно переписать в виде

$$F_k^{(n)} = c_k f_n - d_k. \tag{54}$$

Так как $F_k^{(n)} = F_{-k}^{(n)}$, то достаточно ограничиться неотрицательными значениями k. Очевидно, что равенство (54) будет выполняться при $k=1$ и $k=2$, если положить

$$c_1 = 1, \quad d_1 = 0, \quad c_2 = \alpha, \quad d_2 = -\beta.$$

Для нахождения коэффициентов c_{k+1}, d_{k+1} по известным значениям c_{k-1}, d_{k-1}, c_k, d_k воспользуемся равенством

$$F_{k+1}^{(n)} = \frac{F_k^{(n-1)} F_k^{(n+1)}}{F_{k-1}^{(n)}} f_n^2,$$

которое следует из определения (53).

Преобразуем это равенство с помощью формулы (54):

$$F_{k+1}^{(n)} = \frac{(c_k f_{n-1} - d_k)(c_k f_{n+1} - d_k)}{c_{k-1} f_n - d_{k-1}} f_n^2 = \frac{c_k^2 f_{n-1} f_n^2 f_{n+1} - c_k d_k f_n^2 (f_{n-1} + f_{n+1}) + d_k^2 f_n^2}{c_{k-1} f_n - d_{k-1}}.$$

К правой части применим соотношения (48) и (6):

$$F_{k+1}^{(n)} = \frac{c_k^2(\alpha f_n + \beta) - c_k d_k (T f_n - \alpha) + d_k^2 f_n^2}{c_{k-1} f_n - d_{k-1}}.$$

Значит, равенство $F_{k+1}^{(n)} = c_{k+1} f_n - d_{k+1}$ равносильно тому, что

$$d_k^2 f_n^2 + c_k f_n (\alpha c_k - T d_k) + c_k(\beta c_k + \alpha d_k) - (c_{k+1} f_n - d_{k+1})(c_{k-1} f_n - d_{k-1}) = 0.$$

Приравнивая к нулю коэффициенты при различных степенях f_n, получаем **переопределённую** систему уравнений с неизвестными c_{k+1}, d_{k+1}:

$$c_{k+1} c_{k-1} = d_k^2, \tag{55}$$

$$c_{k-1} d_{k+1} + c_{k+1} d_{k-1} = -c_k(\alpha c_k - T d_k), \tag{56}$$

$$d_{k-1} d_{k+1} = c_k(\beta c_k + \alpha d_k). \tag{57}$$

Решение задачи 47.

$$c_1 = 1, \quad d_1 = 0, \quad c_2 = \alpha, \quad d_2 = -\beta.$$

$$c_3 = d_2^2 = \beta^2, \quad d_3 = -c_2(\alpha c_2 - T d_2) = -\alpha(\alpha^2 + \beta T)$$

Решение задачи 48. При $k = 2$ последнее уравнение вырождается, и значения $c_3 = \beta^2$, $d_3 = -\alpha(\alpha^2 + T\beta)$ находятся из первых двух уравнений. При $k \geq 3$ совместность системы (55)–(57) нуждается в обосновании. Будем предполагать, что значения c_{k+1} и d_{k+1} находятся из уравнений (55) и (57), то есть

$$c_{k+1} = \frac{d_k^2}{c_{k-1}}, \qquad d_{k+1} = \frac{c_k(\beta c_k + \alpha d_k)}{d_{k-1}}. \tag{58}$$

Подставляя их в уравнение (56) и деля на $c_k d_k$, получаем условие на совместность системы:

$$g_{k-1} g_k + \alpha \left(\frac{1}{g_{k-1}} + \frac{1}{g_k} \right) + \frac{\beta}{g_{k-1} g_k} = T, \tag{59}$$

где $g_k = d_k / c_k$. Из равенств $g_2 = -\beta/\alpha$, $g_3 = -\alpha(\alpha^2 + T\beta)/\beta^2$ следует справедливость формулы (59) при $k = 3$. Поделив второе из равенств (58) на первое, находим, что последовательность (g_k) удовлетворяет рекуррентному соотношению, совпадающему с рекуррентным соотношением для элементов последовательности (f_k):

$$g_{k-1} g_k^2 g_{k+1} = \alpha g_k + \beta.$$

Поэтому справедливость формулы (59) вытекает из задачи 14.

Для завершения решения необходимо обосновать корректность определения последовательностей (c_k) и (d_k) с помощью рекуррентных соотношений (58). Как отмечалось выше, последовательность

$s_n = n$ является последовательностью Сомос-4 и удовлетворяет рекуррентному уравнению $s_{n+2}s_{n-2} = 4s_{n+1}s_{n-1} - 3s_n^2$. Она удовлетворяет соотношению (54) при $c_k = k^2$, $d_k = k^2 - 1$. Поэтому элементы последовательностей (c_k) и (d_k), вычисленные по формулам (58), являются не равными тождественному нулю рациональными функциями от параметров α, β, T. Таким образом, элементы последовательностей (c_k) и (d_k) (за исключением $d_1 = 0$) не обращаются в ноль и поэтому действительно могут вычисляться по формулам (58).

Решение задачи 49. Последовательность (f_n) изначально строилась по последовательности (s_n). Поэтому аналогичной последовательности (g_n) должна также соответствовать некоторая последовательность Сомос–4, которую будем обозначать через (w_n). Из равенства $g_k = w_{k-1}w_{k+1}/w_k^2$ следует, что при заданных значениях $g_k = d_k/c_k$ элементы последовательности (w_n) определены однозначно с точностью до умножения на геометрическую прогрессию. Элементы последовательности (w_n) принимают наиболее простую форму, если считать, что $w_k^2 = c_k$, $w_{k-1}w_{k+1} = d_k$ $(k = 1, 2, \ldots)$. Тогда, исходя из начальных условий $w_0w_2 = 0$, $w_1^2 = 1$, $w_2^2 = \alpha$, естественно выбрать первые элементы последовательности следующим образом:

$$w_0 = 0, \quad w_1 = 1, \quad w_2 = -\sqrt{\alpha}. \tag{60}$$

Остальные элементы однозначно находятся из равенства $w_{k-1}w_{k+1} = d_k$ $(k = 2, 3, \ldots)$. Например,

$$w_3 = -\beta, \quad w_4 = \sqrt{\alpha}(\alpha^2 + T\beta), \quad w_5 = \beta^3 - \alpha^2(\alpha^2 + T\beta). \tag{61}$$

В терминах последовательности (w_n) равенство (54) записывается в виде

$$w_1^2 s_{n+k}s_{n-k} = w_k^2 s_{n+1}s_{n-1} - w_{k+1}w_{k-1}s_n^2, \tag{62}$$

что совпадает с формулой (14).

Решение задачи 50. Формула (62) применима, в частности, и к последовательности $s_n = w_n$. Отсюда и получается (15).

Решение задачи 51. Очевидно, что в качестве начальных условий достаточно взять

$$u_0 = 0, \quad v_0 = -1, \quad u_1 = 1, \quad v_1 = 0.$$

Коэффициенты, найденные в задаче 15, показывают, что $u_2 = -\beta$, $v_2 = -(\alpha^2 + T\beta)$.

Введём новые переменные

$$G_k^{(n)} = \frac{s_{n+k+1}s_{n-k}}{s_n s_{n+1}}. \tag{63}$$

В частности, $G_0^{(n)} = 1$, $G_1^{(n)} = h_n$, $G_2^{(n)} = h_{n-1}h_nh_{n+1} = -\beta h_n + \alpha^2 + T\beta$. Теперь равенство (13) можно переписать в виде

$$G_k^{(n)} = u_k h_n - v_k. \tag{64}$$

Так как $G_{-k}^{(n)} = G_{k-1}^{(n)}$, то для доказательства леммы достаточно определить (u_k) и (v_k) для неотрицательных значений k и положить $u_{-k} = u_{k-1}$, $v_{-k} = v_{k-1}$ $(k \geq 1)$.

Для нахождения коэффициентов u_{k+1}, v_{k+1} по известным значениям u_{k-1}, v_{k-1}, u_k, v_k воспользуемся равенством

$$G_{k+1}^{(n)} = \frac{G_k^{(n-1)}G_k^{(n+1)}}{G_{k-1}^{(n)}}h_n$$

которое следует из определения (63). Преобразуем это равенство с помощью формулы (64):

$$(u_{k+1}h_n - v_{k+1})(u_{k-1}h_n - v_{k-1}) = (u_kh_{n-1} - v_k)(u_kh_{n+1} - v_k)h_n.$$

С помощью формул (38) и (32) (и с учётом того, что, как мы выяснили в задаче 31, $J = T$) это равенство приводится к виду

$$\begin{aligned} h_n^2(u_{k+1}u_{k-1} - u_kv_k) - h_n(u_{k+1}v_{k-1} + u_{k-1}v_{k+1} - \beta u_k^2 - u_kv_kT + v_k^2) + \\ + (v_{k-1}v_{k+1} - u_k^2(\alpha^2 + T\beta) + u_kv_k\beta) = 0. \end{aligned}$$

Приравнивая к нулю коэффициенты при различных степенях h_n, получаем **переопределённую** систему уравнений с неизвестными u_{k+1}, v_{k+1} ($k \geq 2$):

$$u_{k+1}u_{k-1} = u_k v_k, \tag{65}$$
$$u_{k+1}v_{k-1} + u_{k-1}v_{k+1} = \beta u_k^2 + u_k v_k T - v_k^2, \tag{66}$$
$$v_{k-1}v_{k+1} = u_k^2(\alpha^2 + T\beta) - u_k v_k \beta. \tag{67}$$

Решение задачи 52. Из предыдущей задачи получаем

$$u_0 = 0, \quad v_0 = -1, \quad u_1 = 1, \quad v_1 = 0, \quad u_2 = -\beta, \quad v_2 = -(\alpha^2 + T\beta),$$
$$u_3 = \beta(\alpha^2 + T\beta), \quad v_3 = \beta^3 + (\alpha^2 + T\beta)T\beta - (\alpha^2 + T\beta)^2 = \beta^3 - \alpha^2(\alpha^2 + T\beta).$$

Подставляя значения u_{k+1} и v_{k+1}, выраженные из (65) и (67), в уравнение (66) и деля на $u_k v_k$, получаем условие на совместность системы

$$\xi_{k-1} + \xi_k - \beta\left(\frac{1}{\xi_{k-1}} + \frac{1}{\xi_k}\right) + \frac{\alpha^2 + T\beta}{\xi_{k-1}\xi_k} = T, \tag{68}$$

в котором $\xi_k = v_k/u_k$. В частности,

$$\xi_2 = \frac{\alpha^2 + T\beta}{\beta}, \qquad \xi_3 = \frac{\beta^3 - \alpha^2(\alpha^2 + T\beta)}{\beta(\alpha^2 + T\beta)};$$

подставляя, убеждаемся, что равенство (68) выполняется при $k = 3$.

Поделив (67) на (65) приходим к рекуррентному соотношению на элементы последовательности (ξ_k):

$$\xi_{k-1}\xi_k\xi_{k+1} = -\beta\xi_k + (\alpha^2 + T\beta). \tag{69}$$

Оно совпадает с соотношением (38) при $\mu = -\beta$ и $\nu = \alpha^2 + T\beta$. Таким образом справедливость формулы (68), а тем самым, и совместность системы (65)–(67) вытекает из решения задачи 26.

Корректность рекуррентных соотношений (65) и (67) (отсутствие деления на ноль) проверяется так же как и в задаче 48.

Решение задачи 53. Элементы последовательности (h_n) строились по последовательности Сомос-5 (s_n) по формуле

$$h_n = f_n f_{n+1} = \frac{s_{n-1}s_{n+2}}{s_n s_{n+1}}. \tag{70}$$

Однако на самом деле каждая получающаяся последовательность (h_n) соответствует некоторой последовательности Сомос-4. Действительно, по задаче 32 последовательность (s_n) можно преобразовать в Сомос-4, умножив члены с чётными номерами на константу. Это преобразование не меняет последовательности (h_n).

Поэтому последовательности (ξ_n) также должна соответствовать последовательность Сомос–4. Оказывается, что это будет та же последовательность (w_n), которая была описана в решению задачи 49. Действительно, при $k = 2, 3$ равенство $\xi_k = \frac{w_{k-1}w_{k+2}}{w_k w_{k+1}}$ проверяется с помощью формул (60) и (61), а при $k \geq 4$ оно следует из совпадения рекуррентных соотношений (38) и (69) (здесь мы пользуемся задачей 15, то есть тем, что (w_n) есть последовательность Сомос-5 с коэффициентами $\mu = -\beta$ и $\nu = \alpha^2 + T\beta$).

Теперь нетрудно догадаться, что

$$u_k = \frac{w_k w_{k+1}}{w_1 w_2}, \qquad v_k = \frac{w_{k+2}w_{k-1}}{w_1 w_2}.$$

Чтобы убедиться в этом, достаточно заметить, что эти равенства верны при $k = 1, 2$, и проверить, что эти равенства согласуются с формулами (65)–(67). Равенство (65) оказывается тождеством, равенство (67) — рекуррентным соотношением Сомос-5 для последовательности (w_n), а равенство (66) имеет вид (40).

Таким образом, соотношение (13) можно переписать в виде

$$w_1w_2s_{n+k+1}s_{n-k} = w_kw_{k+1}s_{n+2}s_{n-1} - w_{k+2}w_{k-1}s_ns_{n+1}. \tag{71}$$

В частности, при $s_n = w_n$

$$w_1w_2w_{n+k+1}w_{n-k} = w_kw_{k+1}w_{n+2}w_{n-1} - w_{k+2}w_{k-1}w_nw_{n+1}. \tag{72}$$

Решение задачи 54. Рассмотрим сначала случай, когда $k+l+m+n \equiv 0 \pmod 2$. Переходя к параметрам

$$a = \frac{k+l+m+n}{2}, \quad b = \frac{k+l-m-n}{2}, \quad c = \frac{k-l+m-n}{2}, \quad d = \frac{k-l-m+n}{2}, \tag{73}$$

равенство (16) можно переписать в виде

$$s_{a+b}s_{a-b}w_{c+d}w_{c-d} + s_{a+d}s_{a-d}w_{b+c}w_{b-c} - s_{a+c}s_{a-c}w_{b+d}w_{b-d} = 0. \tag{74}$$

Чтобы проверить справедливость этого равенства, достаточно ко всем произведениям вида $s_{x+y}s_{x-y}$ и $w_{x+y}w_{x-y}$ применить формулы (14) и (15) соответственно.

Рассмотрим теперь случай, когда $k+l+m+n \equiv 1 \pmod 2$. Заменой $k \to k+1$ формула (16) приводится к виду

$$s_{k+l+1}s_{m+n}w_{k-l+1}w_{m-n} + s_{k+n+1}s_{l+m}w_{k-n+1}w_{l-m} - s_{k+m+1}s_{l+n}w_{k-m+1}w_{l-n} = 0, \tag{75}$$

где $k+l+m+n \equiv 0 \pmod 2$. Та же замена переменных (73) позволяет переписать формулу (75) в виде

$$s_{a+b+1}s_{a-b}w_{c+d+1}w_{c-d} + s_{a+d+1}s_{a-d}w_{b+c+1}w_{b-c} - s_{a+c+1}s_{a-c}w_{b+d+1}w_{b-d} = 0. \tag{76}$$

Как и в предыдущем случае, для завершения доказательства остается ко всем произведениям вида $s_{x+y+1}s_{x-y}$ и $w_{x+y+1}w_{x-y}$ применить формулы (71) и (72) соответственно.

Замечание. Доказывая тождества для последовательностей Сомоса, мы фактически на элементарном языке строим теорию эллиптических функций. Одним из важных инструментов этой теории является σ-функция Вейерштрасса. Это функция комплексного аргумента, которая является двумерным аналогом синуса, она обращается в нуль в узлах данной решётки

$$\Lambda = \{x_1\omega_1 + x_2\omega_2 : x_1, x_2 \in \mathbb{Z}\},$$

где ω_1, ω_2 — два линейно независимых вектора на комплексной плоскости. Определяется σ-функция через бесконечное произведение

$$\sigma(z) = z \prod_{w \in \Lambda \setminus \{0\}} \left(1 - \frac{z}{w}\right) e^{\frac{z}{w} + \frac{z^2}{2w^2}}.$$

Равенство (74) является аналогом трёхчленного тождества Вейерштрасса

$$\sigma(a+b)\sigma(a-b)\sigma(c+d)\sigma(c-d) - \sigma(a+c)\sigma(a-c)\sigma(b+d)\sigma(b-d) + \\ + \sigma(a+d)\sigma(a-d)\sigma(b+c)\sigma(b-c) = 0.$$

В терминах σ-функции выписывается и общее решение уравнения Сомос-4:

$$s_n = AB^n \frac{\sigma(z_0 + nz)}{\sigma(z)^{n^2}}.$$

Шести параметрам, которые задают последовательность Сомос-4, в этой формуле отвечают другие шесть свободных параметров A, B, z, z_0, и неявно присутствующие ω_1, ω_2. Для последовательностей (ψ_n) формула проще:

$$\psi_n = \frac{\sigma(nz)}{\sigma(z)^{n^2}}.$$

Решение задачи 55. Отметим сначала, что равенство $s_n = (-1)^n\psi_{2n-3}$ выполняется при $n = 0, 1, 2, 3$. Поэтому, чтобы доказать равенство этих двух последовательностей, достаточно проверить, что числа $t_n = (-1)^n\psi_{2n-3}$ удовлетворяют тому же рекуррентному соотношению, которое задаёт последовательность Сомос-(4).

Элементы последовательности (ψ_n) удовлетворяют уравнению (15) с $k = 2$ вкупе с условиями $\psi_0 = 0$, $\psi_1 = 1$. Это означает, что к ним применима и формула (17). Заменим в ней параметры k, l, m и n на $2k+1$, 4, 2 и 0 соответственно. Получим равенство

$$\psi_{2k+5}\psi_{2k-3}\psi_2\psi_{-2} + \psi_{2k+3}\psi_{2k-1}\psi_4^2 - \psi_{2k+1}^2\psi_6\psi_4 = 0.$$

Подставляя в него значения $\psi_2 = 1$, $\psi_4 = 1$, $\psi_6 = -1$, для переменных $t_k = (-1)^n\psi_{2k-3}$ получаем нужное уравнение $t_{k+2}t_{k-2} = t_{k+1}t_{k-1} + t_k^2$.

Решение задачи 56. Превратим уравнение (16) в нужное нам рекуррентное соотношение. Для этого выберем параметры k, l, m, n равными соответственно

$$\frac{1}{2}(an+b+3a), \quad \frac{1}{2}(an+b+a), \quad \frac{1}{2}(an+b-3a), \quad \frac{1}{2}(an+b-a).$$

В итоге получится уравнение Сомос-4: $\tau_{n+2}\tau_{n-2}w_a w_{-a} + \tau_{n+1}\tau_{n-1}w_{2a}^2 - \tau_n^2 w_{3a}w_a = 0$.

Замечание. Другое решение этой задачи можно получить методами из предыдузего раздела, заметив, что *любая* арифметическая прогрессия на эллиптической кривой задаётся последовательностью Сомос-4.

Сложные задачи

К этим задачам мы приводим лишь ответы или наброски решений. Детали предлагаем восполнить интересующемуся читателю.

Решение задачи 57. Уравнение последовательности Сомос-6 в однородных переменных принимает вид

$$f_{n+2}f_{n+1}^2f_n^3f_{n-1}^2f_{n-2} = \alpha f_{n+1}f_n^2f_{n-1} + \beta f_n + \gamma.$$

У неё есть два независимых инварианта

$$\begin{aligned}
T_1 =&\gamma(f_1f_2f_3 + f_2f_3f_4) + \beta f_1f_2f_3f_4 + \frac{\beta^2}{f_1f_2f_3f_4} + \frac{\gamma^2}{f_1f_2^2f_3^2f_4} + \\
&+ \alpha\gamma\left(\frac{1}{f_1f_2} + \frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \alpha\beta\left(\frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4}\right) + \frac{\beta\gamma}{f_1f_2f_3f_4}\left(\frac{1}{f_2} + \frac{1}{f_3}\right) = \\
=&\gamma(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5) + \beta(f_1f_2f_3f_4 + f_2f_3f_4f_5) + \alpha\gamma\left(\frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \alpha\beta\left(\frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4}\right), \\
T_2 =&\gamma f_1f_2^2f_3^2f_4 + \alpha\beta(f_1f_2 + f_2f_3 + f_3f_4) + \beta\gamma\left(\frac{1}{f_1f_2} + \frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + (\alpha^2\beta + \gamma^2)\left(\frac{1}{f_1f_2f_3} + \frac{1}{f_2f_3f_4}\right) + \\
&+ \alpha\gamma\left(\frac{f_1f_2}{f_4} + \frac{f_3f_4}{f_1}\right) + \alpha^2\gamma\left(\frac{1}{f_1f_2^2f_3} + \frac{1}{f_2f_3^2f_4}\right) + \frac{\alpha\beta^2}{f_1f_2^2f_3^2f_4} + \frac{\alpha\gamma^2}{f_1f_2^3f_3^3f_4} + \frac{\alpha\beta\gamma}{f_1f_2^2f_3^2f_4}\left(\frac{1}{f_2} + \frac{1}{f_3}\right) = \\
=&\gamma(f_1f_2^2f_3^2f_4 + f_2f_3^2f_4^2f_5) + \alpha\beta(f_1f_2 + f_2f_3 + f_3f_4 + f_4f_5) + \beta\gamma\left(\frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \\
&+ \alpha\gamma\left(\frac{f_1f_2}{f_4} + \frac{f_4f_5}{f_2}\right) + (\alpha^2\beta + \gamma^2)\frac{1}{f_2f_3f_4} + \alpha^2\gamma\frac{1}{f_2f_3^2f_4}.
\end{aligned}$$

Решение задачи 58. Пусть в последовательности Сомос-(6) элементы s_0, s_1, …, s_n — целые числа. Тогда в любой тройке (s_{k-2}, s_{k-1}, s_k), где $k = 2, \dots, n$, числа в совокупности взаимно просты (если некоторое простое p делит s_{k-2}, s_{k-1} и s_k, то p делит и s_{k-3}). Так же как с помощью инварианта T мы доказали, что произвольная последовательность Сомос-4 удовлетворяет рекуррентному соотношению порядка 5, для последовательности Сомос-(6) можно получить рекуррентные соотношения порядков 9, 10 и 11 соответственно:

$$s_{n+5}s_{n-4} = -s_{n+4}s_{n-3} - s_{n+3}s_{n-2} + s_{n+2}s_{n-1} + 34s_{n+1}s_n, \tag{77}$$
$$s_{n+5}s_{n-5} = s_{n+4}s_{n-4} + 15s_{n+2}s_{n-2} - 19s_{n+1}s_{n-1} + 34s_n^2, \tag{78}$$
$$s_{n+5}s_{n-6} = s_{n+3}s_{n-4} + 19s_{n+2}s_{n-3} + 34s_{n+1}s_{n-2} + 19s_ns_{n-1}. \tag{79}$$

Предположим, что числа s_0, s_1, $\ldots$, s_{n+4} — целые. Тогда из условия $(s_{n-4}, s_{n-5}, s_{n-6}) = 1$ и равенств (77)–(79) следует, что и число s_{n+4} также является целым.

Решение задачи 59. В предыдущей задаче мы доказали, что любые три соседних элемента последовательности Сомос-(6) взаимно просты в совокупности. Значит, для любого модуля вида p^γ хотя бы одно из трёх соотношений (77)–(79) позволяет находить значение $s_{n+5} \mod p^\gamma$ при условии, что известны остатки $s_{n-i} \bmod p^\gamma$, где $i = -4, -3, \ldots, 5, 6$. Так как наборы остатков повторяются, то последовательность $(s_n \mod p^\gamma)$ является периодической. Поскольку формулы (77)–(79) позволяют находить не только следующие элементы, но и предыдущие, последовательность $(s_n \bmod p^\gamma)$ является чисто периодической. Значит, она будет периодической и по произвольному модулю.

Решение задачи 60. Уравнение Сомос-7 имеет три независимых инварианта. Первый из них в однородных переменных f_k имеет вид

$$\begin{aligned}\mathcal{H}_0 =&\beta f_1f_2f_3f_4f_5 + \gamma\left(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5\right) + \alpha\beta\left(\frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} + \frac{1}{f_5}\right) + \frac{\gamma^2}{f_1f_2^2f_3^3f_4^2f_5}\\ &+ \alpha\gamma\left(\frac{1}{f_1f_2f_3} + \frac{1}{f_2f_3f_4} + \frac{1}{f_3f_4f_5}\right) + \frac{\beta^2}{f_1f_2f_3f_4f_5} + \beta\gamma\left(\frac{1}{f_1f_2f_3^2f_4^2f_5} + \frac{1}{f_1f_2^2f_3^2f_4f_5}\right),\end{aligned}$$

Для этого инварианта можно написать и второе представление

$$\begin{aligned}\mathcal{H}_0 =&\alpha\beta\left(\frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} + \frac{1}{f_5}\right) + \alpha\gamma\left(\frac{1}{f_2f_3f_4} + \frac{1}{f_3f_4f_5}\right) +\\ &+\beta\left(f_1f_2f_3f_4f_5 + f_2f_3f_4f_5f_6\right) + \gamma\left(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5 + f_4f_5f_6\right),\end{aligned}$$

из которого видно, что $\mathcal{H}_0 = F(f_1, f_2, f_3, f_4, f_5) + F(f_2, f_3, f_4, f_5, f_6)$, где

$$F(f_1, f_2, f_3, f_4, f_5) = \alpha\beta\left(\frac{1}{f_3} + \frac{1}{f_5}\right) + \frac{\alpha\gamma}{f_2f_3f_4} + \beta f_1f_2f_3f_4f_5 + \gamma\left(f_1f_2f_3 + f_3f_4f_5\right)$$

— число, не меняющееся при изменении всех индексов на 2.

Ещё два инварианта удобней записать, используя переменные $h_k = f_kf_{k+1}$:

$$\begin{aligned}\mathcal{H}_1 =&\gamma h_1h_2h_3h_4 + \alpha\beta\left(h_1h_3 + h_1h_4 + h_2h_4\right) + \alpha\gamma\left(h_1 + h_2 + h_3 + h_4 + \frac{h_1h_3}{h_4} + \frac{h_2h_4}{h_1}\right)\\ &+ \alpha^2\beta\left(\frac{1}{h_1} + \frac{1}{h_2} + \frac{1}{h_3} + \frac{1}{h_4} + \frac{h_2}{h_1h_3} + \frac{h_3}{h_2h_4}\right) + \beta\gamma\left(\frac{1}{h_1} + \frac{1}{h_2} + \frac{1}{h_3} + \frac{1}{h_4}\right)\\ &+ \alpha^2\gamma\left(\frac{1}{h_1h_2} + \frac{1}{h_2h_3} + \frac{1}{h_3h_4} + \frac{1}{h_1h_3} + \frac{1}{h_2h_4}\right) + \gamma^2\left(\frac{1}{h_1h_3} + \frac{1}{h_2h_4}\right) + \alpha\beta^2\left(\frac{1}{h_1h_2h_4} + \frac{1}{h_1h_3h_4}\right)\\ &+ \alpha\beta\gamma\left(\frac{2}{h_1h_2h_3h_4} + \frac{1}{h_1h_2^2h_4} + \frac{1}{h_1h_3^2h_4}\right) + \alpha\gamma^2\left(\frac{1}{h_1h_2^2h_3h_4} + \frac{1}{h_1h_2h_3^2h_4}\right),\\ \mathcal{H}_2 =&\gamma\left(h_1h_2h_3 + h_2h_3h_4\right) + \alpha\beta\left(h_1 + h_2 + h_3 + h_4\right) + \alpha\gamma\left(\frac{h_1}{h_4} + \frac{h_4}{h_1}\right) + \alpha^2\beta\left(\frac{1}{h_1h_3} + \frac{1}{h_2h_4}\right)\\ &+ \beta\gamma\left(\frac{1}{h_1h_2} + \frac{1}{h_2h_3} + \frac{1}{h_3h_4}\right) + \gamma\left(\alpha^2 + \gamma\right)\left(\frac{1}{h_1h_2h_3} + \frac{1}{h_2h_3h_4}\right) + \frac{\alpha\beta^2}{h_1h_2h_3h_4}\\ &+ \alpha\beta\gamma\left(\frac{1}{h_1h_2^2h_3h_4} + \frac{1}{h_1h_2h_3^2h_4}\right) + \frac{\alpha\gamma^2}{h_1h_2^2h_3^2h_4}.\end{aligned}$$

Somos sequences

I.I.Bogdanov, G.A.Golovanov, K.G.Kuyumjiyan,
A.V.Miroshnikov, A.V.Ustinov, B.R.Frenkin

Introduction

The first nontrivial example of a *Somos sequence* is a sequence Somos-4. It is given by the recurrence relation

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \tag{1}$$

where α and β are arbitrary constants. The '4' in the name of the sequence is the order of the recurrence relation (1). It shows how many initial elements of the sequence (s_n) are needed to determine all the others. For Somos-4 usually s_0, s_1, s_2 and s_3 are given.

Taking coefficients $\alpha = \beta = 1$ and initial conditions $s_0 = s_1 = s_2 = s_3 = 1$, we obtain the Somos-(4) sequence

$$s_0, s_1, \ldots = 1, 1, 1, 1, 2, 3, 7, 23, 59, 314, 1529, 8209, 83313, \ldots, \tag{2}$$

which surprisingly occurs to be integer-valued. Another its unexpected feature is periodicity modulo an arbitrary integer.

Definition 1. In general, a sequence $(s_n)_{n=-\infty}^{\infty}$ is called *a Somos-k sequence* if it satisfies a quadratic recurrence relation of k-th order ($k \geq 2$)

$$s_{n+k}s_n = \sum_{1\leq j\leq k/2} \alpha_j s_{n+k-j}s_{n+j}, \tag{3}$$

where α_j ($1 \leq j \leq k/2$) are some constants.

We assume that all elements in the sequences as well as their parameters are complex numbers. (If you wish, you usually may confine to real numbers.)

Definition 2. By *Somos-(k)* we denote the sequence Somos-k such that all parameters and initial conditions are equal to 1, and so this sequence is determined by the initial elements $s_0 = s_1 = \cdots = s_{k-1} = 1$ and the relation

$$s_{n+k}s_n = \sum_{1\leq j\leq k/2} s_{n+k-j}s_{n+j}.$$

It occurs that not only Somos-(4) but also the sequences Somos-(k) for $k = 5, 6, 7$ are integer-valued. For greater k this feature is lost. Nevertheless for each $k \geq 4$ there is a wide class of Somos-k sequences which are integer-valued.

Integer values of the elements are a clear sign that the sequence in question possesses rich arithmetical, algebraic, combinatorial, and analytic properties. For instance, integer-valuedness and periodicity of Somos-(4) form just the tip of an iceberg. They hide invariants not seen at first glance, concealed addition theorems, tropical arithmetic, perfect matchings and so on. For Somos-4 and Somos-5 the explanation consists in elliptic curves behind these sequences. Since Somos-6, the situation becomes more complicated and interesting.

The project is aimed first of all to get acquainted with the ideas behind Somos-4. Furthermore you are suggested to apply these ideas to Somos sequences of higher orders in hope for advancement in unsolved problems.

1 Getting started

The initial conditions s_0, …, s_{k-1} uniquely determine the whole sequence (s_n) if all its elements are nonzero. Otherwise some additional conditions are needed for specifying its elements.

In this project, we always assume that the sequences Somos-k contain no zeros unless otherwise indicated. For Somos-(k) this is provided by Problem 1(a).

Problem 1.
(a) The sequences Somos-(k) are correctly defined: no their elements are zero.

(b) The sequences Somos-(2) and Somos-(3) are trivial: they consist of ones only.
(c) The sequences Somos-(k), $k \geq 4$, are nontrivial: present a non-unit element.
(d) The sequences Somos-(k) are symmetric: for any positive integer n we have $s_{-n} = s_{n+k-1}$.

Problem 2. Suppose a Somos-2 sequence is given by the equation $s_{n+2}s_n = \alpha s_{n+1}^2$. Obtain a formula for its elements, which expresses s_n through α and the initial conditions s_0, s_1.

Problem 3. Suppose a Somos-3 sequence is given by the equation $s_{n+3}s_n = \alpha s_{n+2}s_{n+1}$. Express s_n through s_{-1}, s_0, s_{-1} and α.

Problem 4.
(a) Suppose $k \geq 2$, $a, b, c, q \in \mathbb{R}$, $q > 0$ and (s_n) is a Somos-k sequence. Then $(q^{an^2+bn+c}s_n)$ also is a Somos-k sequence. For $k = 4$, find the recurrence relation for the new sequence, given the relation for the initial one.
(b) Suppose $k \geq 2$ is odd, $\gamma \in \mathbb{C}$ and (s_n) is a Somos-k sequence. Then the sequences (a_n) and (b_n) of the form

$$a_n = \begin{cases} s_n, & \text{for } n \text{ even}, \\ \gamma s_n, & \text{for } n \text{ odd} \end{cases} \quad \text{and} \quad b_n = \begin{cases} \gamma s_n, & \text{for } n \text{ even}, \\ s_n, & \text{for } n \text{ odd} \end{cases}$$

are also Somos-k sequences satisfying the same recurrence relation.
(c) Suppose (s_n) is a Somos-3 sequence; then there exist Somos-2 sequences (a_n) and (b_n) such that $s_n = \begin{cases} a_n, & \text{for } n \text{ even}, \\ b_n, & \text{for } n \text{ odd}. \end{cases}$.

2 Elementary properties of Somos-4 sequences

Remind that a Somos-4 sequence is a sequence satisfying the relation

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \qquad \alpha, \beta \in \mathbb{C}. \tag{4}$$

Problem 5. Suppose a sequence (s_n) satisfies a linear recurrence equation of the second order $s_{n+2} = us_{n+1} + vs_n$, $u, v \in \mathbb{C}$. Prove that (s_n) is a Somos-4 sequence. Express the constants α and β in the equality (4) through u and v.

Problem 6. Prove that the sequence

$$s_n = (An + B)q^{an^2+bn+c} \tag{5}$$

is Somos-4. Express the constants α and β in (4) through A, B, a, b, c, q.

Problem 7. Prove that the Somos-(4) sequence is not a sequence of the form (5).

Problem 8. For the sequences (n^2), (2^{n^3}) determine whether they are (a) Somos-4, (b) Somos-6.

Problem 9*. Let (s_n) be a Somos-4 sequence subject to (4) for $\alpha = \beta = 1$. Suppose $s_0 = 0$, $s_1 = s_2 = s_4 = 1$, $s_3 = -1$. (It is natural to complete this sequence for negative indices by oddness: $s_{-n} = -s_n$.) Then the sequence is uniquely determined and its elements with odd indices form the alternating Somos-(4) sequence. [1]

3 Somos-(4)

Problem 10. Suppose in the Somos-(4) sequence the elements $s_0, \ldots, s_n$ are integer. Then in any four-tuple of consecutive elements $(s_{k-3}, s_{k-2}, s_{k-1}, s_k)$, where $3 \leq k \leq n$, any two numbers are coprime.

Problem 11.
(a) Suppose in the Somos-(4) sequence the elements $s_{n-3} = a$, $s_{n-2} = b$, $s_{n-1} = c$, and s_n are integer. Using Problem 10, express the values of s_{n+1}, s_{n+2}, s_{n+3} modulo s_n.
(b) Prove that all elements in the Somos-(4) sequence are integer.

[1] If this problem seems difficult to you, you may postpone solving it up to obtaining more information about Somos-4 sequences.

Remark. The Somos-(5), Somos-(6) and Somos-(7) sequences also consist of integers. This is not the case for Somos-(k) sequences with $k \geq 8$. For instance, the beginning of Somos-(8) looks as follows:

$$\ldots, 1, 1, 1, 1, 1, 1, 1, 1, 4, 7, 13, 25, 61, 187, 775, 5827, 14815, \frac{420514}{7}, \ldots$$

In the project we consider various approaches to the proof of integer-valuedness of Somos-(4) and Somos-(5). In the sequel they will be useful for the case of Somos sequences of higher orders.

Problem 12. A sequence $a_1, a_2, a_3, \ldots$ is given by the initial conditions $a_1 = 1, a_2 = 1$ and the recurrence relation

$$a_n = \frac{a_{n-1}^2 + 2}{a_{n-2}} \qquad (n \geq 3).$$

Prove that all elements of the sequence are integer.

4 A hidden invariant of a Somos-4 sequence

As we see from Problem 4(a), a Somos-k sequence satisfies the same equation after certain substitutions. This often can be used to decrease the order of the recurrence relation.

Specifically, let (s_n) be a Somos-k sequence. The corresponding *homogeneous sequence* (f_n) will be given by

$$f_n = \frac{s_{n-1}s_{n+1}}{s_n^2}.$$

Observe that the change $(s_n) \mapsto (q^{bn+c}s_n)$ does not affect the homogeneous sequence.

Problem 13.
(a) Let (s_n) be a Somos-4 sequence. Find a recurrence relation of order 2 for the homogeneous sequence (f_n).
(b) Let (s_n) be a Somos-5 sequence. Find a recurrence relation of order 3 for the homogeneous sequence (f_n).

Problem 14. Let (s_n) be a Somos-4 sequence with the corresponding homogeneous sequence (f_n).
(a) Prove that the value of

$$T_n = f_{n-1}f_n + f_nf_{n+1} + \frac{\alpha}{f_n} \tag{6}$$

is independent of n.
(b) Find the expression $T(x, y)$ such that $T_n = T(f_n, f_{n+1})$.

Remark. To curious participants, we recommend to think about a way to *invent* the expression (6)! This will be of use in the sequel.

We see that for a given (s_n) all the expressions of the form $T(f_n, f_{n+1})$ take the same value .

Definition 3. The above value of T is called *the invariant* of the given Somos-4 sequence.

Problem 15. Let (s_n) be a Somos-4 sequence subject to relation (4); let T be its invariant. Prove that (s_n) is Somos-5 as well, so it satisfies an equation

$$s_{n+3}s_{n-2} = \mu s_{n+2}s_{n-1} + \nu s_{n+1}s_n$$

for some constants μ and ν. Express these constants through α, β and T.

Remark. A more general fact holds: any Somos-4 sequence is a Somos-k sequence, $k \geq 4$. The proof of this fact will be a subject of a specific section.

Problem 16. Using Problem 14 (and Problem 10), obtain one more proof that all elements of the Somos-(4) sequence are integer.

Problem 17. Using Problem 15 (and Problem 10), obtain yet another proof that all elements of Somos-(4) sequence are integer.

Problem 18. (a) For which Somos-4 sequences their integervaluedness can be proved using the same ideas as in Problems 16 and 17?

(b) Try to derive a criterion of integer-valuedness of a Somos-4 sequence.

Problem 19*. Let (s_n) be a Somos-4 sequence. Prove that the subsequences of its elements with even and odd indices (s_{2n}) and (s_{2n+1}) are Somos-4 as well.

5 Periodicity of a Somos-4 sequence modulo an arbitrary integer

Problem 20. Prove that Somos-(4) contains no multiples of 5.

Definition 4. Let us call a sequence (s_n) *primitive* if all its elements are integers coprime in total (there is no divisor common for all of them and greater than 1).

Problem 21. (a) Suppose p is a prime, and (s_n) is a primitive Somos-4 sequence satisfying the recurrence relation (4) with integer coefficients such that $(\alpha\beta, p) = 1$. Then in this sequence there exist three consecutive elements coprime with p.
(b) Under the conditions of part (a) the sequence (s_n) has a correctly defined invariant $T \pmod{p^\gamma}$, $\gamma \in \mathbb{N}$.

Problem 22. Suppose p is a prime, $\gamma \in \mathbb{N}$ and (s_n) is a primitive Somos-4 sequence subject to the recurrence relation (4) with integer coefficients such that $(\alpha\beta, p) = 1$.. Then the sequence of the remainders of the elements from (s_n) modulo p^γ is periodical.

Problem 23. (a) Let $m = p_1^{\gamma_1} \dots p_l^{\gamma_l}$ be the canonical factorization of an integer m into primes. The sequence (a_n) is periodical modulo each $p_i^{\gamma_i}$, $1 \le i \le l$. Prove that (a_n) is periodical modulo m as well.
(b) Suppose $m \in \mathbb{N}$, and (s_n) is a primitive Somos-4 sequence subject to the recurrence relation (4) with integer coefficients such that $(\alpha\beta, m) = 1$. Then the remainders of elements of (s_n) modulo m form a periodical sequence.
(c) The remainders of elements of Somos-(4) modulo an arbitrary positive integer m form a periodical sequence.

Problem 24. Prove that in Problem 22 the condition $(\alpha\beta, p) = 1$ cannot be removed.

6 Somos-5 sequences

Problem 25. Suppose in the sequence Somos-(5) the elements $s_0, \dots, s_n$ are integer. Then any five consecutive elements $s_{k-4}, s_{k-3}, s_{k-2}, s_{k-1}, s_k$, where $4 \le k \le n$, are pairwise coprime.

Suppose (s_n) is a Somos-5 sequence subject to the recurrence relation

$$s_{n+3}s_{n-2} = \mu s_{n+2}s_{n-1} + \nu s_{n+1}s_n. \tag{7}$$

Denote the respective homogeneous sequence by (f_n) as above.

The following two problems are devoted to the search of two *independent* invariants of Somos-(5), analogous to the invariant T of a Somos-4 sequence.

Problem 26. (a) Show that in the resulting equation of Problem 13(b) one more change of variables is possible such that the order of the equation is decreased (and the equation is simplified).
(b) Find an expression of the form $J_n = J_n(f_{n-1}, f_n, f_{n+1}, f_{n+2})$ with the same features as T_n in Problem 14a. In other words, the value of J_n is to be constant on any homogeneous sequence (f_n) but these values must not be equal for *all* sequences subject to the given relation (7).
(c) Find a nontrivial function $J(x, y, z)$ which is an invariant of a given homogeneous sequence (that is, the value of $J = J(f_n, f_{n+1}, f_{n+2})$ is independent of n).

Problem 27. (a) Express the relation for (f_n) in another way to find an essentially different *almost invariant*: an expression $K(x, y, z)$ such that the values of $K(f_{n-1}, f_n, f_{n+1})$ are equal for all *even* n.
(b) Find one more (essentially different from that in in Problem 26!) expression of the form
$I_n = I_n(f_{n-1}, f_n, f_{n+1}, f_{n+2})$ with the same features as the expression from Problem 26b,
(c) ... and use it to obtain one more invariant $I(x, y, z)$ of the sequence (f_n).

Remark. If you don't understand the condition of two above problems, please apply for explanation!

Problem 28. Using each one of Problems 26, 27 prove that all elements of Somos-(5) are integer.

Problem 29. Suppose m is a positive integer, and (s_n) is the Somos-(5) sequence. Using invariants from Problems 26, 27 prove that the remainders of the elements from (s_n) modulo m form a periodical sequence.

Problem 30*. Suppose a sequence (s_n) is subject to the recurrence relation (7). Prove that each of the subsequences $(s_n^*) = (s_{2n})$ and $(s_n^*) = (s_{2n+1})$ consisting of elements with even and odd indices respectively, satisfies the Somos-4 equation

$$s_{n+2}^* s_{n-2}^* = \alpha^* s_{n+1}^* s_{n-1}^* + \beta^* (s_n^*)^2.$$

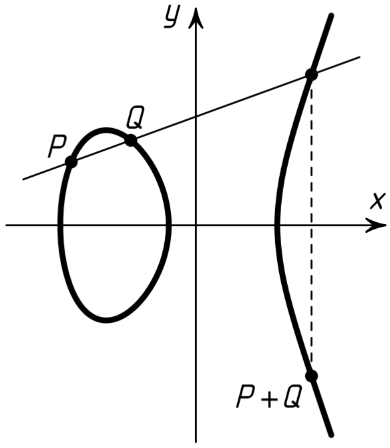
What are the expressions for α^* and β^*?

Problem 31*. Let (s_n) be a Somos-5 sequence subject to (7). Find the conditions on the values of its invariants I and J, equivalent to the fact that (s_n) is a Somos-4 sequence.

Problem 32. Prove that multiplying the elements with even indices from a Somos-5 sequence by some complex number, we can obtain a Somos-4 sequence.

7 Connection with elliptic curves

In this project an elliptic curve is understood as a curve in the plane determined by an equation of the form $y^2 = x^3 + ax + b$ under the restriction $4a^3 + 27b^2 \neq 0$. First of all we are interested in rational points (that is, points with rational coordinates) of such curves. However the main feature (first of all, existence of a group structure on the curve) are valid for all points with real or complex cooerdinates as well.



In general, a line meets an elliptic curve at three points. Let us assume that the sum of these three points is zero. The strict formulation is as follows.

Definition 5. Consider two points P and Q on an elliptic curve, not mutually symmetrical about the OX-axis. Define the sum $P+Q$ as follows: draw a line through P and Q, consider the third point R' of meet of this line with the elliptic curve, and reflect R' about the OX-axis (observe that our curve is symmetrical about OX-axis). The resulting point R is considered as the sum of the original points, notation: $R = P+Q$.

Problem 33. Prove that the definition is correct, and write down the coordinates of R. Prove that $P + Q = Q + P$.

Let us add one more point, the infinite point, to our elliptic curve. We assume that it is the point of meet of all vertical lines.

Problem 34. What is the sum of a finite and the infinite point? In what case the sum of finite points of an elliptic curve is the infinite point?

Problem 35*. Consider two triples ℓ_1, ℓ_2, ℓ_3 and m_1, m_2, m_3 of lines in the plane. Prove that if they have nine distinct points of meet and eight of these belong to an elliptic curve E then the ninth point of meet belongs to E as well.

In the sequel, the result of Problem 35 may be used without a proof.

Problem 36*. Check the identity $(P+Q)+R = P+(Q+R)$ for points of an elliptic curve (associativity of addition).

Problem 37. Suppose the coefficients a, b are rational. If the coordinates of P and Q are rational then the coordinates of $P+Q$ are rational as well.

A remark for those acquainted with the notion of group: we have just proved that the points of an elliptic curve form an Abelian group under addition, and the rational points form a subgroup in this group.

Problem 38. What is the definition for $P+P$? Write down the formulas for its coordinates. What is the definition for $3P$, $4P$?

Now suppose (s_n) is a Somos-4 sequence, and (f_n) is the corresponding homogeneous sequence. The invariant T informs that the points of the form (f_n, f_{n+1}) lie on a curve of the fourth order

$$X^2Y^2 + \alpha(X+Y) + \beta - TXY = 0. \tag{8}$$

It occurs that the order of this equation can be decreased.

Problem 39.
(a) In (8) change the variables: $x = -4\alpha X$. $y = 4\alpha(TX - \alpha - 2X^2Y)$. What is the resulting equation?
(b) Reduce the above equation to the standard equation of an elliptic curve.

Problem 40.
(a) Consider the sequence defined in Problem 9 and the corresponding homogeneous sequence (f_n) (what is f_0?). Suppose P_n is the corresponding sequence of points on the cubic curve constructed in the previous problem. Prove that $P_n = nP_1$.
(b) Solve Problem 9.

Problem 41.
(a) Prove that the sequence of points corresponding to an arbitrary Somos-4 is an arithmetical progression, that is, $P_n = P_{n-1} + P$, where P is a constant point.
(b) What does it mean that the resulting progression is of the form (nP)?

Suppose there is an elliptic curve E determined by the equation $y^2 = x^3 + ax + b$ and a point $P = (x, y)$ on it. It occurs that the coordinates of several initial points of the form nP are of special form. There is always a polynomial $\psi_n = \psi_n(x, y) \in \mathbb{Z}[x, y, a, b]$ such that $nP = \left(\frac{\cdots}{\psi_n^2}, \frac{\cdots}{\psi_n^3}\right)$. Here is the beginning of this sequence:

$$\begin{gathered}\psi_0 = 0, \quad \psi_1 = 1, \quad \psi_2 = 2y, \quad \psi_3 = 3x^4 + 6ax^2 + 12bx - a^2, \\ \psi_4 = 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - 8b^2 - a^3).\end{gathered} \tag{9}$$

Furthermore it occurs that the values of $\psi_5, \psi_6, \ldots$ can be determined using the recurrence relation

$$\psi_1^2\psi_{n+2}\psi_{n-2} = \psi_2^2\psi_{n+1}\psi_{n-1} - \psi_1\psi_3\psi_n^2 \qquad (n \geq 3)$$

or the pair of relations

$$\begin{aligned}\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3 \qquad (n \geq 2), \\ \psi_{2n} &= \frac{\psi_n}{2y}\left(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2\right) \qquad (n \geq 3).\end{aligned}$$

The polynomials $\psi_n(x, y)$ related to an elliptic curve E are called *division polynomials*. For a chosen curve with a chosen point on it the sequence $\psi_n(x, y)$ becomes a sequence of numbers.

Problem 42. Check that to the elliptic curve $y^2 = x^3 - x + \frac{1}{4}$ and the point $P = (0, \frac{1}{2})$ there corresponds the sequence

$$\psi_0, \psi_1, \ldots = 0, \mathbf{1}, 1, -\mathbf{1}, 1, \mathbf{2}, -1, -\mathbf{3}, -5, \mathbf{7}, -4, -\mathbf{23}, 29, \mathbf{59}, 129, \ldots, \tag{10}$$

determined by the initial conditions $\psi_1 = \psi_2 = 1$, $\psi_3 = -1$, $\psi_4 = 1$ and the recurrence relation

$$\psi_{n+2}\psi_{n-2} = \psi_{n+1}\psi_{n-1} + \psi_n^2 \qquad (n \geq 3).$$

Prove that in terms of the variables $f_n = \psi_{n+1}\psi_{n-1}/\psi_n^2$ the coordinates of a point nP for $n \geq 2$ have the form

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1})\right).$$

Problem 43. Prove that for an arbitrary curve $y^2 = x^3 + ax + b$ and a point $P = (x, y)$ on it, the coordinates of nP for $n \geq 2$ are of the form

$$nP = \left(\frac{\varphi_n}{\psi_n^2}, \frac{\omega_n}{\psi_n^3}\right) = \left(x - f_n, \frac{f_n^2}{4y}(f_{n+1} - f_{n-1})\right),$$

where $\varphi_n = x\psi_n^2 - \psi_{n-1}\psi_{n+1}$, $\omega_n = \frac{1}{4y}(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)$.

To this end establish that the sequence (ψ_n) has the invariant $T = 2(a+3x^2)$, and the slope of the secant through nP and P equals $k_n = -\frac{1}{4y}(2f_nf_{n+1} - T)$.

8 Somos-4 is Somos-m

One of features of low-order Somos sequences is that they satisfy recurrence relations of higher orders.

Problem 44. Prove that an arbitrary Somos-2 sequence is Somos-m for every $m \geq 3$.

Problem 45. Prove that an arbitrary Somos-3 sequence is Somos-m for every $m \geq 4$.

A similar fact holds for an arbitrary Somos-4 sequence: it is Somos-m for every $m \geq 5$. Moreover a stronger assertion holds: there exist sequences $(c_k)_{k=1}^{\infty}$ and $(d_k)_{k=1}^{\infty}$ such that

$$s_{n+k}s_{n-k} = c_k s_{n+1}s_{n-1} - d_k s_n^2, \tag{11}$$

and sequences $(u_k)_{k=-\infty}^{\infty}$ and $(v_k)_{k=-\infty}^{\infty}$ such that

$$s_{n+k+1}s_{n-k} = u_k s_{n+2}s_{n-1} - v_k s_n s_{n+1}. \tag{12}$$

The subsequent problems are devoted to the proof of this fact and its consequences.

Problem 46. For $k \geq 2$ find the formulas for calculation of the coefficients c_{k+1}, d_{k+1} through c_{k-1}, d_{k-1}, c_k, d_k.

Problem 47. Find the values of c_k, d_k for $k = 1, 2, 3$.

Problem 48. Write down the relation between parameters c_{k-1}, d_{k-1}, c_k, d_k which provides for $k \geq 3$ that the values c_{k+1}, d_{k+1} can be determined using the recurrence formulas from Problem 46. Prove that this relation really holds.

Problem 49. Prove that in fact the formula (11) can be written in the form

$$w_1^2 s_{n+k}s_{n-k} = w_k^2 s_{n+1}s_{n-1} - w_{k+1}w_{k-1}s_n^2, \tag{13}$$

where (w_n) is a Somos-4 sequence. What initial values for this sequence are the most suitable?

Problem 50. Prove that the elements of the sequence (w_n) from the above problem satisfy the equation

$$w_1^2 w_{n+k}w_{n-k} = w_k^2 w_{n+1}w_{n-1} - w_{k+1}w_{k-1}w_n^2. \tag{14}$$

Problem 51. For $k \geq 2$ find formulas which provide determination of the coefficients u_{k+1}, v_{k+1} of the recurrence relation (12) through u_{k-1}, v_{k-1}, u_k, v_k.

Problem 52. Write down the relation between parameters u_{k-1}, v_{k-1}, u_k, v_k which provides for $k \geq 3$ that the values u_{k+1}, v_{k+1} can be determined using the recurrence formulas from Problem 51. Prove that this relation really holds.

Problem 53. Express u_k, v_k through elements of the sequence (w_n) from Problem 49.

Problem 54. Suppose the numbers k, l, m, n are either all integer or all semi-integer. Prove that

$$s_{k+l}s_{m+n}w_{k-l}w_{m-n} + s_{k+n}s_{l+m}w_{k-n}w_{l-m} - s_{k+m}s_{l+n}w_{k-m}w_{l-n} = 0. \tag{15}$$

In particular,

$$w_{k+l}w_{m+n}w_{k-l}w_{m-n} + w_{k+n}w_{l+m}w_{k-n}w_{l-m} - w_{k+m}w_{l+n}w_{k-m}w_{l-n} = 0. \tag{16}$$

Problem 55. Using the formulas of the preceding problem, give another solution for Problem 9: prove that the elements of (10) are relted to the elements of Somos-(4) by the equation $s_n = (-1)^n \psi_{2n-3}$ (boldface in (10)).

Problem 56. Let a sequence (s_n) be Somos-4. Prove that for any a and b the sequence $(\tau_n) = (s_{an+b})$ is Somos-4 as well.

9 Difficult problems

Problem 57*. Determine the invariants of a Somos-6 sequence satisfying the equation

$$s_{n+3}s_{n-3} = \alpha s_{n+2}s_{n-2} + \beta s_{n+1}s_{n-1} + \gamma s_n^2, \qquad \alpha, \beta, \gamma \in \mathbb{C}. \tag{17}$$

Problem 58*. Prove that Somos-(6) consists of integers.

Problem 59*. Prove that the sequence Somos-(6) modulo an arbitrary positive integer is preiodical.

Problem 60*. Determine the invariants of a Somos-7 sequence satisfying the equation

$$s_{n+4}s_{n-3} = \alpha s_{n+3}s_{n-2} + \beta s_{n+2}s_{n-1} + \gamma s_{n+1}s_n, \qquad \alpha, \beta, \gamma \in \mathbb{C}. \tag{18}$$

10 Unsolved problems

Problem 61*. For a Somos-6 sequence prove the «addition theorem» similar to the formula (13).

Problem 62*. For a Somos-7 sequence prove the «addition theorem» similar to the formula (13).

Problem 63*. Is it possible to multiply a constant by the elements with odd indices in a Somos-7 sequence so that the resulting sequence is Somos-6?

Problem 64*. Prove that Somos-(7) modulo an arbitrary positive integer is periodical.

Problem 65*. Prove that Somos-(8) is not a Somos-k sequence for $k \neq 8$.

Problem 66*. It is not hrd to see that the Somos-k sequences for $k = 4, 5, 6, 7$ are particular cases of *Gale — Robinson sequences* determined by recurrence relations of two types: a two-term relation

$$s_n s_{n-k} = \alpha s_{n-l}s_{n-k+l} + \beta s_{n-m}s_{n-k+m},$$

where $0 < l < m < k$, or a three-term relation

$$s_n s_{n-k} = \alpha s_{n-p}s_{n-k+p} + \beta s_{n-q}s_{n-k+q} + \gamma s_{n-r}s_{n-k+r},$$

where $0 < p < q < r < k$ and $p + q + r = k$. Find an approach to such sequences, which enables us to determine their invariants, to prove periodicity or addition theorems, ...

Solutions

Getting started

Solution 1. All asertions are proved by induction.
It is suitable to begin with part (d). The base of induction $n = 0$ is valid by condition. Suppose that for $m < n$ we have $s_{-m} = s_{m+k-1}$. Then the recurrence formula implies

$$s_{-n} = \frac{1}{s_{k-n}} \sum_{1 \le j \le k/2} s_{-n+k-j}s_{-n+j} = \frac{1}{s_{n-1}} \sum_{1 \le j \le k/2} s_{n+j-1}s_{n-j+k-1} = s_{n+k-1}.$$

Now in view of part (d) we may consider the assertions about Somos-(k) sequence for positive integers only. Part (a) is true since the numerator is strictly positive.

Part (b) is proved by induction. The base is valid by condition. The induction step: $s_{n+2} = \frac{s_{n+1}^2}{s_n} = \frac{1}{1} = 1$ for Somos-2 and $s_{n+3} = \frac{s_{n+2}s_{n+1}}{s_n} = \frac{1}{1} = 1$ for Somos-3.
For part (c), it suffices to consider the element $s_k = [k/2]$.

Solution 2. The formula is

$$s_n = \alpha^{n(n-1)/2} s_0^{1-n} s_1^n. \tag{19}$$

We prove it by induction. It fits for $n = 0$ and $n = 1$. Suppose it is valid for $n = k - 1$ and $n = k$ ($k \geq 1$). Then for s_{k+1} the recurrence relation gives the required representation:

$$s_{k+1} = \alpha s_k^2 s_{k-1}^{-1} = \alpha \cdot \alpha^{k(k-1)} s_0^{2(1-k)} s_1^{2k} \alpha^{-(k-1)(k-2)/2} s_0^{2k} s_1^{1-k} = \alpha^{k(k+1)/2} s_0^{-k} s_1^{k+1}.$$

Solution 3. The formula is

$$s_n = \begin{cases} \alpha^{n^2/4} s_{-1}^{-n/2} s_0 s_1^{n/2}, & \text{for } n \text{ even;} \\ \alpha^{(n^2-1)/4} s_{-1}^{(1-n)/2} s_1^{(n+1)/2}, & \text{for } n \text{ odd.} \end{cases}$$

The proof is similar, by induction.

Solution 4.
(a) It suffices to prove separately the following: if the elements of (s_n) are multiplied by $q \in \mathbb{C}$, q^n or q^{n^2}, then it remains a Somos-k sequence.
For (qs_n) we have to check the equality

$$(qs_{n+k})(qs_n) = \sum_{1 \leq j \leq k/2} \alpha_j (qs_{n+k-j})(qs_{n+j}), \quad \text{or} \quad q^2 s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \alpha_j q^2 s_{n+k-j} s_{n+j}.$$

It is obtained from the original one by multiplication by q^2.
For $(q^n s_n)$ the required equality has the form

$$(q^{n+k} s_{n+k})(q^n s_n) = \sum_{1 \leq j \leq k/2} \alpha_j (q^{n+k-j} s_{n+k-j})(q^{n+j} s_{n+j}), \quad \text{or} \quad q^{2n+k} s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \alpha_j q^{2n+k} s_{n+k-j} s_{n+j}.$$

It is obtained from the original one by multiplication by q^{2n+k}.
For $(q^{n^2} s_n)$ the equation changes. We wish to obtain an equality of the form

$$(q^{(n+k)^2} s_{n+k})(q^{n^2} s_n) = \sum_{1 \leq j \leq k/2} \beta_j (q^{(n+k-j)^2} s_{n+k-j})(q^{(n+j)^2} s_{n+j}),$$

which can be transformed to

$$s_{n+k} s_n = \sum_{1 \leq j \leq k/2} \left(\beta_j q^{2j^2 - 2kj} \right) s_{n+k-j} s_{n+j}.$$

Thus it suffices to choose $\beta_j = \alpha_j q^{2kj - 2j^2}$.
(b) Observe that if k is odd then for any integer j the integers $n + k - j$ and $n + j$ are of different parity. Hence $a_{n+k-j} a_{n+j} = b_{n+k-j} b_{n+j} = \gamma s_{n+k-j} s_{n+j}$, and we can cancel $\gamma \neq 0$ in every summand of the recurrence relation.
(c) The result of Problem 3 implies that for even n we should have $a_n = \alpha^{n^2/4} s_{-1}^{-n/2} s_0 s_1^{n/2}$; now the result of Problem 2 rather easily implies that a sequence of the form

$$a_n = (\alpha^{1/2})^{n(n-1)/2} (\alpha^{1/4} (s_1/s_{-1})^{1/2})^n s_0$$

does fit if for instance $\alpha^{1/4}$ denotes a complex number β such that $\beta^4 = \alpha$. The resulting sequence satisfies the relation $a_{n+2} a_n = \alpha^{1/2} a_{n+1}^2$.
The sequence (b_n) is constructed similarly and satisfies the same relation.

Elementary properties of Somos-4 sequences

Solution 5. Suppose $v \neq 0$. If $s_{n+2} = us_{n+1} + vs_n$ then $s_{n-2} = -\frac{u}{v}s_{n-1} + \frac{1}{v}s_n$. Thus

$$s_{n+2}s_{n-2} = (us_{n+1} + vs_n)\left(-\frac{u}{v}s_{n-1} + \frac{1}{v}s_n\right) =$$
$$= s_n^2 - \frac{u^2}{v}s_{n-1}s_{n+1} + s_n\left(\frac{u}{v}s_{n+1} - us_{n-1}\right) = s_n^2\left(1 + \frac{u^2}{v}\right) - \frac{u^2}{v}s_{n-1}s_{n+1}.$$

Hence $\alpha = -u^2/v$ and $\beta = 1 + u^2/v$.
The case $v = 0$ gives the recurrence formula $s_n = us_{n-1}$, whence $s_n = u^n s_0$. Then $s_{n+2}s_{n-2} = u^{2n}s_0^2 = s_n^2 = s_{n+1}s_{n-1}$. Thus s_n is a Somos-4 sequence for any α, β such that $\alpha + \beta = 1$.

Solution 6. Substitution $s_n = (An + B)q^{an^2+bn+c}$ in (1) leads to the equality

$$(A^2(n^2 - 4) + 2ABn + B^2)q^{8a} = \alpha(A^2(n^2 - 1) + 2ABn + B^2)q^{2a} + \beta(A^2n^2 + 2ABn + B^2),$$

which is to be valid for all integer n. This means that the coefficients at any power of n are to be equal in both parts of the equality. Comparison of the coefficients at n^2 and at n^0 leads to the system of equaions

$$q^{8a} = \alpha q^{2a} + \beta, \qquad (-4A^2 + B^2)q^{8a} = \alpha(-A^2 + B^2)q^{2a} + \beta B^2.$$

The equality of coefficients at n^1 also reduces to the first equation. The system has the unique solution $\alpha = 4q^{6a}$, $\beta = -3q^{8a}$.

Solution 7. If Somos-(4) is of the form $s_n = (An + B)q^{an^2+bn+c}$ then according to Problem 6 we have equalities $q^{6a} = 1/4$, $q^{8a} = -1/3$. But these two equalities are incompatible since otherwise it would be $4^{-4} = q^{24a} = -3^{-3}$.

Solution 8. On one hand, if $s_n = n^2$ is a Somos-4 sequence then for some α, β and all integer n we must have

$$n^4 - 8n^2 + 16 = \alpha(n^4 - 2n^2 + 1) + \beta n^4.$$

Comparison of coefficients at various powers of n leads to an inconsistent system of equations for α and β. Hence $s_n = n^2$ is not Somos-4. On the other hand, it is Somos-6 since there exist coefficients α, β, γ such that for all integer n we have

$$n^4 - 18n^2 + 81 = \alpha(n^4 - 8n^2 + 16) + \beta(n^4 - 2n^2 + 1) + \gamma n^4.$$

Comparison of coefficients at various powers of n leads to the system

$$1 + \alpha + \beta + \gamma, \quad -18 = -8\alpha - 2\beta, \quad 81 = 16\alpha + \beta$$

with the single solution of the form $(\alpha, \beta, \gamma) = (6, -15, 10)$.

Substitution $s_n = 2^{n^3}$ in the equation (1) leads to the equality $2^{24n} = \alpha 2^{6n} + \beta$. This equality cannot hold for all integer n since the left side grows faster than the right side when $n \to \infty$. Similarly we check that the sequence $s_n = 2^{n^3}$ cannot be Somos-k for all $k \geq 2$. In particular, this sequence cannot be Somos-6.

Solution 9. See the solutions of Problems 30, 40 and 55 below.

Somos-(4)

Solution 10. Let us use induction. For $n = 0$ we have the four $(s_0, s_1, s_2, s_3) = (1, 1, 1, 1)$ whose elements are pairwise coprime. Suppose $(s_{n+3}, s_{n+2}, s_{n+1}, s_n)$ are the first four elements such that some of them aren't coprime. Then there exists a prime p which divides s_{n+3} and some of s_{n+2}, s_{n+1}, s_n. The recurrence relation $s_{n+3}s_{n-1} = s_{n+2}s_n + s_{n+1}^2$ implies that if $p \mid s_{n+2}$ or $p \mid s_n$ then $p \mid s_{n+1}$. If $p \mid s_{n+1}$ then $p \mid s_{n+2}s_n$. In any case $p \mid (s_n, s_{n+2}s_{n+1})$, which contradicts the assumption.

Solution 11.
(a) In our notation, $s_{n-3} = a$, $s_{n-2} = b$, $s_{n-1} = c$. Then $s_n s_{n-4} = ac + b^2$, and s_n divides $ac + b^2$. According to Problem 10, we have $(abc, s_n) = 1$. Thus we may repeatedly apply the recurrence relation $s_{k+1}s_{k-3} = s_k s_{k-2} + s_{k-1}^2$ modulo s_n for $k = n,\ n+1,\ n+2$:

$$\begin{gathered}
s_{n+1}a = s_n b + c^2 \equiv c^2 \pmod{s_n}, \text{that is, } s_{n+1} \equiv c^2 a^{-1} \pmod{s_n};\\
s_{n+2}b = s_{n+1}c + s_n^2 \equiv s_{n+1}c \pmod{s_n}, \text{ that is, } s_{n+2} \equiv c^3 a^{-1} b^{-1} \pmod{s_n};\\
s_{n+3}c = s_{n+2}s_n + s_{n+1}^2 \equiv s_{n+1}^2 \pmod{s_n}, \text{that is, } s_{n+3} \equiv c^3 a^{-2} \pmod{s_n}.
\end{gathered}$$

Here we always assume that the inverse element [2] is determined modulo s_n.
(b) Let us check that if $s_{n-4}, \ldots, s_n, \ldots, s_{n+3}$ are integer (obviously this is true for $n = 4$) then s_{n+4} is integer as well. By induction we obtain that all s_n are integer.
In view of the above formulas, our segment of the sequence modulo s_n looks like

$$a, \quad b, \quad c, \quad 0, \quad c^2 a^{-1}, \quad c^3 a^{-1} b^{-1}, \quad c^3 a^{-2}.$$

The next element s_{n+4} is to be determined from the equality $s_n s_{n+4} = s_{n+1}s_{n+3} + s_{n+2}^2$. But now we can check divisibility of the right side by s_n, replacing the integers by their residues modulo s_n:

$$s_{n+1}s_{n+3} + s_{n+2}^2 \equiv c^5(ac + b^2)a^{-3}b^{-2} \equiv 0 \pmod{s_n}.$$

Thus s_n divides $s_{n+1}s_{n+3} + s_{n+2}^2$, and s_{n+4} is integer.

Solution 12. By induction, we shall prove that all a_n are integer. Suppose $n \geq 3$ and $a_1, a_2, \ldots, a_n$ are integer. Let us check that a_{n+1} is integer.

The initial conditions and the recurrence relation imply that all integers $a_1, a_2, \ldots, a_n$ are odd. This in turn implies that for $k = 2, \ldots, n-1$ the integers a_{k-1} and a_k are coprime. (If not, and k is the minimal number such that $d = (a_{k-1}, a_k) > 1$, then the equality $a_{k-1}a_{k+1} = a_k^2 + 2$ implies $d = 2$. But this is impossible since d is odd.)

The value of a_{n+1} is determined from $a_{n+1}a_{n-1} = a_n^2 + 2$, and a_{n+1} surely is integer if $a_n^2 + 2 \equiv 0 \pmod{a_{n-1}}$. The recurrence relation implies

$$a_n^2 + 2 = \left(\frac{a_{n-1}^2 + 2}{a_{n-2}}\right)^2 + 2 = \frac{a_{n-1}^2(a_{n-1}^2 + 4) + 2a_{n-1}a_{n+1}}{a_{n-2}^2}.$$

Since $(a_{n-1}, a_{n-2}) = 1$, after cancelling the numerator and the denominator by a_{n-2}^2 the numerator still is a multiple of a_{n-1}, hence $(a_n^2 + 2)/a_{n-1}$ is integer.

The hidden invariant of a Somos-4 sequence

Solution 13. (a) $f_{n-1}f_n^2 f_{n+1} = \alpha f_n + \beta$, (б) $f_{n-1}f_n^2 f_{n+1}^2 f_{n+2} = \mu f_n f_{n+1} + \nu$.

Solution 14.
(a) Rewrite the relations from Problem 13(a) in two forms:

$$f_n f_{n+1} = \frac{\alpha}{f_{n-1}} + \frac{\beta}{f_{n-1}f_n} \quad \text{and} \quad f_{n-2}f_{n-1} = \frac{\alpha}{f_n} + \frac{\beta}{f_{n-1}f_n} \tag{20}$$

(in the second case we shift the index by 1). Subtracting one equality from the other one, we get

$$f_n f_{n+1} + \frac{\alpha}{f_n} = f_{n-2}f_{n-1} + \frac{\alpha}{f_{n-1}}.$$

Adding $f_{n-1}f_n$ to both sides, we get $T_n = T_{n-1}$ as required.
(b) Express $f_{n-1}f_n$ through f_n and f_{n+1} to see that the function

$$T(x, y) = xy + \alpha\left(\frac{1}{x} + \frac{1}{y}\right) + \frac{\beta}{xy}$$

[2]The integer inverse to a modulo m is the integer a^{-1} such that $aa^{-1} \equiv 1 \pmod{m}$. The inverse element exists iff $(a, m) = 1$. In the sequel, in all congruences the inverse elements are considered just in this case.

does fit.

Solution 15. Let us pass to the homogeneous sequence (f_n). By Problem 13(b) the equation (7) takes the form

$$f_{n+2}f_{n+1}^2 f_n^2 f_{n-1} = \mu f_n f_{n+1} + \nu.$$

Let us try to choose coefficients μ and ν such that the equation does hold. The recurrence relation 13(a) implies

$$f_{n+2}f_{n+1}f_n = \alpha + \frac{\beta}{f_{n+1}}, \qquad f_{n+1}f_n f_{n-1} = \alpha + \frac{\beta}{f_n}.$$

Multiplying one equality by the other one, we see that μ and ν must satisfy for any n the relation

$$\left(\alpha + \frac{\beta}{f_{n+1}}\right)\left(\alpha + \frac{\beta}{f_n}\right) = \mu f_n f_{n+1} + \nu,$$

which is equivalent to

$$\nu - \alpha^2 = -\mu f_n f_{n+1} + \alpha\beta\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) + \frac{\beta^2}{f_n f_{n+1}}. \tag{21}$$

The right side occurs to be similar to the formula (6) for the invariant T. In view of this formula we see that μ and ν must satisfy the relation

$$\nu - \alpha^2 = \beta T - (\beta + \mu) f_n f_{n+1}.$$

Since the product $f_n f_{n+1}$ is not a constant, the last equality implies $\mu = -\beta$. Now we find that $\nu = \alpha^2 + \beta T$. The necessary conditions for μ and ν just obtained are also sufficient to provide the formula (21) equivalent to (7).

Solution 16. Rewrite the expression (6) in terms of the sequence (s_n) to obtain

$$T = \frac{s_{n-2}s_{n+1}}{s_{n-1}s_n} + \frac{s_{n-1}s_{n+2}}{s_n s_{n+1}} + \frac{\alpha s_n^2}{s_{n-1}s_{n+1}}, \tag{22}$$

whence

$$s_{n+2} = \frac{T s_{n+1}s_n s_{n-1} - s_{n+1}^2 s_{n-2} - \alpha s_n^3}{s_{n-1}^2}. \tag{23}$$

For Somos-(4) the invariant T equals 4. Assume that $n \geq 3$ and the elements $s_0, \ldots, s_{n+1}$ are proved to be integer. Then the recurrence relation implies that $s_{n-2}s_{n+2}$ is integer, and the above relation implies that $s_{n-1}^2 s_{n+2}$ is integer as well. Hence the denominator of s_{n+2} in irreducible form divides both s_{n-2} and s_{n-1}^2. Since they are coprime, this implies that s_{n+2} is integer. By induction, the whole sequence Somos-(4) consists of integers.

Solution 17. For Somos-(4) the invariant T equals 4. By Problem 15 this sequence satisfies the equation

$$s_{n+2}s_{n-3} = -s_{n+1}s_{n-2} + 5 s_n s_{n-1}. \tag{24}$$

Now we use induction as above: since $s_{n+2}s_{n-2}$ and $s_{n+2}s_{n-3}$ are integer and moreover $(s_{n-2}, s_{n-3}) = 1$, the element s_{n+2} is integer as well.

Solution 18. (a) We shall find some sufficient conditions for integer-valuedness of the sequence in question, using the idea from Problem 15 (existence of two recurrence relations). Suppose that the coefficients α and β, the invariant T and five initial elements $s_0, s_1, \ldots, s_4$ are integers. Then every subsequent element of the sequence can be determined using the formulas

$$s_{n+2}s_{n-2} = \alpha s_{n+1}s_{n-1} + \beta s_n^2, \quad s_{n+2}s_{n-3} = \mu s_{n+1}s_{n-2} + \nu s_n s_{n-1},$$

where $\mu = -\beta$ and $\nu = \alpha^2 + \beta T$ are integer.
If $s_0, s_1, \ldots, s_{n+1}$ are integer then s_{n+2} will be integer for sure if $(s_{n-2}, s_{n-3}) = 1$; otherwise any prime divisor p of (s_{n-2}, s_{n+3}) can appear in the denominator of s_{n+2} and of all the subsequent elements. The condition $(s_{n-2}, s_{n-3}) = 1$ would be valid for all $n \geq 3$ for sure if $(s_0, s_1) = 1$ and $\beta = \pm 1$.

If $\beta \neq \pm 1$ then all elements in the sequence are integer for sure if no prime divisor p of β is a divisor of any element of the sequence. This implies the requirement that $(\alpha, p) = 1$. Then we have the congruence $s_{n+2}s_{n-2} \equiv \alpha s_{n+1}s_{n-1} \pmod p$ which implies that the elements of the sequence are not multiples of p if this is valid for s_0, s_1, s_2, s_3.

(b) The precise criterion for integer-valuedness of elements in a Somos-4 sequence is not known. A little later we will get some useful instrument, see the section «Somos-4 is Somos-m».

Solution 19. Let us find constants α' and β' such that

$$s_{n+4}s_{n-4} = \alpha' s_{n+2}s_{n-2} + \beta' s_n^2. \tag{25}$$

In terms of f_n it becomes a recurrence relation of the sixth order

$$f_{n+3}f_{n+2}^2 f_{n+1}^3 f_n^4 f_{n-1}^3 f_{n-2}^2 f_{n-3} = \alpha' f_{n+1}f_n^2 f_{n-1} + \beta'.$$

In view of the equalities

$$f_{n+3}f_{n+2}^2 f_{n+1} = \alpha f_{n+2} + \beta, \quad f_{n-3}f_{n-2}^2 f_{n-1} = \alpha f_{n-2} + \beta, \quad f_{n+1}f_n^2 f_{n-1} = \alpha f_n + \beta,$$

the order can be decreased to 4:

$$(\alpha f_{n+2} + \beta)(\alpha f_{n-2} + \beta)(\alpha f_n + \beta)^2 = \alpha'(\alpha f_n + \beta) + \beta'. \tag{26}$$

Now let us remove f_{n+2} and f_{n-2}. Their positions in the formula are symmetric. Thus the reduction to f_{n+1}, f_n and f_{n-1} is possible if the product $f_{n+2}f_{n-2}$ and the sum $f_{n+2} + f_{n-2}$ are expressed through them. Similarly any symmetric polynomial in f_{n+1} and f_{n-1} can be expressed in f_n, since

$$f_{n+1}f_{n-1} = \frac{\alpha f_n + \beta}{f_n^2} \text{ and } f_{n+1} + f_{n-1} = \frac{T f_n - \alpha}{f_n^2}. \tag{27}$$

To begin with, let us simplify the product:

$$f_{n+2}f_{n-2} = \frac{f_{n+2}f_{n+1}^2 f_n \cdot f_n f_{n-1}^2 f_{n-2}}{f_{n+1}^2 f_n^4 f_{n-1}^2} f_n^2 = \frac{(\alpha f_{n+1} + \beta)(\alpha f_{n-1} + \beta)}{(\alpha f_n + \beta)^2} f_n^2 = \frac{\alpha(\alpha^2 + \beta T)f_n + \beta^2 f_n^2}{(\alpha f_n + \beta)^2}.$$

The last transformation uses the equalities (27).

Now let us simplify the sum:

$$f_{n+2} + f_{n-2} = \frac{\alpha f_{n+1} + \beta}{f_{n+1}^2 f_n} + \frac{\alpha f_{n-1} + \beta}{f_{n-1}^2 f_n} = \frac{\alpha f_{n+1}f_{n-1}(f_{n+1} + f_{n-1}) + \beta(f_{n+1}^2 + f_{n-1}^2)}{(\alpha f_n + \beta)^2} f_n^3.$$

Remove f_{n+1}, f_{n-1} once more, using equalities (27) to get

$$f_{n+2} + f_{n-2} = \frac{-2\alpha\beta f_n^2 + (\alpha^2 T + \beta T^2 - 2\beta^2)f_n - \alpha(\alpha^2 + \beta T)}{(\alpha f_n + \beta)^2}.$$

Substituting the obtained representations for $f_{n+2}f_{n-2}$ and $f_{n+2} + f_{n-2}$ into (26) we obtain an equation in a single variable f_n:

$$\begin{aligned}\alpha^2(\alpha^3 f_n + \alpha\beta T f_n + \beta^2 f_n^2) + \alpha\beta(-2\alpha\beta f_n^2 + (\alpha^2 T + \beta T^2 - 2\beta^2)f_n - \\ - \alpha(\alpha^2 + \beta T)) + \beta^2(\alpha f_n + \beta)^2 = \alpha'(\alpha f_n + \beta) + \beta'.\end{aligned}$$

The coefficients at f_n^2 in this equation cancel. Equality of coefficients at f_n^1 and f_n^0 results in a system of two equations with two variables α' and β'. Solving the system, we find the only possible values $\alpha' = (\alpha^2 + \beta T)^2$, $\beta' = \beta^4 - \beta(\alpha^2 + \beta T)(2\alpha^2 + \beta T)$. Since all transformations were invertible, these α' and β' satisfy the recurrence relation (25).

The assertion of the problem also has a simpler proof, see the comment to Problem 30.

We may remark that this problem enables us to solve Problem 9. However below we will obtain several more conceptual solutions.

Periodicity of a Somos-4 sequence modulo an arbitrary integer

Solution 20.
The remainders of s_n modulo 5 are of the form

$$1, 1, 1, 1, 2, 3, 2, 3, 4, 4, 4, 4, 3, 2, 3, 2, 1, 1, 1, 1, \dots$$

Thus $s_n \equiv s_{n+16} \pmod 5$ for $n = 0, 1, 2, 3$. Between fours of consecutive units there are no zeros. Thus any subsequent remainder also can be computed using the recurrence relation

$$s_{n+2}s_{n-2} \equiv s_{n+1}s_{n-1} + s_n^2 \pmod 5.$$

In particular, this implies that the remainders repeat with period 16, and no zeros occur.

We get one more solution using the recurrence relation (24). Considered modulo 5 it turns into the congruence

$$s_{n+2}s_{n-3} \equiv -s_{n+1}s_{n-2} \pmod 5.$$

Suppose s_{n+2} is the first element in the sequence which is a multiple of 5. Then this congruence implies that $s_{n+1}s_{n-2} \equiv 0 \pmod 5$. Hence one of the integers s_{n+1}, s_{n-2} must be a multiple of 5, which contradicts our assumption.

Solution 21.
(a) First observe that the sequence (s_n) cannot contain two consecutive multiples of p. Indeed, if $p \mid s_{n-2}$ and $p \mid s_{n-1}$ then (1) and $(\beta, p) = 1$ imply $p \mid s_n$. Repeating this argument we get that all elements in the sequence (s_n) are multiples of p. Hence our assumption contradicts primitivity of (s_n).

Suppose there are two elements divisible by p and having indices which differ by 3. Then we get a contradiction again. Indeed, if $p \mid s_{n-2}$ and $p \mid s_{n+1}$ then (1) and the condition $(\beta, p) = 1$ imply $p \mid s_n$. Hence two consecutive elements s_n and s_{n+1} are multiples of p which was already proved impossible.

Suppose now that the sequence (s_n) contains two multiples of p with indices which differ by 2. If $p \mid s_{n-2}$ and $p \mid s_n$ then (1) and the condition $(\alpha, p) = 1$ imply $p \mid s_{n-1}s_{n+1}$. Then p divides s_n and one of the neighboring elements. This leads to a contradiction as well since p can divide either two neighboring elements of the sequence or two elements with indices which differ by 3.

The above implies that the indices of two multiples of p in the sequence differ by 4 at least. Hence it is always possible to choose three consecutive elements coprime with p.

(b) By lemma 10 the sequence (s_n) contains three consecutive elements coprime with p. This enables us to find the value of $T \pmod{p^\gamma}$ from formula (22).

Solution 22. Let us check that the value of $s_{n+2} \bmod p^\gamma$ is uniquely determined by the remainders of s_{n+1}, s_n, s_{n-1}, s_{n-2}, s_{n-3} when divided by p^γ. Indeed, let us find $s_{n+2} \bmod p^\gamma$ using recurrence relations (1) and (7) in the following form:

$$\begin{aligned} s_{n+2} &\equiv (\alpha s_{n+1}s_{n-1} + \beta s_n^2)s_{n-2}^{-1} \pmod{p^\gamma}, \\ s_{n+2} &\equiv (\widetilde{\alpha} s_{n+1}s_{n-2} + \widetilde{\beta} s_n s_{n-1})s_{n-3}^{-1} \pmod{p^\gamma}. \end{aligned} \tag{28}$$

The first relation makes sense if $(s_{n-2}, p) = 1$. The second one makes sense if $(s_{n-3}, p) = 1$. But at least one of these relations is valid since two consecutive elements of (s_n) are coprime (see the solution of Problem 10).

Consider the first $p^{5\gamma}$ fives of the form $(s_{n-3}, s_{n-2}, s_{n-1}, s_n, s_{n+1})$. There are at least two of them such that their corresponding elements have equal remainders when divided by p^γ. Formulas (28) imply that the sequence is periodical modulo p^γ.

Solution 23.
(a) Suppose T_i is the period of (a_n) modulo $p_i^{\gamma_i}$ $(i = 1, 2, \dots, l)$. Then for any $i = 1, 2, \dots, l$ and any integer n we have $a_{n+T} \equiv a_n \pmod{p_i^{\gamma_i}}$, where $T = [T_1, T_2, \dots, T_l]$ is the least common multiple of all periods. Since all $p_i^{\gamma_i}$ are pairwise coprime, the above congruences imply $a_{n+T} \equiv a_n \pmod m$ for $n \in \mathbb{Z}$.
(b) Suppose $m = p_1^{\gamma_1} \dots p_l^{\gamma_l}$ is the canonical decomposition of the integer m. From $(\alpha\beta, m) = 1$ we get $(\alpha\beta, p_i) = 1$ for $1 \le i \le l$. Hence the conditions of Problem 22 are fulfilled, and the sequence (s_n) is

periodical modulo each of $p_i^{\gamma_i}, 1 \le i \le l$. By part (a), the sequence is periodical modulo m as well.
(c) The sequence Somos-(4) satisfies the conditions of part (b), hence it is periodical modulo any integer.

Solution 24. For a prime p, the sequence $s_n = p^{n^2}$ satisfies (1) for $\alpha = 0$, $\beta = p^8$, but it is not periodical modulo p^γ for any $\gamma > 0$.

The Somos-5 sequences

Solution 25. We prove the assertion by induction. For $n = 0$ we have five pairwise coprime consecutive elements $(s_0, s_1, s_2, s_3, s_4) = (1, 1, 1, 1, 1)$. Suppose $(s_{n+4}, s_{n+3}, s_{n+2}, s_{n+1}, s_n)$ is the first five not consisting of coprime integers. Then some prime p divides s_{n+4} and one of s_{n+3}, s_{n+2}, s_{n+1}, s_n. Using the recurrence relation $s_{n+4}s_{n-1} = s_{n+3}s_n + s_{n+2}s_{n+1}$ we find that if $p \mid s_{n+3}$ or $p \mid s_n$ then $p \mid s_{n+2}s_{n+1}$. If $p \mid s_{n+2}$ or $p \mid s_{n+1}$ then $p \mid s_{n+3}s_n$. In any case $p \mid (s_{n+3}s_n, s_{n+2}s_{n+1})$, a contradiction with our assumption.

Solution 26.
(a) Set $h_n = f_n f_{n+1}$ to get

$$h_{n-1}h_n h_{n+1} = \mu h_n + \nu.$$

(b) From part (a) we get

$$h_{n+1} = \frac{\mu}{h_{n-1}} + \frac{\nu}{h_{n-1}h_n}, \quad h_{n-2} = \frac{\mu}{h_n} + \frac{\nu}{h_{n-1}h_n}.$$

Thus

$$\mu\left(\frac{1}{h_{n-1}} + \frac{1}{h_n}\right) + \frac{\nu}{h_{n-1}h_n} = h_{n-2} + \frac{\mu}{h_{n-1}} = h_{n+1} + \frac{\mu}{h_n}.$$

Hence

$$J = h_{n-2} + h_{n-1} + h_n + \frac{\mu}{h_{n-1}} = h_{n-1} + h_n + h_{n+1} + \frac{\mu}{h_n}. \tag{29}$$

This is just the required invariant.
(c)

$$J(x, y, z) = xy + yz + \mu\left(\frac{1}{xy} + \frac{1}{yz}\right) + \frac{\nu}{xy^2z}.$$

Solution 27. (a) Set $x_n = f_{n-1}f_n f_{n+1}$. Then the recurrence relation from Problem 13(b) takes the form

$$x_n x_{n+1} = \mu f_n f_{n+1} + \nu,$$

whence

$$x_{n+1} = \frac{\mu}{f_{n-1}} + \frac{\nu}{x_n}. \quad x_{n-1} = \frac{\mu}{f_{n+1}} + \frac{\nu}{x_n},$$

Thus

$$\mu\left(\frac{1}{f_{n+1}} + \frac{1}{f_{n-1}}\right) + \frac{\nu}{x_n} = x_{n-1} + \frac{\mu}{f_{n-1}} = x_{n+1} + \frac{\mu}{f_{n+1}}.$$

This gives even two (complementary) almost-invariants:

$$K_1(x, y, z) = \mu\left(\frac{1}{x} + \frac{1}{z}\right) + \frac{\nu}{xyz} \quad \text{and} \quad K_2(x, y, z) = xyz + \frac{\mu}{y}, \tag{30}$$

since $K_1(f_{n-1}, f_n, f_{n+1}) = K_2(f_{n-2}, f_{n-1}, f_n)$ and conversely.
(b,c) The above argument implies that for I we can take the sum of two above almost-invariants:

$$I(x, y, z) = K_1(x, y, z) + K_2(x, y, z) = xyz + \mu\left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right) + \frac{\nu}{xyz}. \tag{31}$$

Moreover we can obtain other expressions for the value of this invariant:

$$I_n = I(f_{n-1}, f_n, f_{n+1}) = K_1(f_{n-1}, f_n, f_{n+1}) + K_1(f_n, f_{n+1}, f_{n+2}) = K_2(f_{n-1}, f_n, f_{n+1}) + K_2(f_n, f_{n+1}, f_{n+2}) =$$
$$= \mu \left(\frac{1}{f_{n-1}} + \frac{1}{f_n} + \frac{1}{f_{n+1}} + \frac{1}{f_{n+2}} \right) + \nu \left(\frac{1}{f_{n-1} f_n f_{n+1}} + \frac{1}{f_n f_{n+1} f_{n+2}} \right) =$$
$$= f_{n-1} f_n f_{n+1} + f_n f_{n+1} f_{n+2} + \mu \left(\frac{1}{f_n} + \frac{1}{f_{n+1}} \right). \quad (32)$$

Solution 28. We will use induction in n. The base is $s_0 = \ldots = s_4 = 1$. Let s_k be integer for any $k \le n+2$. Denote $s_{n-2} = a$, $s_{n-1} = b$, $s_n = c$, $s_{n+1} = d$, $s_{n+2} = e$. Then the relation7 implies that s_{n+3} is integer if $be + cd \equiv 0 \pmod a$.

Both invariants J and I of Somos-(5) are equal to 5 by Problems 26 and 27. They can be presented in the form

$$J = \frac{ad}{bc} + \frac{be}{cd} + \frac{bc}{ad} + \frac{cd}{be} + \frac{c^2}{ae} \quad (33)$$

$$I = \frac{b^2}{ac} + \frac{c^2}{bd} + \frac{d^2}{ce} + \frac{ae}{bd} + \frac{bd}{ae} \quad (34)$$

Multiplying (33) and (34) by $abcde$ modulo a, we get $bc^2(be+cd) \equiv 0 \pmod a$ and $b^2d(be+cd) \equiv 0 \pmod a$ respectively. Since b, c and d are coprime with a by Problem 25, in both cases $be+cd$ is a multiple of a.

Solution 29. Choose a prime p and a positive integer γ. Let us use induction in n to prove that s_n is correctly defined modulo p^γ. The base is $s_0 = \ldots = s_4 = 1$. Suppose s_k (integer for any k by Problem 28) is correctly defined modulo p^γ for any $k \le n+2$. Denote $s_{n-2} = a$, $s_{n-1} = b$, $s_n = c$, $s_{n+1} = d$, $s_{n+2} = e$.

If a is not a multiple of p then $s_{n+3} = \frac{be+cd}{a}$ is correctly defined modulo p^γ. Otherwise p^γ does not divide b, c, d, e by Problem 25. Then $f_{n-1}, \ldots, f_{n+1} \pmod{p^\gamma}$ are correctly defined. Transform the polynomial 31 and substitute $y = f_n$, $z = f_{n+1}$:

$$f_n^2 f_{n+1}^2 x^2 + (f_n + f_{n+1} - I f_n f_{n+1})x + f_n f_{n+1} = 0.$$

This polynomial has two roots: f_{n-1} and f_{n+2}. By Vieta's theorem, $f_{n+2} = \frac{I f_n f_{n+1} - (f_n + f_{n+1})}{f_n^2 f_{n+1}^2} - f_{n-1}$, hence f_{n+2} is correctly defined modulo p^γ, then $s_{n+3} = \frac{f_{n+2} s_{n+2}^2}{s_{n+1}}$ is correctly defined modulo p^γ as well. Thus the whole sequence is correctly defined modulo p^γ. By the pigeonhole principle there exist two fives of consecutive elements which are the same modulo p^γ. They form the period of Somos-(5) modulo p^γ.

To pass to an arbitrary positive integer m, it suffices to use Problem 23(a).

Solution 30. Let us use the results of Problems 26(a) and 26(c). Consider the sequence $h_n = f_n f_{n+1}$ such that the following relations hold:

$$h_{n-1} h_n h_{n+1} = \mu h_n + \nu, \quad (35)$$

$$J = h_{n-1} + h_n + \alpha \left(\frac{1}{h_{n-1}} + \frac{1}{h_n} \right) + \frac{\beta}{h_{n-1} h_n}. \quad (36)$$

We have

$$\frac{s_{n-4} s_{n+4}}{s_n^2} = h_{n-3} h_{n-2} h_{n-1}^2 h_n^2 h_{n+1} h_{n+2} = h_{n-1} h_n (\mu h_{n-2} + \nu)(\mu h_{n+1} + \nu).$$

Remove h_{n-2} and h_{n+1} by means of equalities

$$h_{n-2} = \frac{\mu}{h_n} + \frac{\nu}{h_{n-1} h_n}, \qquad h_{n+1} = \frac{\mu}{h_{n-1}} + \frac{\nu}{h_{n-1} h_n}$$

and use (36) to obtain an equation equivalent to (1):

$$\frac{s_{n-4} s_{n+4}}{s_n^2} = \nu^2 h_{n-1} h_n + \mu(\mu^3 + 2\nu^2 + \mu\nu J) = \alpha^* \frac{s_{n-2} s_{n+2}}{s_n^2} + \beta^*$$

where $\alpha^* = \nu^2$ and $\beta^* = \mu(\mu^3 + 2\nu^2 + \mu\nu J)$.

This equation in particular enables us solve Problem 9. For the sequence (ψ_n) the parameters have the following values: $\alpha = \beta = 1$, $T = -2$, $\mu = -\beta = -1$, $\nu = \alpha^2 + \beta T = -1$, $J = -1$. Hence $\alpha^* = \beta^* = 1$, so the sequence $s_n = (\psi_{2n-3})$ satisfies the equation $s_{n+2}s_{n-2} = s_{n+1}s_{n-1} + s_n^2$. Since the first four elements of this sequence are units, this is Somos-(4).

The assertion just proved enables us to obtain a simpler solution of Problem 19. By Problem 15, a Somos-4 sequence satisfies the equation for a Somos-5 sequence with the coefficients $\tilde{\alpha} = -\beta$ and $\tilde{\beta} = \alpha^2 + \beta T$. Now apply Problem 30 to establish that a Somos-4 sequence satisfies the equation (25) with coefficients $\alpha' = \alpha^* = \tilde{\beta}^2 = (\alpha^2 + \beta T)^2$ and $\beta' = \beta^* = \tilde{\alpha}^4 + \tilde{\alpha}\tilde{\beta}(2\tilde{\beta} + \tilde{\alpha}J) = \beta^4 - \beta(\alpha^2 + \beta T)(2\alpha^2 + \beta T)$.

Solution 31. The relation $I^2 = 4(\nu + \mu J)$ is necessary and sufficient.

Let us check its necessity. Suppose a sequence is both Somos-4 (with coefficients α and β) and Somos-5 (with coefficients μ and ν). Problem 15 provides formulas $\mu = -\beta$, $\nu = \alpha^2 + \beta T$. Moreover there exists a connection between the invariants: the formula (32) implies the presentation

$$I = f_{n-1}f_nf_{n+1} + f_nf_{n+1}f_{n+2} + \mu\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) = \left(\alpha + \frac{\beta}{f_n}\right) + \left(\alpha + \frac{\beta}{f_{n+1}}\right) - \beta\left(\frac{1}{f_n} + \frac{1}{f_{n+1}}\right) = 2\alpha,$$

and the formula (29) implies the presentation

$$J = f_{n-1}f_n + f_nf_{n+1} + f_{n+1}f_{n+2} + \frac{\mu}{f_nf_{n+1}} = f_{n-1}f_n + f_nf_{n+1} + \left(\frac{\alpha}{f_n} + \frac{\beta}{f_nf_{n+1}}\right) - \frac{\beta}{f_nf_{n+1}} = T. \tag{37}$$

Hence

$$I^2 = 4\alpha^2 = 4(\alpha^2 + \beta T - \beta T) = 4(\nu + \mu J).$$

To prove sufficiency of $I^2 = 4(\nu + \mu J)$ observe that in the notation from the solutions of Problems 26 and 27 we have

$$4(\nu + \mu J) = 4\left(x_n + \frac{\mu}{f_n}\right)\left(\frac{\mu}{f_{n-1}} + \frac{\mu}{f_{n+1}} + \frac{\nu}{x_n}\right) = I^2 - \left(x_n + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{x_n}\right)^2,$$

and thus

$$I^2 - 4(\nu + \mu J) = \left(f_{n-1}f_nf_{n+1} + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{f_{n-1}f_nf_{n+1}}\right)^2.$$

Hence the equality $I^2 = 4(\nu + \mu J)$ means that

$$f_{n-1}f_nf_{n+1} + \mu\left(\frac{1}{f_n} - \frac{1}{f_{n-1}} - \frac{1}{f_{n+1}}\right) - \frac{\nu}{f_{n-1}f_nf_{n+1}} = 0. \tag{38}$$

From (31) and (38) we get the equation $f_{n-1}f_nf_{n+1} + \frac{\mu}{f_n} = I/2$ which coincides with 13(a) for $\mu = -\beta$ and $I = 2\alpha$. Hence the sequence is Somos-4 with $\beta = -\mu$ and $\alpha = I/2$.

Solution 32. The replacement $s_{2n} \mapsto ts_{2n}$ $(t \neq 0)$ acts on the variables f_n as follows: $f_{2n} \mapsto t^{-2}f_{2n}$, $f_{2n+1} \mapsto t^2 f_{2n+1}$. Hence the value of J does not change, and almost invariants K_1 and K_2 (computed for even n) turn to $K_{n,1}(t)$ and $K_{n,2}(t)$, where

$$K_{n,1}(t) = \frac{\mu}{t^2}\left(\frac{1}{f_{n-1}} + \frac{1}{f_{b+1}}\right) + \frac{\nu}{t^2 f_{n-1}f_nf_{n+1}} = \frac{K_{0,1}}{t^2},$$

$$K_{n,2}(t) = t^2 f_{n-1}f_nf_{n+1} + \frac{\mu t^2}{f_n} = t^2 K_{0,2}.$$

Hence I is replaced by $I(t) = K_{0,1}/t^2 + K_{0,2}t^2$. According to Problem 31, the necessary and sufficient condition for a Somos-5 sequence to be Somos-4 is the equality $I(t)^2 = 4(\nu + \mu J)$. As an equation in t it always has a complex solution perhaps except the case $K_{0,1} = K_{0,2} = 0$.

This last case means that

$$\mu(f_{-1}f_0 + f_0f_1) + \nu = f_{-1}f_0^2f_1 + \mu = 0.$$

Denoting $f_{-1} = a$, $f_0 = b$, $f_1 = c$, we get $\mu = -ab^2c$, $\nu = -\mu(ab + bc) = ab^3c(a + c)$, $J = ab + bc - (ab + bc) + b(a + c) = ab + bc$. Then $I^2 - 4(\nu + \mu J) = -4ab^3c(a + c) + ab^2c \cdot (ab + bc) = 0$, so the required condition is satisfied automatically.

Connection with elliptic curves

Solution 33. Let points P and Q have coordinates (x_P, y_P) and (x_Q, y_Q). By condition, $x_P \neq x_Q$, thus the line through P and Q is determined by the equation

$$(y - y_P)(x_Q - x_P) = (x - x_P)(y_Q - y_P).$$

Express y from this equation:

$$y = y_P + (x - x_P)\frac{y_Q - y_P}{x_Q - x_P} = x\frac{y_Q - y_P}{x_Q - x_P} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P}.$$

To find the points of meet of the given line with the elliptic curve, it suffices to substitute y into the equation $y^2 = x^3 + ax + b$:

$$\left(x\frac{y_Q - y_P}{x_Q - x_P} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P}\right)^2 = x^3 + ax + b.$$

We get a cubic equation in x, two roots of which are x_P and x_Q. Observe that this equation has a third root, by Vieta theorem equal to $\left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q$ (maybe it equals one of the other roots). By the above equality, it corresponds to the value of y

$$\frac{\left(\left(\frac{y_Q-y_P}{x_Q-x_P}\right)^2 - x_P - x_Q\right)(y_Q - y_P)}{x_Q - x_P} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P} =$$
$$= \frac{\left((y_Q - y_P)^2 - (x_P + x_Q)(x_Q - x_P)^2\right)(y_Q - y_P)}{(x_Q - x_P)^3} + \frac{y_P x_Q - x_P y_Q}{x_Q - x_P}.$$

This is the point R'. The problem was to construct the point R, its coordinates are

$$\left(\left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 - x_P - x_Q,\ \frac{\left((y_Q - y_P)^2 - (x_P + x_Q)(x_Q - x_P)^2\right)(y_Q - y_P)}{(x_P - x_Q)^3} + \frac{y_P x_Q - x_P y_Q}{x_P - x_Q}\right). \tag{39}$$

The case of coincidence of P and Q is elaborated in Problem 38.

The resulting formula is symmetrical in P and Q, thus addition is commutative.

Solution 34. Let P be a finite point, and Q the infinite point. Then the line PQ is vertical, R' is symmetrical to P about the x-axis, hence R coincides with P.

The sum of two finite points of en elliptic curve ia the infinite point if the line PQ is vertical. This is possible in two cases: if P and Q are mutually symmetric about the x-axis or if $P = Q$ and the tangent in this point is vertical.

Solution 35. Let the lines l_1, l_2, l_3, m_1, m_2, m_3 be determined by the equations

$$L_1(x, y) = 0,\ L_2(x, y) = 0,\ L_3(x, y) = 0,$$
$$M_1(x, y) = 0,\ M_2(x, y) = 0,\ M_3(x, y) = 0$$

respectively. Let the equation of the elliptic curve have the form $F(x, y) = 0$. We shall prove that for some numbers α, β we have

$$F(x, y) = \alpha L_1(x, y)L_2(x, y)L_3(x, y) + \beta M_1(x, y)M_2(x, y)M_3(x, y). \tag{40}$$

Denote the points of meet of l_1, l_2, l_3 with m_1 as follows: $l_1 \cap m_1 = A$, $l_2 \cap m_1 = B$, $l_3 \cap m_1 = C$. Choose a point $D = (d_1, d_2)$ on m_1, distinct from A, B, C. Since it doesn't belong to any of l_1, l_2, l_3, we have $L_1(d_1, d_2) \neq 0$, $L_2(d_1, d_2) \neq 0$, $L_3(d_1, d_2) \neq 0$. Substitute the coordinates of (d_1, d_2) into (40) to obtain the equation

$$F(d_1, d_2) = \alpha L_1(d_1, d_2)L_2(d_1, d_2)L_3(d_1, d_2),$$

which enables us to determine α. For this value of α, the difference

$$F(x,y) - \alpha L_1(x,y)L_2(x,y)L_3(x,y) - \beta M_1(x,y)M_2(x,y)M_3(x,y) \tag{41}$$

vanishes at four points of m_1. But it is a polynomial of degree 3 at most, thus the difference in question is a multiple of $M_1(x,y)$ (this is not obvious but is easily proved).

Arguing similarly, consider four points on l_1 (three points of meet with m_i's and an additional one) and find the parameter β such that the difference in question is a multiple of $L_1(x,y)$. For obtained values of α, β the difference has the form

$$L_1(x,y)M_1(x,y)N(x,y),$$

where N is a polynomial of degree 1 at most.

Choose one more of the given points, say $G = (g_1, g_2) = l_2 \cap m_3$, and substitute it to the above expression. We have

$$0 = F(g_1,g_2) - \alpha L_1(g_1,g_2)L_2(g_1,g_2)L_3(g_1,g_2) - \beta M_1(g_1,g_2)M_2(g_1,g_2)M_3(g_1,g_2) = \\ = L_1(g_1,g_2)M_1(g_1,g_2)N(g_1,g_2).$$

By condition, the nine points in question are distinct, so $L_1(g_1,g_2) \neq 0$, $M_1(g_1,g_2) \neq 0$, hence $N(g_1,g_2) = 0$. Similarly for points $H = (h_1,h_2) = l_3 \cap m_2$ and $I = (i_1,i_2) = l_2 \cap m_2$ we get $N(h_1,h_2) = 0$ and $N(i_1,i_2) = 0$ (thus we have this for all points of meet except $l_3 \cap m_3$, for which we intend to prove that it belongs to the elliptic curve). So the line with the equation $N(x,y) = 0$ coincides both with l_2 and m_2, a contradiction. Hence the equation has the degree 0, not 1, and it determines the identical zero since it gives zero at $G = (g_1,g_2)$. Hence (41) is zero, and this implies that $l_3 \cap m_3$ lies on the elliptic curve.

Solution 36. Denote the infinite point by O, and let $-P$ be the point such that its sum with P equals O. To prove associativity of addition of P, Q, R consider the following lines:

l_1 through points Q, $-Q-R$, R; l_2 through $-P-Q$, O, $P+Q$; l_3 through P, $Q+R$, $-P-(Q+R)$;
m_1 through Q, $-P-Q$, P; m_2 through $-Q-R$, O, $Q+R$; m_3 through R, $P+Q$, $-R-(P+Q)$.

All the above points except $-P-(Q+R)$ and $-R-(P+Q)$ belong to the elliptic curve for sure. Hence by the preceding problem $l_3 \cap m_3$ belongs to the elliptic curve as well. Thus $l_3 \cap m_3 = -P-(Q+R) = -R-(P+Q)$, so the addition of points is associative.

Solution 37. The formulas for addition imply that if x_P, y_P, x_Q, y_Q are rational then x_R, y_R necessarily are also rational. (In the case $P = Q$ use the next problem and rationality of a and b.)

Solution 38. Differentiate the function $x^3 + ax + b - y^2$ by x and by y to see that its gradient is $(3x^2 + a, -2y)$. Hence the equation for the line tangent to our elliptic curve at point (x_P, y_P) is of the form

$$(3x_P^2 + a)(x - x_P) - 2y_P(y - y_P) = 0. \tag{42}$$

This equation determines a line in all cases except $3x_P^2 + a = -2y_P = 0$. It is not hard to see that the conditions $3x_P^2 + a = -2y_P = x_P^3 + ax_P + b - y_P^2 = 0$ imply $4a^3 + 27b^2 = 0$ which is forbidden by definition of an elliptic curve.

The further argument for $y_P \neq 0$ is similar to the solution of Problem 33. Express y from the equation (42):

$$y = y_P + \frac{(x - x_P)(3x_P^2 + a)}{2y_P}.$$

Substitute this to the equation of the elliptic curve:

$$\left(y_P + \frac{(x - x_P)(3x_P^2 + a)}{2y_P}\right)^2 = x^3 + ax + b.$$

Two roots of this equation are equal to x_P. Furthermore by Vieta theorem the sum of the roots of the equation equals the coefficient at x^2 with the opposite sign, that is,

$$\left(\frac{3x_P^2 + a}{2y_P}\right)^2.$$

Hence the third root (exists for sure and) equals

$$\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P.$$

The y-coordinate of this point equals

$$y = y_P + \frac{\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P - x_P\right)(3x_P^2+a)}{2y_P},$$

and the reflection about x-axis gives the point with coordinates

$$\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 2x_P,\ -y_P - \frac{\left(\left(\frac{3x_P^2+a}{2y_P}\right)^2 - 3x_P\right)(3x_P^2+a)}{2y_P}\right).$$

Now consider the case $y_P = 0$. Then the tangent is vertical: $x = x_P$, and the third point of meet with the elliptic curve is the infinite point O. Observe that there are at most three such points $(x_P, 0)$ on our curve, and they correspond to the roots of $x^3 + ax + b = 0$. The picture in Section 7 shows three such points.

Solution 39. (a) We have

$$X = -\frac{x}{4\alpha}, \qquad Y = \frac{1}{2X^2}\left(TX - \alpha - \frac{y}{4\alpha}\right) = -\frac{2\alpha}{x^2}(Tx + 4\alpha^2 + y).$$

This gives the equation

$$(Tx + 4\alpha^2 + y)^2 - (x^3 + 8\alpha^2 Tx + 32\alpha^4 + 8\alpha^2 y) + 4\beta x^2 - (2T^2x^2 + 8\alpha^2 Tx + 2Txy) = 0,$$

or

$$y^2 = x^3 + (T^2 - 4\beta)x^2 + 8\alpha^2 Tx + 16\alpha^4. \tag{43}$$

(b) Rename the coordinate x from the preceding part into x'. To get the standard form of the equation, it suffices to substitute $x = x' + (T^2 - 4\beta)/3$. We get the equation

$$y^2 = x^3 + \left(8\alpha^2 T - \frac{(T^2-4\beta)^2}{3}\right)x + \left(\frac{2(T^2-4\beta)^3}{27} - \frac{8\alpha^2 T}{3}(T^2 - 4\beta) + 16\alpha^4\right). \tag{44}$$

Remark 1. Addition of points on an elliptic curve usually involves their coordinates but not the equation of the curve. Hence the specific values of the coordinates of points are more significant for us than the equation (44) (although it also can occur to be useful).

Remark 2. There was some inaccuracy in the condition of the problem. Namely, we always obtain a sequence of points on a cubic curve of the required form but this curve is not always elliptic. However it is so in the nontrivial cases!

Solution 40. In this solution we use the result of the next problem.

(a) We have $\alpha = \beta = 1$ and $T = -2$. From the preceding problem we obtain the curve $y^2 = x^3 - 16x + 16$ and points $P_n(-4f_n, -4(1 + 2f_n + 2f_n^2 f_{n+1}))$. Now the next problem implies that $P_n = nP$ for $P(0, -4)$.

(b) The elements of the sequence with odd indices correspond to the points $Q_n = (-3P) + n \cdot Q$, where $Q = 2P = P_2 = (4, -4)$ (we have shifted the indices as needed).

Suppose $t_n = (-1)^n s_{2n-3}$; let (g_n) be the homogeneous sequence corresponding to (t_n). Denote by (t'_n) and (g'_n) the sequence Somos-(4) and its homogeneous sequence respectively. We see that $t_n = t'_n$ for $n = 0, 1, 2, 3$ (and so $g_n = g'_n$ for $n = 1, 2$).

Observe that the parameters $\alpha = \beta = 1$, $T = 4$ determine just the curve $y^2 = x^3 - 16x + 16$ and the progression with difference $Q = (4, -4)$. For $g'_1 = g'_2 = 1$ this progression starts from $Q_1 = (0, 4) = P_{-1}$. Hence for the sequence (g'_n) the corresponding sequence of points is (Q_n). This implies that $g'_n = g_n$ for all n. Finally, $t'_n = t_n$ for $n = 0, 1, 2, 3$ implies $t'_n = t_n$ for all n.

Remark. It looks so that the solution works only if we know the required result. However it is not difficult to see that *every* arithmetical progression on an elliptic curve corresponds to a homogeneous sequence which in turn enables us to determine the corresponding Somos-4 sequence. So all the parameters could be determined in the process of solution.

Solution 41.
(a) In general, we obtain the following points on the curve:

$$P_n = (x_n, y_n) = \left(-4\alpha f_n + \frac{T^2 - 4\beta}{3},\ 4\alpha(Tf_n - \alpha - 2f_n^2 f_{n+1})\right).$$

Let us find the point $P = P_{n+1} - P_n = P_{n+1} + (-P_n)$ with coordinates (x, y); we aim to show that it does not depend on n.

To begin with, simplify the formula for the slope of the line $(-P_n)P_{n+1}$:

$$k = \frac{y_{n+1} + y_n}{x_{n+1} - x_n} = \frac{-T(f_n + f_{n+1}) + 2\alpha + 2f_n^2 f_{n+1} + 2f_{n+1}f_{n+2}}{f_{n+1} - f_n}$$
$$= T - 2f_n f_{n+1} + \frac{2f_{n+1}}{f_{n+1} - f_n}\left(-T + \frac{\alpha}{f_{n+1}} + f_n f_{n+1} + f_{n+1}f_{n+2}\right) = T - 2f_n f_{n+1},$$

hence

$$k^2 = (T - 2f_n f_{n+1})^2 = T^2 + 4(f_n^2 f_{n+1}^2 - Tf_n f_{n+1}) = T^2 - 4\alpha(f_n + f_{n+1}) - 4\beta.$$

Thus

$$x = k^2 - x_{n+1} - x_n = T^2 - 4\alpha(f_n + f_{n+1}) - 4\beta + 4\alpha(f_n + f_{n+1}) - \frac{2(T^2 - 4\beta)}{3} = \frac{T^2 - 4\beta}{3},$$

whence

$$-y = -y_n + (x - x_n)k = 4\alpha(-Tf_n + \alpha + 2f_n^2 f_{n+1}) + 4\alpha f_n(T - 2f_n f_{n+1}) = 4\alpha^2.$$

So the point $P = \left(\frac{T^2-4\beta}{3}, -4\alpha^2\right)$ is constant, Q.E.D.

(b) If $P_n = nP$ then $P_0 = 0$ is the infinite point. Thus f_0 must take the infinite value, so $s_0 = 0$.

Solution 42. The recurrence relation for the elements of (ψ_n) in homogeneous coordinates $f_n = \psi_{n-1}\psi_{n+1}/\psi_n^2$ has the form

$$f_{n+1}f_n^2 f_{n-1} = f_n + 1. \tag{45}$$

Using initial values $f_2 = -1$, $f_3 = 1$ we find that $T = -2$. So we may use formulas

$$f_n f_{n-1} + f_n f_{n+1} + \frac{1}{f_n} = f_n f_{n-1} + \frac{1}{f_{n-1}} + \frac{1}{f_n} + \frac{1}{f_n f_{n-1}} = -2. \tag{46}$$

Let us prove the equality

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1})\right) \tag{47}$$

by induction. The coordinates of $P_2 = 2P_1$ are computed directly by duplication: $P_2 = (1, \frac{1}{2})$. Hence (47) is valid for $n = 2$. Suppose (47) is valid for some $n \geq 2$. Let us check it for $n+1$. When we add nP and P, the slope of the secant has the form

$$k_n = \frac{y_n - y_1}{x_n - x_1} = \frac{1}{-f_n}\left(\frac{f_n^2}{2}(f_{n+1} - f_{n-1} - \frac{1}{2}\right) = -(f_n f_{n+1} + 1).$$

Thus

$$x_{n+1} = k_n^2 - x_n - x_1 = (f_n f_{n+1} + 1)^2 + f_n = -f_{n+1}.$$

It remains to determine the y-coordinate of P_{n+1}:

$$y_{n+1} = -k_n(x_{n+1} - x_1) - y_1 = -(f_n f_{n+1} + 1)f_{n+1} - \frac{1}{2} = \frac{f_{n+1}^2}{2}(f_{n+2} - fn).$$

The last transformation uses the recurrence relation (45) and the formulas (46) for the invariant T.

Solution 43. The value of the invariant $T = 2(a+3x^2)$ for the sequence (ψ_n) is determined from the initial conditions (9). Thus we can apply the formulas

$$f_n f_{n-1} + f_n f_{n+1} + \frac{\alpha}{f_n} = f_n f_{n-1} + \alpha\left(\frac{1}{f_{n-1}} + \frac{1}{f_n}\right) + \frac{\beta}{f_n f_{n-1}} = T = 2(a+3x^2). \tag{48}$$

Let us prove the equality

$$nP = \left(-f_n, \frac{f_n^2}{2}(f_{n+1} - f_{n-1})\right) \tag{49}$$

by induction.

The coordinates of $2P$ are determined directly by duplication. Hence the equality (49) holds for $n=2$. Suppose that (49) is valid for some $n \geq 2$. Let us check it for $n+1$. When we sum up points nP and P, the slope of the secant has the form

$$k_n = \frac{y_n - y_1}{x_n - x_1} = \frac{1}{-f_n}\left(\frac{f_n^2}{4y}(f_{n+1} - f_{n-1} - y\right) = -\frac{1}{4y}(2f_n f_{n+1} - T).$$

Hence

$$x_{n+1} = k_n^2 - x_n - x_1 = \frac{1}{16y^2}(2f_n f_{n+1} - T)^2 - 2x + f_n = x - f_{n+1}.$$

It remains to determine the y-coordinate of P_{n+1}:

$$y_{n+1} = -k_n(x_{n+1} - x_1) - y_1 = -\frac{1}{4y}(2f_n f_{n+1} - T)f_{n+1} - y = \frac{f_{n+1}^2}{4y}(f_{n+2} - fn).$$

The last transformation uses the recurrence relation (45) and the formulas (48) for the invariant T.

Somos-4 is Somos-m

Solution 44. The assertion of the problem follows from the equalities

$$s_{n+l}s_{n-l} = \alpha^{l^2} s_n^2 \quad (l \geq 0), \qquad s_{n+l+1}s_{n-l} = \alpha^{l(l+1)} s_{n+1}s_n \quad (l \geq 0),$$

which can be checked using (19).

Solution 45. As in the above problem, the assertion follows from the explicit formulas (20):

$$s_{n+l}s_{n-l} = \alpha^{2l-2} s_{n+l-2}s_{n-l+2} \quad (l \geq 2), \qquad s_{n+l+1}s_{n-l} = \alpha^{l(l+1)/2} s_{n+1}s_n \quad (l \geq 0).$$

Solution 46. Introduce new variables

$$F_k^{(n)} = \frac{s_{n+k}s_{n-k}}{s_n^2}. \tag{50}$$

In particular, $F_0^{(n)} = 1$, $F_1^{(n)} = f_n$, $F_2^{(n)} = \alpha f_n + \beta$. Then the equality (11) can be presented in the form

$$F_k^{(n)} = c_k f_n - d_k. \tag{51}$$

Since $F_k^{(n)} = F_{-k}^{(n)}$, it suffices to consider nonnegative values of k. Clearly (51) is valid for $k=1$ and $k=2$ if we set

$$c_1 = 1, \quad d_1 = 0, \quad c_2 = \alpha, \quad d_2 = -\beta.$$

To determine the coefficients c_{k+1}, d_{k+1} from the known values of vc_{k-1}, d_{k-1}, c_k, d_k, let us use the equality

$$F_{k+1}^{(n)} = \frac{F_k^{(n-1)} F_k^{(n+1)}}{F_{k-1}^{(n)}} f_n^2,$$

which follows from definition (50).

Transform this equality using (51):

$$F_{k+1}^{(n)} = \frac{(c_k f_{n-1} - d_k)(c_k f_{n+1} - d_k)}{c_{k-1} f_n - d_{k-1}} f_n^2 = \frac{c_k^2 f_{n-1} f_n^2 f_{n+1} - c_k d_k f_n^2 (f_{n-1} + f_{n+1}) + d_k^2 f_n^2}{c_{k-1} f_n - d_{k-1}}.$$

Apply (45) and (6) to the right side:

$$F_{k+1}^{(n)} = \frac{c_k^2(\alpha f_n + \beta) - c_k d_k (T f_n - \alpha) + d_k^2 f_n^2}{c_{k-1} f_n - d_{k-1}}.$$

Hence the equality $F_{k+1}^{(n)} = c_{k+1} f_n - d_{k+1}$ is equivalent to

$$d_k^2 f_n^2 + c_k f_n(\alpha c_k - T d_k) + c_k(\beta c_k + \alpha d_k) - (c_{k+1} f_n - d_{k+1})(c_{k-1} f_n - d_{k-1}) = 0.$$

Setting the coefficients at various powers of f_n equal to 0, we obtain an *overdetermined* system of equations in the variables c_{k+1}, d_{k+1}:

$$\begin{aligned} c_{k+1} c_{k-1} =& d_k^2, & (52)\\ c_{k-1} d_{k+1} + c_{k+1} d_{k-1} =& - c_k(\alpha c_k - T d_k), & (53)\\ d_{k-1} d_{k+1} =& c_k(\beta c_k + \alpha d_k). & (54) \end{aligned}$$

Solution 47.

$$c_1 = 1, \quad d_1 = 0, \quad c_2 = \alpha, \quad d_2 = -\beta.$$
$$c_3 = d_2^2 = \beta^2, \quad d_3 = -c_2(\alpha c_2 - T d_2) = -\alpha(\alpha^2 + \beta T)$$

Solution 48. For $k = 2$ the last equation degenerates, and the values $c_3 = \beta^2$, $d_3 = -\alpha(\alpha^2 + T\beta)$ are determined from the first two equations. For $k \geq 3$ consistency of (52)–(54) needs an explanation. Suppose that the values c_{k+1} and d_{k+1} are determined from (52) and (54), that is,

$$c_{k+1} = \frac{d_k^2}{c_{k-1}}, \qquad d_{k+1} = \frac{c_k(\beta c_k + \alpha d_k)}{d_{k-1}}. \tag{55}$$

Substitute these to (53) and divide by $c_k d_k$ to obtain the condition for consistency of the system:

$$g_{k-1} g_k + \alpha \left(\frac{1}{g_{k-1}} + \frac{1}{g_k} \right) + \frac{\beta}{g_{k-1} g_k} = T, \tag{56}$$

where $g_k = d_k / c_k$. The formula (56) follows for $k = 3$ from $g_2 = -\beta/\alpha$, $g_3 = -\alpha(\alpha^2 + T\beta)/\beta^2$. Divide the second equality (55) by the first one to get that the sequence (g_k) satisfies a recurrence relation which coincides with the recurrence relation for the elements of (f_k):

$$g_{k-1} g_k^2 g_{k+1} = \alpha g_k + \beta.$$

Thus the formula (56) follows from the result of Problem 14.

To complete the solution, it is necessary to justify correctness of the definition of (c_k) and (d_k) by recurrence relations (55). As mentioned above, the sequence $s_n = n$ is Somos-4 and satisfies the recurrence equation $s_{n+2} s_{n-2} = 4 s_{n+1} s_{n-1} - 3 s_n^2$. It satisfies the relation (51) for $c_k = k^2$, $d_k = k^2 - 1$.Thus the elements of (c_k) and (d_k), calculated from (55) are rational and not identically zero functions of the parameters α, β, T. Thus algebraic independence of α, β and T provides that the elements of (c_k) and (d_k) (except $d_1 = 0$) don't vanish and hence in fact can be determined by (55).

Solution 49. The sequence (f_n) was constructed using (s_n). Thus the similar sequence (g_n) must also have a corresponding Somos−4 sequence that will be denoted by (w_n). The equality $g_k = w_{k-1} w_{k+1} / w_k^2$ implies that for given $g_k = d_k / c_k$ the elements of (w_n) are uniquely determined up to multiplication by a geometrical progression. The elements of (w_n) take the simplest form if we assume that $w_k^2 = c_k$,

$w_{k-1}w_{k+1} = d_k$ $(k = 1, 2, \ldots)$. Then for the initial conditions $w_0 w_2 = 0$, $w_1^2 = 1$, $w_2^2 = \alpha$ it is natural to choose the starting elements of the sequence as follows:

$$w_0 = 0, \quad w_1 = 1, \quad w_2 = -\sqrt{\alpha}. \tag{57}$$

The other elements are uniquely determined from the equality $w_{k-1}w_{k+1} = d_k$ $(k = 2, 3, \ldots)$. For instance,

$$w_3 = -\beta, \quad w_4 = \sqrt{\alpha}(\alpha^2 + T\beta), \quad w_5 = \beta^3 - \alpha^2(\alpha^2 + T\beta). \tag{58}$$

In termas of (w_n) the equality (51) takes the form

$$w_1^2 s_{n+k}s_{n-k} = w_k^2 s_{n+1}s_{n-1} - w_{k+1}w_{k-1}s_n^2, \tag{59}$$

which coincides with (13).

Solution 50. The formula (59) can be applied for instance to the sequence $s_n = w_n$. This implies (14).

Solution 51. Obviously it suffices to choose the initial conditions of the form

$$u_0 = 0, \quad v_0 = -1, \quad u_1 = 1, \quad v_1 = 0.$$

The coefficients obtained in Problem 15 lead to $u_2 = -\beta$, $v_2 = -(\alpha^2 + T\beta)$.

Introduce the new variables

$$G_k^{(n)} = \frac{s_{n+k+1}s_{n-k}}{s_n s_{n+1}}. \tag{60}$$

In particular, $G_0^{(n)} = 1$, $G_1^{(n)} = h_n$, $G_2^{(n)} = h_{n-1}h_nh_{n+1} = -\beta h_n + \alpha^2 + T\beta$. Now the equality (12) can be presented in the form

$$G_k^{(n)} = u_k h_n - v_k. \tag{61}$$

Since $G_{-k}^{(n)} = G_{k-1}^{(n)}$, for the proof of the lemma it suffices to determine (u_k) and (v_k) for nonnegative k and put $u_{-k} = u_{k-1}$, $v_{-k} = v_{k-1}$ $(k \geq 1)$.

To determine the coefficients u_{k+1}, v_{k+1} from the known values of u_{k-1}, v_{k-1}, u_k, v_k we use the equality

$$G_{k+1}^{(n)} = \frac{G_k^{(n-1)}G_k^{(n+1)}}{G_{k-1}^{(n)}}h_n$$

which follows from Definition (60). Transform this equality using (61):

$$(u_{k+1}h_n - v_{k+1})(u_{k-1}h_n - v_{k-1}) = (u_k h_{n-1} - v_k)(u_k h_{n+1} - v_k)h_n.$$

Using (35) and (29) (as well as the equality $J = T$ established in Problem 31) this equality is reduced to the form

$$h_n^2(u_{k+1}u_{k-1} - u_kv_k) - h_n(u_{k+1}v_{k-1} + u_{k-1}v_{k+1} - \beta u_k^2 - u_kv_kT + v_k^2) + \\ + (v_{k-1}v_{k+1} - u_k^2(\alpha^2 + T\beta) + u_kv_k\beta) = 0.$$

Setting the coefficients at various powers of h_n equal to 0, we obtain an *overdetermined* system of equations in variables u_{k+1}, v_{k+1} $(k \geq 2)$:

$$u_{k+1}u_{k-1} = u_kv_k, \tag{62}$$
$$u_{k+1}v_{k-1} + u_{k-1}v_{k+1} = \beta u_k^2 + u_kv_kT - v_k^2, \tag{63}$$
$$v_{k-1}v_{k+1} = u_k^2(\alpha^2 + T\beta) - u_kv_k\beta. \tag{64}$$

Solution 52. From the previous problem we get

$$u_0 = 0, \quad v_0 = -1, \quad u_1 = 1, \quad v_1 = 0, \quad u_2 = -\beta, \quad v_2 = -(\alpha^2 + T\beta),$$
$$u_3 = \beta(\alpha^2 + T\beta), \quad v_3 = \beta^3 + (\alpha^2 + T\beta)T\beta - (\alpha^2 + T\beta)^2 = \beta^3 - \alpha^2(\alpha^2 + T\beta).$$

Substitute the values u_{k+1} and v_{k+1} obtained from (62) and (64) into the equation (63) and divide by $u_k v_k$. We obtain a condition for consistency of the system

$$\xi_{k-1} + \xi_k - \beta\left(\frac{1}{\xi_{k-1}} + \frac{1}{\xi_k}\right) + \frac{\alpha^2 + T\beta}{\xi_{k-1}\xi_k} = T, \tag{65}$$

where $\xi_k = v_k/u_k$. In particular,

$$\xi_2 = \frac{\alpha^2 + T\beta}{\beta}, \qquad \xi_3 = \frac{\beta^3 - \alpha^2(\alpha^2 + T\beta)}{\beta(\alpha^2 + T\beta)};$$

the substitution into (65) shows that it is valid for $k = 3$.

Divide (64) by (62) to get a recurrence relation for the elements of (ξ_k):

$$\xi_{k-1}\xi_k\xi_{k+1} = -\beta\xi_k + (\alpha^2 + T\beta). \tag{66}$$

It coincides with the relation (35) for $\mu = -\beta$ and $\nu = \alpha^2 + T\beta$. Thus the formula (65) and, consequently, consistency of the system (62)–(64) follows from the solution of Problem 26.

Correctness of the recurrence relations (62) and (64) (absence of division by zero) is checked as in Problem 48.

Solution 53. The elements of (h_n) were obtained from the Somos-5 sequence (s_n) using the formula

$$h_n = f_n f_{n+1} = \frac{s_{n-1}s_{n+2}}{s_n s_{n+1}}. \tag{67}$$

However every resulting sequence (h_n) corresponds to some Somos-4 sequence. In fact by Problem 32 the sequence (s_n) can be transformed into a Somos-4 sequence by multiplying elements with even indices by a constant. This transformation does not change (h_n).

Thus to the sequence (ξ_n) there also corresponds a Somos-4 sequence. It occurs that this is (w_n) that was described in the solution of Problem 49. In fact for $k = 2, 3$ the equality $\xi_k = \frac{w_{k-1}w_{k+2}}{w_k w_{k+1}}$ is checked using formulas (57) и (58), and for $k \geq 4$ it follows from the coincidence of the recurrence relations (35) and (66) (here we use Problem 15, namely the fact that (w_n) is Somos-5 with coefficients $\mu = -\beta$ and $\nu = \alpha^2 + T\beta$).

Now it is not difficult to see that

$$u_k = \frac{w_k w_{k+1}}{w_1 w_2}, \qquad v_k = \frac{w_{k+2} w_{k-1}}{w_1 w_2}.$$

To check this, it suffices to observe that the equalities in question are valid for $k = 1, 2$, and to check that these equalities agree with (62)–(64). The equality (62) occurs to be an identity, (64) is the recurrence relation for the sequence (w_n) to be Somos-5, and (63) is the equality (37).

Thus the relation (12) takes the form

$$w_1 w_2 s_{n+k+1} s_{n-k} = w_k w_{k+1} s_{n+2} s_{n-1} - w_{k+2} w_{k-1} s_n s_{n+1}. \tag{68}$$

In particular, for $s_n = w_n$ we have

$$w_1 w_2 w_{n+k+1} w_{n-k} = w_k w_{k+1} w_{n+2} w_{n-1} - w_{k+2} w_{k-1} w_n w_{n+1}. \tag{69}$$

Solution 54. To begin with, consider the case $k + l + m + n \equiv 0 \pmod 2$. In terms of

$$a = \frac{k+l+m+n}{2}, \quad b = \frac{k+l-m-n}{2}, \quad c = \frac{k-l+m-n}{2}, \quad d = \frac{k-l-m+n}{2}, \tag{70}$$

the equality (15) takes the form

$$s_{a+b}s_{a-b}w_{c+d}w_{c-d} + s_{a+d}s_{a-d}w_{b+c}w_{b-c} - s_{a+c}s_{a-c}w_{b+d}w_{b-d} = 0. \tag{71}$$

To check this equality, it suffices to apply (59) or (14) to all products of the form $s_{x+y}s_{x-y}$ or $w_{x+y}w_{x-y}$ respectively.

Now consider the case $k+l+m+n \equiv 1 \pmod 2$. After replacement $k \to k+1$ the formula (15) takes the form

$$s_{k+l+1}s_{m+n}w_{k-l+1}w_{m-n} + s_{k+n+1}s_{l+m}w_{k-n+1}w_{l-m} - s_{k+m+1}s_{l+n}w_{k-m+1}w_{l-n} = 0, \tag{72}$$

where $k+l+m+n \equiv 0 \pmod 2$. The same replacement (70) enables us to present (72) in the form

$$s_{a+b+1}s_{a-b}w_{c+d+1}w_{c-d} + s_{a+d+1}s_{a-d}w_{b+c+1}w_{b-c} - s_{a+c+1}s_{a-c}w_{b+d+1}w_{b-d} = 0. \tag{73}$$

As in the preceding case, to complete the proof it suffices to apply (68) or (69) to all products of the form $s_{x+y+1}s_{x-y}$ or $w_{x+y+1}w_{x-y}$ respectively.

Remark. When we prove identities for Somos sequences, in fact we develop the theory of elliptic function using elementary language. One of important tools of this theory is Weierstrass σ-function. This is a function of complex argument, the two-dimensional analogue of sine. It vanishes at the nodes of a given lattice

$$\Lambda = \{x_1\omega_1 + x_2\omega_2 : x_1, x_2 \in \mathbb{Z}\},$$

where ω_1, ω_2 are two linearly independent vectors in the complex plane. The σ-function is defined by the infinite product

$$\sigma(z) = z \prod_{w \in \Lambda\setminus\{0\}} \left(1 - \frac{z}{w}\right) e^{\frac{z}{w} + \frac{z^2}{2w^2}}.$$

The equality (71) is the analogue of the Weierstrass three-term identity

$$\sigma(a+b)\sigma(a-b)\sigma(c+d)\sigma(c-d) - \sigma(a+c)\sigma(a-c)\sigma(b+d)\sigma(b-d) +$$
$$+\sigma(a+d)\sigma(a-d)\sigma(b+c)\sigma(b-c) = 0.$$

The general solution for the Somos-4 equation can be expressed in terms of the σ-function:

$$s_n = AB^n \frac{\sigma(z_0 + nz)}{\sigma(z)^{n^2}}.$$

In this formula, to the six parameters that determine a Somos-4 serquence there correspond the other six free parameters A, B, z, z_0 and the implicit parameters ω_1, ω_2. For (ψ_n) the formula is simpler:

$$\psi_n = \frac{\sigma(nz)}{\sigma(z)^{n^2}}.$$

Solution 55. Observe that the equality $s_n = (-1)^n\psi_{2n-3}$ holds for $n = 0, 1, 2, 3$. Thus the coincidence of the sequences would be proved if we check that $t_n = (-1)^n\psi_{2n-3}$ satisfy the same recurrence relation as Somos-(4).

The elements of (ψ_n) satisfy the equation (14) for $k = 2$, along with the initial conditions $\psi_0 = 0$, $\psi_1 = 1$. This yields that we can apply the formula (16). Replacing k, l, m and n by $2k+1$, 4, 2 and 0 respectively, we arrive to the equality

$$\psi_{2k+5}\psi_{2k-3}\psi_2\psi_{-2} + \psi_{2k+3}\psi_{2k-1}\psi_4^2 - \psi_{2k+1}^2\psi_6\psi_4 = 0.$$

For the variables $t_k = (-1)^n\psi_{2k-3}$ in this equality, substitute the values $\psi_2 = 1$, $\psi_4 = 1$, $\psi_6 = -1$ to get the required equation $t_{k+2}t_{k-2} = t_{k+1}t_{k-1} + t_k^2$.

Solution 56. Let us transform the equation (15) into the required recurrence relation. For this end, choose the parameters k, l, m, n equal to

$$\frac{1}{2}(an+b+3a), \quad \frac{1}{2}(an+b+a), \quad \frac{1}{2}(an+b-3a), \quad \frac{1}{2}(an+b-a)$$

respectively. We get the equation for Somos-4: $\tau_{n+2}\tau_{n-2}w_a w_{-a} + \tau_{n+1}\tau_{n-1}w_{2a}^2 - \tau_n^2 w_{3a}w_a = 0$.

Remark. One can obtain a different solution of this problems implementing methods from the previous section. For that purpose, it suffices to show that *any* arithmetical progression on an elliptic curve corresponds to a Somos-4 sequence.

Difficult problems

To these problems, we show either answers, or sketches of solutions. A curious reader may fill the details.

Solution 57. The equation for a Somos-6 sequence takes the following form in homogeneous variables:

$$f_{n+2}f_{n+1}^2f_n^3f_{n-1}^2f_{n-2} = \alpha f_{n+1}f_n^2f_{n-1} + \beta f_n + \gamma.$$

It has two independent invariants:

$$\begin{aligned}
T_1 =&\gamma(f_1f_2f_3 + f_2f_3f_4) + \beta f_1f_2f_3f_4 + \frac{\beta^2}{f_1f_2f_3f_4} + \frac{\gamma^2}{f_1f_2^2f_3^2f_4} + \\
&+ \alpha\gamma\left(\frac{1}{f_1f_2} + \frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \alpha\beta\left(\frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4}\right) + \frac{\beta\gamma}{f_1f_2f_3f_4}\left(\frac{1}{f_2} + \frac{1}{f_3}\right) = \\
=&\gamma(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5) + \beta(f_1f_2f_3f_4 + f_2f_3f_4f_5) + \alpha\gamma\left(\frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \alpha\beta\left(\frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4}\right), \\
T_2 =&\gamma f_1f_2^2f_3^2f_4 + \alpha\beta(f_1f_2 + f_2f_3 + f_3f_4) + \beta\gamma\left(\frac{1}{f_1f_2} + \frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + (\alpha^2\beta + \gamma^2)\left(\frac{1}{f_1f_2f_3} + \frac{1}{f_2f_3f_4}\right) + \\
&+ \alpha\gamma\left(\frac{f_1f_2}{f_4} + \frac{f_3f_4}{f_1}\right) + \alpha^2\gamma\left(\frac{1}{f_1f_2^2f_3} + \frac{1}{f_2f_3^2f_4}\right) + \frac{\alpha\beta^2}{f_1f_2^2f_3^2f_4} + \frac{\alpha\gamma^2}{f_1f_2^3f_3^3f_4} + \frac{\alpha\beta\gamma}{f_1f_2^2f_3^2f_4}\left(\frac{1}{f_2} + \frac{1}{f_3}\right) = \\
=&\gamma(f_1f_2^2f_3^2f_4 + f_2f_3^2f_4^2f_5) + \alpha\beta(f_1f_2 + f_2f_3 + f_3f_4 + f_4f_5) + \beta\gamma\left(\frac{1}{f_2f_3} + \frac{1}{f_3f_4}\right) + \\
&+ \alpha\gamma\left(\frac{f_1f_2}{f_4} + \frac{f_4f_5}{f_2}\right) + (\alpha^2\beta + \gamma^2)\frac{1}{f_2f_3f_4} + \alpha^2\gamma\frac{1}{f_2f_3^2f_4}.
\end{aligned}$$

Solution 58. Assume that the elements s_0, s_1, …, s_n of the Somos-(6) sequence are integers. Then in each triple (s_{k-2}, s_{k-1}, s_k) with $k = 2, \dots, n$ the numbers are coprime in total (if a prime p divides s_{k-2}, s_{k-1} and s_k then p divides s_{k-3} as well). Using the invariant T we have proved that any Somos-4 sequence satisfies a recurrence relation of order 5, and for the Somos-(6) there exist recurrence relations of orders 9, 10 и 11:

$$s_{n+5}s_{n-4} = -s_{n+4}s_{n-3} - s_{n+3}s_{n-2} + s_{n+2}s_{n-1} + 34s_{n+1}s_n, \tag{74}$$
$$s_{n+5}s_{n-5} = s_{n+4}s_{n-4} + 15s_{n+2}s_{n-2} - 19s_{n+1}s_{n-1} + 34s_n^2, \tag{75}$$
$$s_{n+5}s_{n-6} = s_{n+3}s_{n-4} + 19s_{n+2}s_{n-3} + 34s_{n+1}s_{n-2} + 19s_ns_{n-1}. \tag{76}$$

Suppose that s_0, s_1, …, s_{n+4} are integer. Then the condition $(s_{n-4}, s_{n-5}, s_{n-6}) = 1$ and the equalities (74)–(76) imply that s_{n+4} is integer as well.

Solution 59. In the preceding problem we have proved that any three consecutive elements of the Somos-(6) sequence are coprime in total. Hence for any p^γ at least one of the relations (74)–(76) enables us to determine $s_{n+5} \mod p^\gamma$ if we know the residues $s_{n-i} \mod p^\gamma$ for $i = -4, -3, \dots, 5, 6$. Since the residues are periodical, the sequence $(s_n \mod p^\gamma)$ is periodical as well. Since (74)–(76) enable us to determine not only subsequent but all preceding elements, the sequence $(s_n \mod p^\gamma)$ is entirely periodical. Hence it is periodical modulo any integer.

Solution 60. The Somos-7 equation has three independent invariants. First of these has the following form in the homogeneous variables f_k:

$$\begin{aligned}
\mathcal{H}_0 =&\beta f_1f_2f_3f_4f_5 + \gamma(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5) + \alpha\beta\left(\frac{1}{f_1} + \frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} + \frac{1}{f_5}\right) + \frac{\gamma^2}{f_1f_2^2f_3^3f_4^2f_5} \\
&+ \alpha\gamma\left(\frac{1}{f_1f_2f_3} + \frac{1}{f_2f_3f_4} + \frac{1}{f_3f_4f_5}\right) + \frac{\beta^2}{f_1f_2f_3f_4f_5} + \beta\gamma\left(\frac{1}{f_1f_2f_3^2f_4^2f_5} + \frac{1}{f_1f_2^2f_3^2f_4f_5}\right),
\end{aligned}$$

This invariant also has another presentation

$$\begin{aligned}
\mathcal{H}_0 =&\alpha\beta\left(\frac{1}{f_2} + \frac{1}{f_3} + \frac{1}{f_4} + \frac{1}{f_5}\right) + \alpha\gamma\left(\frac{1}{f_2f_3f_4} + \frac{1}{f_3f_4f_5}\right) + \\
&+\beta(f_1f_2f_3f_4f_5 + f_2f_3f_4f_5f_6) + \gamma(f_1f_2f_3 + f_2f_3f_4 + f_3f_4f_5 + f_4f_5f_6),
\end{aligned}$$

which shows that $\mathcal{H}_0 = F(f_1, f_2, f_3, f_4, f_5) + F(f_2, f_3, f_4, f_5, f_6)$, where

$$F(f_1, f_2, f_3, f_4, f_5) = \alpha\beta\left(\frac{1}{f_3} + \frac{1}{f_5}\right) + \frac{\alpha\gamma}{f_2 f_3 f_4} + \beta f_1 f_2 f_3 f_4 f_5 + \gamma\left(f_1 f_2 f_3 + f_3 f_4 f_5\right)$$

does not change when all indices are changed by 2.

To express two more invariants, it is suitable to use the variables $h_k = f_k f_{k+1}$:

$$\begin{aligned}
\mathcal{H}_1 =& \gamma h_1 h_2 h_3 h_4 + \alpha\beta\left(h_1 h_3 + h_1 h_4 + h_2 h_4\right) + \alpha\gamma\left(h_1 + h_2 + h_3 + h_4 + \frac{h_1 h_3}{h_4} + \frac{h_2 h_4}{h_1}\right)\\
&+ \alpha^2\beta\left(\frac{1}{h_1} + \frac{1}{h_2} + \frac{1}{h_3} + \frac{1}{h_4} + \frac{h_2}{h_1 h_3} + \frac{h_3}{h_2 h_4}\right) + \beta\gamma\left(\frac{1}{h_1} + \frac{1}{h_2} + \frac{1}{h_3} + \frac{1}{h_4}\right)\\
&+ \alpha^2\gamma\left(\frac{1}{h_1 h_2} + \frac{1}{h_2 h_3} + \frac{1}{h_3 h_4} + \frac{1}{h_1 h_3} + \frac{1}{h_2 h_4}\right) + \gamma^2\left(\frac{1}{h_1 h_3} + \frac{1}{h_2 h_4}\right) + \alpha\beta^2\left(\frac{1}{h_1 h_2 h_4} + \frac{1}{h_1 h_3 h_4}\right)\\
&+ \alpha\beta\gamma\left(\frac{2}{h_1 h_2 h_3 h_4} + \frac{1}{h_1 h_2^2 h_4} + \frac{1}{h_1 h_3^2 h_4}\right) + \alpha\gamma^2\left(\frac{1}{h_1 h_2^2 h_3 h_4} + \frac{1}{h_1 h_2 h_3^2 h_4}\right),\\
\mathcal{H}_2 =& \gamma\left(h_1 h_2 h_3 + h_2 h_3 h_4\right) + \alpha\beta\left(h_1 + h_2 + h_3 + h_4\right) + \alpha\gamma\left(\frac{h_1}{h_4} + \frac{h_4}{h_1}\right) + \alpha^2\beta\left(\frac{1}{h_1 h_3} + \frac{1}{h_2 h_4}\right)\\
&+ \beta\gamma\left(\frac{1}{h_1 h_2} + \frac{1}{h_2 h_3} + \frac{1}{h_3 h_4}\right) + \gamma\left(\alpha^2 + \gamma\right)\left(\frac{1}{h_1 h_2 h_3} + \frac{1}{h_2 h_3 h_4}\right) + \frac{\alpha\beta^2}{h_1 h_2 h_3 h_4}\\
&+ \alpha\beta\gamma\left(\frac{1}{h_1 h_2^2 h_3 h_4} + \frac{1}{h_1 h_2 h_3^2 h_4}\right) + \frac{\alpha\gamma^2}{h_1 h_2^2 h_3^2 h_4}.
\end{aligned}$$

Друзья бродят по графу

Проект представляют Бурсиан О., Кохась Д., Кохась К., Ретинский В.

В этой задаче мы рассматриваем конечные неориентированные графы без петель и кратных ребер. Если G — граф, то через $V(G)$ обозначается множество его вершин, $E(G)$ — множество ребер, $\delta(G)$ — минимальная степень вершины. Кроме того, мы используем стандартные обозначения графов: P_n — путь из n вершин, C_n — цикл из n вершин, $K_{m,n}$ — полный двудольный граф с долями по m и n вершин, граф $K_{1,n-1}$ будем называть *звездой* и обозначать $Star_n$. Вершина x_0 графа G называется *точкой сочленения*, если после ее удаления из графа G количество компонент связности в образовавшемся графе больше, чем в исходном. Связный граф без точек сочленения называется *двусвязным*. *Мост* — это ребро uv, при удалении которого граф распадается на две компоненты. Если ни одна из вершин u, v не является висячей вершиной графа G, будем называть мост *существенным*. Граф H называется *индуцированным* подграфом графа G, если $V(H) \subset V(G)$ и $E(H) = \{uv \in E(G) : u \in V(H), v \in V(H)\}$.

1 Игра в 15

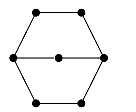
Головоломка «Игра в 15» была изобретена приблизительно 150 лет назад. Вы можете прочесть о ней в журнале Квант [1]. Там же приведено обобщение этой игры на произвольные графы (это обобщение мы тоже будем называть игрой в 15, хотя число вершин графа может быть произвольным, а не только 16) и доказана теорема Уилсона, которая описывает все графы, на которых игра в 15 «собирается».

Теорема Уилсона. Пусть дан граф G, который удовлетворяет четырем условиям:

1) он не является циклом C_n, $n \geqslant 4$, 2) не является двудольным,

3) не содержит точек сочленения, 4) не совпадает с графом «Θ» (см. рис. справа).

Тогда на графе G головоломка «15» собирается!

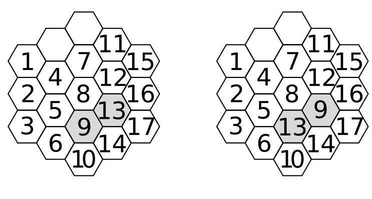


На самом деле Уилсон доказал несколько больше: если $G \neq \Theta$, $G \neq C_n$ — двусвязный двудольный граф, то в игре 15 на нем имеется два класса неэквивалентных перестановок. Если же $G = \Theta$, имеется 6 классов.

1.1. a) При $n > 3$ проверьте, что если $\delta(G) > n/2$, то на графе G головоломка «15» собирается.

b) Соберется ли игра «15» на произвольном связном графе с двумя пустыми вершинами?

1.2. Есть гексагональная доска со стороной n клеток, на ее клетках лежат шестиугольные плитки, пронумерованные натуральными числами. Две соседние клетки доски оставлены пустыми, благодаря чему плитки можно двигать. Две соседние по стороне плитки поменяли местами (см. пример на рисунке). Докажите, что при $n \geqslant 3$, двигая плитки, не удастся из первого положения получить второе.



Примечание. Чтобы подвинуть плитку a, рядом должны находиться две пустые клетки. Например, если они расположены справа от плитки a (см. левый рис.), мы можем подвинуть эту плитку вправо, пока она не упрется углом (рис. в центре), после чего ее можно сдвинуть вправо вверх или вправо вниз (рис. справа).

1.3. Докажите, что в игре в 15 на любом двусвязном графе G (где $|V(G)| \geqslant 3$) любую фишку удастся передвинуть в любую вершину графа.

1.4. В 100-вершинном графе G любой индуцированный подграф на 30 вершинах связен. Докажите, что существует такой 30-вершинный подграф в G, на котором игра «15» всегда собирается.

2 Друзья бродят по графу

Пусть имеется группа из n человек, некоторые из которых дружат, их отношение «дружба» описывается графом Y. Самих людей мы будем отождествлять с вершинами графа Y. И пусть дан еще один граф — граф X из n вершин, будем условно называть его «географическим», в его вершинах мы будем расставлять людей из компании $V(Y)$ — всегда по одному человеку в каждой вершине. Два человека, находящиеся в соседних вершинах графа X, могут поменяться местами, если они друзья. Такую операцию будем называть *обменом.* Построим новый граф $\mathsf{FS}(X,Y)$, вершины которого — это всевозможные расстановки людей на графе X, ребрами соединены расстановки, получающиеся друг из друга с помощью одной операции обмена. Формально говоря, *расстановка* людей на графе — это биекция $\tau\colon V(X)\to V(Y)$, которая для каждой вершины $u\in V(X)$ показывает, какой человек $\tau(u)\in V(Y)$ должен занять эту вершину. Будем говорить, что множество (всевозможных) расстановок людей на графе *связно*, если граф $\mathsf{FS}(X,Y)$ связен. Для любой расстановки людей в вершинах связного графа X будем говорить, что два человека $u,v\in Y$ образуют *перестановочную пару*, если существует цепочка обменов, в результате которой u и v поменяются местами, а все остальные останутся на прежних местах.

Если S — произвольное множество, то через $|S|$ мы обозначаем число элементов множества S.

2.1. Докажите, граф $\mathsf{FS}(X,Y)$ изоморфен графу $\mathsf{FS}(Y,X)$.

2.2. Докажите, что граф $\mathsf{FS}(X,Y)$ всегда двудольный.

2.3. Пусть X и Y — связные графы, $|V(X)|=|V(Y)|\geqslant 3$. Пусть x_0 — точка сочленения графа X и после ее удаления граф X распадается на компоненты $X_1,\ \dots,\ X_r$; y_0 — точка сочленения графа Y и после ее удаления граф Y распадается на компоненты $Y_1,\ \dots,\ Y_s$. Обозначим через $\mathcal{M}$ множество матриц $r\times s$ из неотрицательных целых чисел, в которых при всех i сумма элементов i-й строки равна $|V(X_i)|$, и при всех j сумма элементов j-го столбца равна $|V(Y_j)|$. Докажите, что число компонент связности графа $\mathsf{FS}(X,Y)$ не меньше чем количество таких матриц.

2.4. Докажите, что если для каждой расстановки людей на связном графе X любые два человека из Y, оказавшиеся в вершинах, соединенных ребром, образуют перестановочную пару, то граф $\mathsf{FS}(X,Y)$ связный.

2.5. Пусть X и Y — связные графы на n вершинах, при этом хотя бы у одного человека из Y не менее k друзей ($k\geqslant 2$), и каждый индуцированный k-вершинный подграф в X связен. Пусть одна из вершин X называется «угол», а какого-то человека из Y зовут Вася. Докажите, что для любой расстановки людей на графе X с помощью операций обмена Васю удастся поместить в угол.

Следующие задачи обобщают теорему об игре в 15.

2.6. a) Если графы X и Y двудольные на n вершинах ($n\geqslant 3$), то граф $\mathsf{FS}(X,Y)$ несвязный.

b) Пусть графы X и Y двудольные, $V(X)=A_X\cup B_X$, $V(Y)=A_Y\cup B_Y$ — разбиения их множеств вершин на доли. Докажите, что если две расстановки людей $\sigma,\tau\colon V(X)\to V(Y)$ находятся в одной компоненте связности графа $\mathsf{FS}(X,Y)$, то четность перестановки $\sigma^{-1}\circ\tau$ совпадает с четностью числа $|\tau(A_X)\cap A_Y|-|\sigma(A_X)\cap A_Y|$.

2.7. Докажите, что граф $\mathsf{FS}(K_{r,r},K_{r,r})$ имеет две компоненты связности.

2.8. Пусть двудольный граф X удовлетворяет условиям 1), 3), 4) теоремы Уилсона, граф Y — это граф «звезда» $K_{1,n}$, к которому добавлено одно ребро. Докажите, что граф $\mathsf{FS}(X,Y)$ связный.

2.9. Пусть X — граф, в котором $n\geqslant 4$ вершин. Докажите, граф $\mathsf{FS}(X,K_{2,n-2})$ связен тогда и только тогда, когда X — связный недвудольный граф без существенных мостов и $X\neq C_n$.

a) $\Rightarrow$ b) $\Leftarrow$

2.10. Пусть X и Y — связные графы на n вершинах, при этом хотя бы у одного человека из Y не менее k друзей ($k\geqslant 2$), и каждый индуцированный k-вершинный подграф в X связен. Пусть известно, что существует хотя бы один k-вершинный индуцированный подграф X_0 графа X, на котором игра в 15 собирается. Докажите, что граф $\mathsf{FS}(X,Y)$ связный.

2.11. Пусть X и Y — связные графы на n вершинах, и пусть $x_1,x_2,\dots,x_d$ ($d\geqslant 1$) — это «длинный мост» в X, т. е. путь в X, концы которого — точки сочленения, а все промежуточные вершины $x_2,\ \dots,\ x_{d-1}$ имеют степень ровно 2. Пусть $\delta(Y)\leqslant d$. Докажите, что граф $\mathsf{FS}(X,Y)$ несвязен.

3 Друзья ходят кругами

3.1. Пусть сначала друзья ходят по прямой. Дан граф Y — пятиугольник $ABCDE$ с диагоналями AC и AD. Сколько компонент связности имеет граф $\mathsf{FS}(P_5, Y)$?

Пусть дан граф $\overline{Y}$. Введем на нем ориентацию, задав направление каждого ребра. Ориентация α называется *ациклической*, если в результате не образовалось ни одного цикла. Если задана ориентация α, рассмотрим всевозможные расстановки вершин графа $\overline{Y}$ вдоль прямой (= в вершинах графа P_n), для которых все стрелки ведут слева направо. Множество таких расстановок обозначим через $\mathcal{L}(\alpha)$.

Следующая задача — это пример «математической зоологии». Если все аккуратно и правильно обозначено, то доказывать нечего.

3.2. Пусть $X = P_n$, $|V(Y)| = n$. Докажите, что для каждой ациклической ориентации α дополнительного графа $\overline{Y}$ множество $\mathcal{L}(\alpha)$ представляет собой компоненту связности графа $\mathsf{FS}(P_n, Y)$.

3.3. *Леденец* $L_{k,m}$ — это граф с $k + m$ вершинами, представляющий собой m-клику, к одной из вершин которой подвешен «хвост» (т.е. просто путь) из k вершин.

а) Пусть Y — граф на n вершинах, такой что граф $\mathsf{FS}(L_{n-m,m}, Y)$ связен. Докажите, что $\delta(Y) \geqslant n - m + 1$.

b) Пусть Y — граф на n вершинах. Докажите, что граф $\mathsf{FS}(L_{n-3,3}, Y)$ связен тогда и только тогда, когда $\delta(Y) \geqslant n - 2$.

c) Пусть $n > 4$, D_n — это путь P_{n-1}, вершины которого пронумерованы от 1 до $n - 1$, к которому добавлена вершина с номером n и ребро $(n - 2) - n$. (Этот граф получается из леденца $L_{n-3,3}$ удалением одного ребра на 3-цикле). Пусть Y — граф на n вершинах. Докажите, что граф $\mathsf{FS}(D_n, Y)$ связен тогда и только тогда, когда $\delta(Y) \geqslant n - 2$.

3.4. По кругу стоят $2n$ человек, образующих n супружеских пар. Соседи могут меняться местами, если они не супруги. Верно ли, что можно всех переставить в любом порядке? (Перестановки, отличающиеся циклическим сдвигом, считаются различными.)

3.5. По кругу стоит $3n$ человек — это n семей «мама–папа–ребенок». Любые два человека, стоящие рядом, могут поменяться местами, кроме случая, когда ребёнок меняется местом с одним из своих родителей (это не разрешено). При каких n с помощью таких обменов людей можно расставить по кругу в любом порядке? (Перестановки, отличающиеся циклическим сдвигом, считаются различными.)

3.6. Пусть $Y = K_{k,n-k}$. Сколько компонент связности имеет граф $\mathsf{FS}(C_n, Y)$?

3.7. Пусть $X = C_n$, $n \geqslant 3$, а дополнительный граф $\overline{Y}$ представляет собой какой-то связный граф на n вершинах. Докажите, что любые две расстановки, отличающиеся циклическим сдвигом, лежат в разных компонентах связности графа $\mathsf{FS}(C_n, Y)$, в частности, он имеет как минимум n компонент связности.

После промежуточного финиша

1.4. b) Пусть $n \geqslant 2k-1$ и граф G на n вершинах таков, что любой его индуцированный подграф на k вершинах является связным. Тогда среди индуцированных подграфов G на k вершинах найдется такой подграф G_0, что $\mathsf{FS}(G_0, Star_k)$ связный.

3.8. Пусть $X = C_n$, $n \geqslant 3$, а дополнительный граф $\overline{Y}$ представляет собой дерево. Докажите, что граф $\mathsf{FS}(C_n, Y)$ состоит ровно из n компонент связности, которые попарно изоморфны.

3.9. Пусть $X = C_n$, $n \geqslant 3$, а дополнительный граф $\overline{Y}$ представляет собой лес из деревьев T_1, T_2, …, T_r. Положим $\nu = \text{НОД}\big(|V(T_1)|, |V(T_2)|, \ldots, |V(T_r)|\big)$. Тогда граф $\mathsf{FS}(C_n, Y)$ состоит из ν компонент связности, которые попарно изоморфны и имеют по $n!/\nu$ вершин.

3.10. Пусть $X = C_n$, $n \geqslant 3$, а дополнительный граф $\overline{Y}$ представляет собой несколько компонент связности $\overline{Y}_1$, $\overline{Y}_2$, …, $\overline{Y}_r$. Положим $\nu = \text{НОД}\big(|V(Y_1)|, |V(Y_2)|, \ldots, |V(Y_r)|\big)$. Обозначим через $\mathsf{fs}(X, Y)$ количество компонент связности графа $\mathsf{FS}(X, Y)$. Докажите, что

$$\mathsf{fs}(C_n, Y) = \nu \prod_{i=1}^{r} \frac{\mathsf{fs}(C_{|V(Y_i)|}, Y_i)}{|V(Y_i)|}.$$

4 Гарантированная связность

Как мы видели, если графы X и/или Y имеют «мало» ребер, граф $\mathsf{FS}(X, Y)$ часто получается несвязным. Поставим такую задачу: найти (оценить) минимальное d_n, для которого любые n-вершинные графы X и Y, у которых $\delta(X) \geqslant d_n$, $\delta(Y) \geqslant d_n$, дают связный граф $\mathsf{FS}(X, Y)$. Чтобы избегать анализа «краевых эффектов», вы можете в своих решениях накладывать какие-либо арифметические ограничения на n (чтобы доказанная вами оценка работала пусть не для всех, но по крайней мере для бесконечно многих n). Задача 2.6 a) дает нам оценку $d_n \geqslant \frac{n}{2}$.

4.1. Докажите, что если графы X и Y содержат вершины степени не меньше $\frac{n}{2}$, то граф $\mathsf{FS}(X, Y)$ не имеет изолированных вершин.

4.2. Докажите, что $d_n \geqslant \frac{3}{5}n - 2$.

4.3. Пусть X и Y — связные графы, $\delta(X) \leqslant \delta(Y)$ и $\delta(X) + 2\delta(Y) \geqslant 2n$. Докажите, что граф $\mathsf{FS}(X, Y)$ связный.

Если в утверждении задачи 4.3 взять графы X и Y, для которых $\delta(X) = \delta(Y)$, мы получаем оценку сверху $d_n \leqslant \frac{2}{3}n + \text{const}$.

4.4. Докажите, что $d_n \leqslant \frac{3}{5}n + \text{const}$.

Для двудольных графов X и Y граф $\mathsf{FS}(X, Y)$ имеет не меньше двух компонент связности и можно поставить вопрос о минимальной степени вершины, которая гарантирует наличие ровно двух компонент. Пусть b_r — минимальное натуральное число, для которого любые два двудольных графа X и Y с долями по r вершин и $\delta(X) \geqslant b_r$, $\delta(Y) \geqslant b_r$, дают граф $\mathsf{FS}(X, Y)$ с двумя компонентами связности.

4.5. a) Докажите, что $b_r \geqslant \lceil \frac{3r+1}{4} \rceil$.

b) Найдите какое-нибудь $\alpha \in (0, 1)$, дающее оценку сверху $b_r \leqslant \alpha r$.

4.6. Пусть $r \geqslant 2$, а натуральные числа δ_1 и δ_2 удовлетворяют условиям

$$\delta_1 + \delta_2 = \left\lfloor \frac{3r}{2} \right\rfloor, \quad \delta_1 \leqslant r, \quad \delta_2 \leqslant r.$$

Докажите, что существуют двудольные графы X и Y с долями по r вершин и $\delta(X) = \delta_1$, $\delta(Y) = \delta_2$, для которых граф $\mathsf{FS}(X, Y)$ имеет больше двух компонент связности.

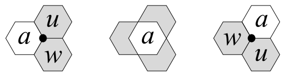
Решения

1 Игра в 15

1.1. a) Никто ведь не спрашивает, как она собирается. Просят проверить просто, что собирается. Она собирается по теореме Уилсона. Потому что граф со столь большими степенями вершин не является ни циклом, ни односвязным, ни двудольным, ни Θ.

b) Ответ: вообще говоря, нет. Если граф содержит k пустышек и «длинный мост» из k вершин, то не удастся поменять местами фишки из разных компонент.

1.2. Будем считать, что одна пустая клетка на самом деле накрыта «прозрачной» плиткой u, вторая пустая клетка — плиткой v, а при движении «настоящей» клетки a происходит циклический сдвиг: a занимает место u, u занимает место v, а v — место a.



Проверим, что если при движении плиток пустышки u и v вернулись на две исходные клетки, то каждая из них вернулась на свое исходное место (не могло быть так, что u и v поменялись местами).

Чтобы легко различать пустышки, будем рисовать вектор, идущий из центра клетки u в центр клетки v. Как видно из предыдущей картинки, при движении настоящей плитки происходит поворот этого вектора на $\pm 120°$. Для того чтобы пустышки поменялись местами, вектор должен повернуться на $180°$, очевидно, что этого не может произойти с помощью повторения операций поворота на $\pm 120°$.

Итак, мы установили, что если при движении плиток две настоящие плитки поменялись местами, а все остальные плитки вернулись на первоначальные места, то прозрачные плитки тоже вернулись на первоначальные места, и таким образом рассматриваемая перестановка — это транспозиция. Но транспозиция — это нечетная перестановка. Получить ее, последовательно выполняя 3-циклы, невозможно.

1.3. Решение 1. Пусть фишка стоит в вершине A_0, место, куда должна она попасть, — вершина A ($A_0, A \in G$). Так как G — связный, то в нем существует путь, связывающий эти две вершины, $A_0, A_1, A_2, \ldots, A_s = A$. Пусть пустышка стоит в вершине B_1 (B_1 может совпадать с вершинами $A_1, \ldots, A_s$). Так как граф G — двусвязный, то между парой вершин A_1 и B_1 есть два пути. На хотя бы одном из этих путей не стоит фишка. Проведем пустышку по этому пути в A_1, при этом плитки сдвинутся, но фишка останется на прежнем месте. Теперь поменяем местами фишку и пустышку, расстояние между фишкой и целью сократилось на один шаг, а пустышка стоит в вершине, которую мы обозначим B_2, при этом длина пути от фишки до цели уменьшилась на 1. Применим то же рассуждение для пары вершин A_2 и B_2 и так далее.

Решение 2 ([4, Lemma 3.1]). Если G — это цикл или Θ, утверждение очевидно. Если G не двудольный, то результат следует из теоремы Уилсона. Что касается двусвязных двудольных графов, уточненная теорема Уилсона утверждает, что там есть всего два класса неэквивалентных перестановок, которые различаются инвариантом

«четность суммы: четность всей перестановки плюс номер доли, где сидит пустышка».

Нетрудно построить такие две перестановки α и β, что в обеих пустышка сидит в одной и той же доле, а заданная фишка находится в нужной вершине, но значение инварианта для перестановок различно. Тогда для любой исходной перестановки мы сможем, двигая фишки, получить перестановку α или β, поскольку одна из них в том же классе эквивалентности, что и исходная.

1.4. a) Пункт a) это частный случай п. б) при $n = 100$, $k = 30$. Он имеет следующее совсем простое решение.

Наблюдение. Заметим, что у любой вершины степень не меньше $n-(k-1)$, иначе взяв эту вершину и $k-1$ не смежных с ней вершин, мы получим индуцированный граф с изолированной вершиной.

Это наблюдение почти сразу решает нам пункт а). Действительно, возьмем ребро ab и еще 28 вершин, смежных и с a, и с b. Нетрудно видеть, что индуцированный подграф на этих вершинах удовлетворяет теореме Уилсона.

Вот другое решение, найденное участниками.

По задаче 1.1 а) достаточно найти индуцированный подграф G_i на 30 вершинах с $\delta(G_i) > 15$. Предположим, что такого подграфа не существует, и оценим общее число антиребер в G сверху и снизу.

Как следует из наблюдения выше, у любой вершины графа G меньше 29 антиребер. Значит, всего количество антиребер в G меньше чем $29 \cdot 100/2 = 1450$ (сумма степеней вершин равна удвоенному количеству ребер).

Рассмотрим произвольный индуцированный подграф G' на 30 вершинах. Возьмем произвольную вершину A из G'. Так как мы предположили, что $\delta(G') \leqslant 15$, число антиребер внутри G', выходящих из вершины A, больше или равно 14. Выкинем эти антиребра. Теперь рассмотрим индуцированный подграф на тех же вершинах, но вместо A возьмем одну из 70 вершин, не принадлежащих G'. Получим еще 14 антиребер, которые тоже выкинем. И так сделаем для каждой из 70 вершин. Всего выкинули $14 \cdot 71$ антиребер, причем у каждого из них один конец лежит в множестве $V(G') \backslash \{A\}$. Теперь возьмем 70 вершин, не принадлежащих G', и отделим от них 30, на которых построим индуцированный подграф G''. Возьмем произвольную вершину A' из G''. Аналогично, число антиребер внутри G'' у A' больше или равно 14. Выкинем эти антиребра. Теперь рассмотрим индуцированный подграф на тех же вершинах из G'', но вместо A' возьмем одну из 40 вершин, не принадлежащих G' и G''. Получим еще 14 антиребер. И так сделаем для каждой из 40 вершин. Всего выкинули $14 \cdot 41$ антиребер. Итого, было выкинуто $14 \cdot 71 + 14 \cdot 41 = 1568$ антиребер, среди которых нет совпадающих. Противоречие.

б) Мы предлагаем два доказательства.

Доказательство 1. Поскольку $n \geqslant 2k - 1$, в силу наблюдения степень каждой вершины не меньше k. Рассмотрим произвольную вершину v и индуцированный граф на k смежных с ней вершинах. По условию этот граф связен. Мы можем удалить одну из вершин графа с сохранением связности (например удалив лист остовного дерева). Тогда на индуцированном графе, состоящем из вершины v и $k-1$ остальных вершин, игра «15» собирается. Действительно, этот граф очевидно удовлетворяет условиям 1), 2), 4) теоремы Уилсона. Точек сочленения он тоже не имеет, потому что вершина v смежна со всеми, а после удалении v граф остаётся связным по построению.

Доказательство 2 ([4, theorem 1.2]). Будем доказывать индукцией по ℓ, что G содержит подграф $G^{(\ell)}$, который является двусвязным и содержит треугольник K_3. Тогда граф $\mathsf{FS}(G^{(\ell)}, Star_\ell)$ — связный по теореме Уилсона ($3 \leqslant \ell \leqslant k$). При $\ell = k$ получим требуемое утверждение.

Сначала заметим, что поскольку любой индуцированный подграф на k вершинах в G связен, каждая вершина в G имеет степень по крайней мере $n - k + 1$. (В противном случае нашлась бы вершина, которая не связана ребрами с $k-1$ вершинами G, а значит, подграф, индуцированный на этой вершине и этих $k-1$ вершинах, не был бы связным).

Возвращаясь к теореме, докажем, что граф G содержит треугольник. Для этого, пользуясь наблюдением, оценим количество ребер в графе:

$$|E(G)| = \frac{1}{2}\sum_{i=1}^{n} d_i \geqslant \frac{1}{2}\, n(n-k+1) > \frac{n^2}{4}$$

(последнее неравенство после сокращения на n эквивалентно неравенству $n > 2k-2$). Тогда по теореме Турана G содержит треугольник, то есть K_3.

База индукции $\ell = 3$ доказана. Мы нашли подграф $G^{(3)} = K_3$, который содержит треугольник (то есть сам себя), не является двудольным и при этом граф $FS(K_3, Star_3)$ является связным (проверяется перебором).

Докажем индукционный переход. Согласно индукционному предположению существует граф $G^{(\ell-1)}$, который является подграфом G на $\ell - 1$ вершинах, двусвязен и содержит треугольник.

Пусть A — множество вершин подграфа $G^{(\ell-1)}$, а B — множество всех остальных вершин графа G, число ребер между A и B, обозначим через s. Докажем, что $s \geqslant n-\ell+2$. Если это уже сделано, то, так как $|B| = n-\ell+1$, по принципу Дирихле найдется вершина $v \in B$, имеющая хотя бы двух соседей в A. Тогда можно будет построить двусвязный индуцированный подграф $G^{(\ell)}$, добавив v к множеству вершин $G^{(\ell-1)}$. Он будет также содержать треугольник, тот же самый, что в $G^{(\ell-1)}$.

Итак, проверим, что $s \geqslant n-\ell+2$. Каждая вершина из A, как и любая вершина G, имеет степень не меньше $n-k+1$, следовательно, она имеет в множестве B хотя бы $n-k+1-(\ell-2)$ соседей. Значит,

$$s \geqslant (\ell-1)(n-k-\ell+3).$$

Нам осталось доказать, что $(\ell-1)(n-k-\ell+3) \geqslant n-\ell+2$. Обозначим

$$p(\ell) = -\ell^2 + (n-k+5)\ell - (2n-k+5).$$

После приведения подобных членов получается, что нужно доказать, что квадратный трехчлен $p(\ell)$ неотрицателен при $3 \leqslant \ell \leqslant k$. Это выполнено, так как

$$p(3) = -3^2 + 3(n-k+5) - (2n-k+5) = n-2k+1 \geqslant 0$$

и

$$\begin{aligned} p(k) = -k^2 + (n-k+5)k - (2n-k+5) \geqslant -k^2 + (2k-1-k+5)k - (2(2k-1)-k+5) = \\ = -k^2 + 2k^2 - k - k^2 + 5k - 4k + 2 + k - 5 = k-3 \geqslant 0. \end{aligned}$$

Отметим, что при $n = 2k-2$ утверждение теоремы неверно, контрпримером является полный двудольный граф $K_{k-1,k-1}$.

2 Друзья бродят по графу

2.1. В этом легко убедиться, если каждой вершине σ графа $\mathsf{FS}(X,Y)$ (напомним, что σ — это отображение из множества $V(X)$ в множество $V(Y)$), мы сопоставим вершину σ^{-1} (обратное отображение) графа $\mathsf{FS}(Y,X)$.

2.2. Отождествляя множества $V(X)$ и $V(y)$ с множеством натуральных чисел от 1 до n, мы получаем, что вершины графа $\mathsf{FS}(X,Y)$ естественно отождествляются с группой всех перестановок S_n. Тогда очевидно, что ребром соединяются перестановки разной четности.

2.3. [5, Proposition 2.6] Для расстановки $\sigma \in V(\mathsf{FS}(X,Y))$, где $\sigma(x_0) = y_0$. определим матрицу инцидентности $M(\sigma) = (m_{ij}(\sigma))$, полагая $m_{ij}(\sigma) = |\sigma(V(X_i)) \cap V(Y_j)|$. Ясно, что $M(\sigma) \in \mathcal{M}$. Для каждой из остальных расстановок τ подберем расстановку σ, полученную перестановкой $\tau(x_0)$ и y_0, и положим $M(\tau) = M(\sigma)$.

Достаточно проверить, что любые две расстановки σ и σ' лежат в разных компонентах графа $\mathsf{FS}(X,Y)$, если $M(\sigma) \neq M(\sigma')$. Допустим, что это не так и существует цепочка обменов, переводящая σ в σ'. Рассмотрим в этой цепочке две последовательные расстановки τ и τ', для которых впервые случилось, что $M(\tau) \neq M(\tau')$. Пусть перестановка τ' получается из τ обменом вершин y_1 и y_2. Заметим, что $y_1 \neq y_0$ и $y_2 \neq y_0$, и раз мы можем провести обмен, y_1 и y_2 смежны, а значит, лежат в одной компоненте Y_i. Но тогда $M(\tau')$ не может отличаться от $M(\tau)$.

2.4. [2, lemma 2.9] Пусть в графах X и Y по n вершин, тогда вершины графа $\mathsf{FS}(X,Y)$ естественно отождествляются с группой всех перестановок S_n. Каждое ребро (i,j) в графе X определяет транспозицию $(i\ j) \in S_n$, и условие задачи означает, что в графе $\mathsf{FS}(X,Y)$ любая вершина, т. е. перестановка $\sigma \in S_n$, соединена ребром с перестановкой $\sigma \circ (i\ j)$ (так мы обозначаем произведение перестановок, т. е. их последовательное выполнение в порядке справа налево). Следовательно, две вершины σ и σ' в графе $\mathsf{FS}(X,Y)$ лежат в одной компоненте связности, если существует последовательность транспозиций $(i_1\ j_1)$, $(i_2\ j_2)$, $\ldots$, $(i_k\ j_k)$, соответствующих ребрам графа X, такая что

$$\sigma' = \sigma \circ (i_1\ j_1) \circ (i_2\ j_2) \circ \cdots \circ (i_k\ j_k).$$

Таким образом, для доказательства утверждения задачи достаточно проверить, что любая перестановка из S_n есть произведение некоторого набора транспозиций, соответствующих ребрам графа X.

Это утверждение широко известно для случая $X = P_n$: любая перестановка представима в виде произведения транспозиций соседних элементов. Для произвольных связных графов можно ограничиться случаем когда X — дерево. Тогда это утверждение легко получается индукцией по числу вершин.

2.5. Мы доказываем следующую лемму ([4, lemma 3.2]).

Лемма. Пусть X — связный граф с максимальной степенью вершины $k \geqslant 2$, пусть Y — связный граф, любой индуцированный подграф которого на k вершинах является связным. Для любой вершины σ графа $FS(X,Y)$ и для любого $x \in V(X)$ и $y \in Y$ существует $\sigma' \in FS(X,Y)$, такая что $\sigma'(x) = y$ и σ' принадлежит той же компоненте связности $FS(X,Y)$, что и σ.

В терминах задачи x — это угол, y — это Вася, $\sigma(x)$ — это человек, стоящий в углу в расстановке σ (назовем его Кеша); возможность загнать Васю в угол означает наличие пути в графе $FS(X,Y)$, начало которого — это σ, а конец — такая расстановка, при которой Вася стоит в угле.

Если T — это остовное дерево графа X, то $FS(T,Y)$ является подграфом графа $FS(X,Y)$, поэтому достаточно доказать лемму для случая, когда X — дерево (в котором максимальная степень вершины равна k). Если Вася уже стоит в углу, т. е. $\sigma(x) = y$, то доказывать нечего, дальше считаем, что $\sigma(x) \neq y$.

Докажем лемму для случая, когда Кеша дружит с Васей, т. е. $(\sigma(x), y)$ является ребром в Y.

Применим индукцию по n. База $n = k+1$. В этом случае X — это граф-звезда, связность любого индуцированного подграфа в Y на k вершинах эквивалентна двусвязности Y. Тогда по утверждению задачи 1.3 получаем требуемое.

Индукционный переход. Пусть теперь $n \geqslant k+2$. Пусть c — вершина в дереве X максимальной степени k. Тогда в графе X всегда найдется такой лист u, что $u \neq c$ и u не является соседом вершины c. Рассмотрим три случая.

Случай 1. Пусть нашелся лист u, который не является углом и в котором стоит не Вася ($\sigma(u) \neq y$). Тогда отрежем лист u от графа X (новый граф назовем X'), он станет деревом на $n-1$ вершине, максимальная степень вершины в нем не изменится (так как мы не трогали вершину c и ее соседей). Уберем из графа Y человека, стоящего в листе (вершину $\sigma(u)$) вместе с ведущими в нее ребрами (новый граф назовем Y'), любой индуцированный подграф на k вершинах в Y' будет по прежнему связным. По индукционному предположению теорема выполнена для X' и Y'. Тогда последовательность дружеских обменов в графе $FS(X',Y')$ может рассматриваться как последовательность обменов в графе $FS(X,Y)$ (а человек в вершине u просто не будет двигаться).

Случай 2. Пусть этот лист и есть угол. Тогда объявим новым углом соседа этого листа, а старый угол удалим из графа X, а человека, в нем стоящего, (это Кеша) удалим из графа Y. Тогда опять можно отрезать лист и воспользоваться индукционным предположением. Вася встанет в вершину, соседнюю с углом, а так как он дружит с Кешей, то он просто поменяется с ним.

Случай 3. Пусть в этом листе u стоит Вася. Тогда возьмем одного из друзей Васи и будем считать его временно Васей, а новым углом считаем лист u. Тогда действуя, как в случае 2, мы загнали нового Васю в u. При этом старый Вася вынужден был покинуть вершину u, в ней теперь стоит друг Васи и дальше можно действовать, как в случае 1.

Индукционный переход доказан.

Если же Кеша не дружит с Васей, то в силу связности Y существует путь между Кешей и Васей, обозначим первого человека на этом пути Вася$_1$, второго — Вася$_2$ и так далее до Васи. Сначала загоним в угол Васю$_1$, который дружит с Кешей, потом Васю$_2$, который дружит с Васей$_1$ и так далее, пока там не окажется Вася.

2.6. a) [5, Proposition 2.7] Мы можем считать, что $V(X) = V(Y) = \{1, 2, \ldots, n\}$. Обозначим через A_X и B_X доли графа X, A_Y и B_Y доли графа Y. Тогда каждая расстановка людей на графе X — это просто элемент группы S_n. Для $\sigma \in S_n$ положим

$$p(\sigma) = |\sigma(A_X) \cap A_Y| + \frac{1}{2}(\operatorname{sgn}(\sigma) + 1).$$

Проверим, что четность этой величины не меняется при выполнении операции обмена.

Действительно, если два человека $u \in A_Y$ и $v \in B_Y$ меняются местами, то они расположены в вершинах из разных долей графа X. При этом u переходит из одной доли в другую, значит, величина $|\sigma(A_X) \cap A_Y|$ изменяется на 1. Четность перестановки σ в результате этой транспозиции меняется на противоположную, в результате чего значение дроби $\frac{1}{2}(\operatorname{sgn}(\sigma) + 1)$ тоже изменяется на 1.

Отметим, что приведенный инвариант — это естественное обобщение инварианта, решающего головоломку «Игра в 15».

b) [2, Proposition 2.5] Пусть расстановка τ получается из расстановки σ с помощью последовательности обменов $(a_1\ b_1)$, $\ldots$, $(a_\ell\ b_\ell)$, где a_1, a_2, $\ldots$, $a_\ell \in A_X$ и b_1, b_2, $\ldots$, $b_\ell \in B_X$. Положим $\sigma_0 = \sigma$, $\sigma_i = \sigma_{i-1} \circ (a_i\ b_i)$ при $i = 1$, $\ldots$, ℓ. Тогда имеем телескопическую сумму

$$|\tau(A_X) \cap A_Y| - |\sigma(A_X) \cap A_Y| = \sum_{i=1}^{\ell} \bigl(|\sigma_i(A_X) \cap A_Y| - |\sigma_{i-1}(A_X) \cap A_Y|\bigr).$$

Достаточно проверить, что каждое слагаемое этой суммы равно ± 1, тогда четность всей суммы совпадает с $\operatorname{sgn}(\sigma^{-1} \circ \tau) = \operatorname{sgn}\bigl((a_1\ b_1) \circ \ldots \circ (a_\ell\ b_\ell)\bigr)$. Эта проверка аналогична проверке из п. a).

2.7. Как мы знаем из предыдущей задачи, граф $\mathsf{FS}(K_{r,r}, K_{r,r})$ имеет не меньше двух компонент. Мы докажем, что их ровно две, показав, что произвольная расстановка фишек может быть приведена с помощью обменов к одному из двух стандартных видов. Будем считать, что доли наших графов покрашены в черный и белый цвет, а вершины каждой доли пронумерованы. Рассмотрим произвольную расстановку фишек на графе. Пусть в черных вершинах стоит s черных фишек $(0 \leqslant s \leqslant r)$ и $(r-s)$ белых, тогда в белых вершинах стоит s белых и $(r-s)$ черных фишек. С помощью обменов поменяем местами $(r-s)$ черных фишек, стоящих в белых вершинах, и $(r-s)$ белых фишек, стоящих в черных. В результате все черные фишки будут стоять в черных вершинах, а белые — в белых.

Будем говорить, что черные и белые фишки находятся в стандартном порядке, если при всех i i-я черная фишка находится в i-й черной вершине, а i-я белая — в i-й белой.

Далее мы попробуем переставить фишки так, чтобы они расположились в стандартном порядке. Для этого будем систематически применять следующие цепочки обменов. Пусть a и b — номера двух черных фишек. Хитрым обменом назовем следующую цепочку обменов, в которых кроме упомянутых черных фишек участвуют первая и вторая белые фишки: $a1$, $b2$, $a2$, $b1$. В результате хитрого обмена черные фишки a и b поменялись местами (белые фишки тоже поменялись, но нас пока не интересует это обстоятельство).

Пользуясь хитрыми обменами, расположим все черные фишки в стандартном порядке. Теперь будем применять аналогичные обмены к белым фишкам — в результате обмена выбранные белые фишки a и b поменяются местами, а кроме того, первая и вторая черная фишка тоже поменяются местами. Пользуясь хитрыми обменами, расположим все белые фишки в стандартном порядке. Мы получили расстановку, в которой все фишки находятся в стандартном положении, кроме, быть может, первой и второй черных фишек (они могут стоять «наоборот»).

Утверждение задачи взято в [2, Proposition 2.6], где доказывается более общий факт, утверждающий что граф $\mathsf{FS}(K_{r,n-r}, K_{s,n-s})$, где $1 \leqslant r \leqslant n-1$, $2 \leqslant s \leqslant n-2$, состоит из двух компонент связности.

2.8. [5, Remark 2.8] Уточненная теорема Уилсона утверждает, что граф $\mathsf{FS}(X, K_{1,n-1})$ состоит из двух компонент. В этом случае компоненты различаются инвариантом из решения задачи 2.6 a).

Но если к графу $K_{1,n-1}$ добавить одно ребро uv и расставить людей на графе X так, чтобы u и v стояли в смежных вершинах, то можно выполнить транспозицию $(u\ v)$, изменяющую четность инварианта. В результате две компоненты склеятся в одну.

2.9. [6, theorem 1.4] а) Пусть граф $\mathsf{FS}(X, K_{2,n-2})$ связен. Ясно, что тогда граф X тоже связен. Граф X не может быть двудольным в силу результата задачи 2.6 а). Граф X не может быть циклом, поскольку в этом случае число компонент связности велико и подсчитано в задаче 3.6. Наконец, если в графе X есть существенный мост uv, при удалении которого граф распадается на две компоненты, вершины из разных компонент, не совпадающие с u и v, не смогут поменяться местами (это очевидно, если рассматривать на графе игру «15» с двумя пустышками).

б) Обозначим людей из двухэлементной доли $K_{2,n-2}$ через P_1 и P_2. При перемещении человека P_i по графу X будем обозначать через p_i (переменную) вершину, в которой находится P_i.

Лемма 1. P_1 и P_2 образуют перестановочную пару.

Доказательство. Поскольку X — не двудольный граф, в нем есть цикл нечетной длины $2k+1$. Достаточно научиться менять местами P_1 и P_2, когда они находятся в соседних вершинах этого цикла. Возьмём вершину P_1 и проведём её по циклу, чтобы она оказалась в соседней вершине по другую сторону от P_2 (остальные люди при этом сдвинулись вдоль цикла на 1). Теперь возьмём вершину P_2 и проведём её по циклу, чтобы она оказалась в соседней вершине по другую сторону от P_1 (остальные люди при этом сдвинулись вдоль цикла ещё на 1). Совершив $2k+1$ таких транспозиций мы получим, что P_1 иP_2 поменялись местами, а все остальные люди вернулись на свои места. □

Благодаря лемме 1 можно считать, что вершины P_1 и P_2 в графе Y соединены ребром, а также, что P_1 и P_2 образуют перестановочную пару с любым соседом в X. В частности можно считать, что на графе X происходит игра в 15 с двумя пустышками.

Лемма 2. 1) Игра в 15 на цикле с висячей вершиной и двумя пустышками собирается.

2) Игра в 15 на цикле с двумя висячими вершинами и двумя пустышками собирается.

Доказательство. Эти утверждения очевидны каждому, кто хоть немного поиграл в игру в 15. □

Чтобы доказать, что граф $\mathsf{FS}(X, K_{2,n-2})$ связен, достаточно проверить, что в любой расстановке σ любые два человека A и B, стоящие в вершинах a и b, соединённых ребром в X, образуют перестановочную пару.

Если $\{A, B\} \cap \{P_1, P_2\} \neq \varnothing$, утверждение очевидно. В противном случае поскольку в X нет существенных мостов, ребро ab лежит в каком-то цикле. Рассмотрим такой цикл $C_{a,b}$ минимально возможной длины. Поскольку граф X связен, существует путь от вершины p_1 до цикла $C_{a,b}$. С помощью цепочки обменов передвинем P_1 по этому пути, пока P_1 не окажется в вершине, смежной с a или b, или попадёт на цикл $C_{a,b}$. Аналогично переместим P_2, пока P_2 не окажется в вершине, смежной с a, b или p_1, либо попадёт на цикл $C_{a,b}$. В результате возможны следующие варианты расположения вершин a, b, p_1, p_2.

1) Эти четыре вершины находятся на цикле $C_{a,b}$.

2) Одна из вершин p_1 или p_2 лежит на цикле $C_{a,b}$, а другая смежна с циклом.

3) Обе вершины p_1 и p_2 смежны с циклом $C_{a,b}$.

4) Вершины p_1 и p_2 лежат не на цикле, p_1 соединена с a или b ребром r, а p_2 смежна с p_1.

Последний случай сводится к двум предыдущим: если вершина p_1 смежна и a, и с b, возьмем треугольник abp_1 вместо цикла $C_{a,b}$ и получим случай 2. Иначе поскольку r — не существенный мост, найдется путь от p_1 до цикла $C_{a,b}$, не проходящий через ребро r. Проведём P_1 по кратчайшему такому пути, пока p_1 не попадет на цикл или не станет смежной с a или с b, а P_2 поставим на освободившееся от P_1 место — получится расположение из случая 2 или 3.

В случаях 2 и 3 по лемме 2 получаем, что (A, B) — перестановочная пара.

В случае 1 добавим к циклу abc торчащее из него ребро (оно существует, так как граф X — не цикл, а цикл $C_{a,b}$ выбирался с условием минимальности) и опять воспользуемся леммой 2. Итак, мы переставляем A и B местами, после чего возвращаем остальных персонажей обратной цепочкой обменов к расстановке σ.

2.10. Теорема ([4, theorem 1.1]). Пусть X — связный граф на n вершинах и максимальная степень его вершин равна $k \geqslant 2$. Пусть Y — связный граф на n вершинах, любой его индуцированный подграф на k вершинах связен и существует такой его индуцированный подграф Y_0, что граф $\mathsf{FS}(Star_k, Y_0)$ является связным. Тогда граф $\mathsf{FS}(X, Y)$ — связный.

Если T — это остовное дерево графа X, то $\mathsf{FS}(T, Y)$ является подграфом графа $\mathsf{FS}(X, Y)$, поэтому достаточно доказать теорему для случая, когда X — дерево.

Применим индукцию по n. База $n = k + 1 > 3$. (При $n = 3$ утверждение проверяется непосредственно.) В этом случае граф X — это звезда, связность любого индуцированного подграфа в Y на k вершинах эквивалентна двусвязности Y. Поскольку $\mathsf{FS}(Star_k, Y_0)$ — связный граф, то Y не может быть циклом или Θ. Также в силу связности графа $\mathsf{FS}(Star_k, Y_0)$ граф Y_0 не может быть двудольным, а следовательно, и Y тоже не двудольный. Поэтому по теореме Уилсона $\mathsf{FS}(Star_n, Y)$ — связный граф.

Индукционный переход. Пусть теперь $n \geqslant k+2$. Пусть c — вершина в дереве X максимальной степени k. Тогда в графе X всегда найдется такой лист x, что $x \neq c$ и x не является соседом вершины c. Возьмем любую вершину $y \in V(Y) \setminus V(Y_0)$. Пусть τ — вершина графа $\mathsf{FS}(X, Y)$, для которой $\tau(x) = y$ (т. е. эта расстановка ставит человека y в вершину x). Теперь рассмотрим произвольную вершину $\mathsf{FS}(X, Y)$, расстановку σ, и докажем, что между этими вершинами есть путь, это и будет означать требуемое утверждение.

По утверждению задачи 2.5 существует расстановка σ', такая что $\sigma(x) = y$ и при этом есть путь между σ' и σ в графе $\mathsf{FS}(X, Y)$. Удалим лист x из X и вершину y из Y, назовем новые графы X' и Y', они удовлетворяют условию теоремы. Тогда по индукционному предположению существует путь между $\sigma'|_{X'}$ и $\tau|_{X'}$ в графе $\mathsf{FS}(X', Y')$. На него можно смотреть как на путь в графе $\mathsf{FS}(X, Y)$. Осталось дополнить его путем из σ' в σ.

2.11. Поскольку добавление ребер в Y не может привести к потере связности графа $\mathsf{FS}(X, Y)$, достаточно разобрать случай, когда $\delta(Y) = d$. Пусть y_0 — вершина графа Y степени d, а y_1, …, y_d — ее соседи. Поскольку x_1 и x_d — точки сочленения графа X, найдутся две вершины: x_0, соседняя с x_1, и x_{d+1}, соседняя с x_d, кратчайший путь между которыми проходит по длинному мосту. При удалении из графа X длинного моста эти вершины окажутся в разных компонентах связности, обозначим через R множество вершин компоненты, в которой находится x_0.

Рассмотрим расстановки $\sigma, \sigma' \colon V(X) \to V(Y)$, для которых $\sigma(x_0) = y_0$, $\sigma'(x_{d+1}) = y_0$. Мы утверждаем, что эти расстановки лежат в разных компонентах связности графа $\mathsf{FS}(X, Y)$. Это кажется очевидным: чтобы человек y_0 переместился из вершины x_0 в x_{d+1}, он должен пройти по длинному мосту, сделав при этом не меньше $d + 1$ обмена, что превышает его коммуникативные возможности.

Для строгого обоснования предположим, что мы применяем некоторую цепочку обменов к расстановке σ. Проверим, что при выполнении каждого очередного обмена выполняется одно из двух свойств:

1) человек y_0 находится в компоненте R

2) человек y_0 находится в некоторой вершине x_i ($1 \leqslant i \leqslant d$) и при этом не менее i из вершин y_1, …, y_d находятся в множестве $R \cup \{x_1, \ldots, x_{i-1}\}$.

В частности свойство 2) при $i = d$ означает, что y_0 не может перейти из вершины x_d в x_{d+1}, поскольку все его друзья находятся «по другую сторону» от ребра $x_d x_{d+1}$.

Проверка выполнения свойств 1, 2) делается перебором вариантов, какие из вершин затронуты очередным обменом. Мы не будем ее здесь приводить, желающие могут прочесть ее в статье [5, Theorem 6.1], из которой мы взяли эту задачу.

3 Друзья ходят кругами

3.1. Ответ: 8 компонент связности.

Считаем, что граф $X = P_5$ нарисован на горизонтальной прямой. Граф Y содержит ребра между любыми двумя вершинами, кроме ребер DB, BE и EC. Для каждого из этих ребер *назначим*, в каком порядке вдоль прямой (слева направо) расположены его концы. Например, постановим, что D левее B, E левее B, C правее E. Всего имеется 8 вариантов таких назначений. Очевидно, что при обменах назначенные взаиморасположения вершин измениться не могут.

Для каждого назначения приведем любую расстановку расстановку людей, удовлетворяющую этому назначению, к стандартной форме следующего вида. Поскольку на обмены с A ограничения отсутствуют, поставим A на самое левое место. Далее, на обмены с C есть одно ограничение — если это «C правее E», ставим C на самое правое место, а если «C левее E» — на самое левое свободное место, т. е. на второе слева место, так как на первом стоит A. Теперь аналогично поступаем с D: если «D левее B», ставим D как можно левее (самые левые места могут занимать A и C), а если «D правее B», ставим D как можно правее. Что касается вершин B и E, они сами по себе заняли места, подчиняясь последнему ограничению.

Таким образом, количество компонент связности графа $\mathsf{FS}(P_5, Y)$ равно количеству назначений.

3.2. [5, theorem 3.1] Рассмотрим расстановку на графе P_n из множества $\mathcal{L}(\alpha)$. Если человек A стоит левее B и от A к B ведет стрелка (значит, A и B не дружат), то при совершении обменов A всегда будет находиться левее B. Поэтому все расстановки, получающиеся из рассматриваемой расстановки с помощью обменов, лежат в $\mathcal{L}(\alpha)$. Таким образом, $\mathcal{L}(\alpha)$ есть объединение нескольких компонент связности графа $\mathsf{FS}(P_n, Y)$.

Проверим, что на самом деле для каждого графа Y и каждой ациклической ориентации α графа $\overline{Y}$ множество $\mathcal{L}(\alpha)$ состоит всего лишь из одной компоненты связности графа $\mathsf{FS}(P_n, Y)$. Для этого убедимся в том, что любые две расстановки из $\mathcal{L}(\alpha)$ получаются друг из друга с помощью обменов. Это делается спуском по количеству изолированных вершин графа $\overline{Y}$.

База: граф $\overline{Y}$ состоит из n изолированных вершин — тривиальна.

Индукционный переход $k \to k-1$. Пусть $\overline{Y}_{k-1}$ — граф на n вершинах, имеющий $k-1$ изолированных вершин. Пусть α_{k-1} — произвольная ациклическая ориентация графа $\overline{Y}_{k-1}$. Пусть $u \in V(\overline{Y}_{k-1})$ — сток (имеет хотя бы одно входящее ребро и ни одного выходящего). Обозначим через $\overline{Y}_k$ граф, получающийся из $\overline{Y}_{k-1}$ удалением всех ребер, ведущих в вершину u, а через α_k — ациклическую ориентацию $\overline{Y}_k$, заданную оставшимися ребрами. Ээээ, дальше очевидно.

3.3. а) Сразу следует из задачи 2.11.

б) [5, Corollary 6.3] Необходимость неравенства $\delta(Y) \geqslant n-2$ следует из п. а). Достаточность легко доказывается индукцией по n.

с) Если $\delta(Y) \leqslant n-3$, то по результатам предыдущих пунктов несвязен даже граф $\mathsf{FS}(L_{n-3,3}, Y)$, в котором больше свободы для перемещения людей.

Пусть $\delta(Y) \geqslant n-2$. Тогда $\delta(\overline{Y}) \leqslant 1$, т. е. $\overline{Y}$ — это набор изолированных ребер и изолированных вершин. Люди, соответствующие изолированным вершинам, могут перемещаться по графу D_n, меняясь местами с соседями без всяких ограничений. Люди, соответствующие ребрам, могут свободно передвигаться по графу D_n, за исключением возможности непосредственно поменяться местами друг с другом, но мы можем осуществить их обмен, загнав обоих в «тупиковые» $(n-1)$-ю и n-ю вершины, и «доставая» их оттуда в нужном порядке. В результате мы всегда можем поставить первого человека в первую вершину, после чего индукционным рассуждением расставить остальных. База проверяется при $n = 5$ (При $n = 4$ утверждение неверно).

Более формальное доказательство можно прочесть в статье [5, Theorem 6.5], из которой взято утверждение задачи.

3.4. Ответ: нет.

Разорвем круг в любом месте и в образовавшейся шеренге подсчитаем число супружеских пар, в которых жена стоит левее мужа. Четность этой величины не меняется при перестановках.

3.5. О т в е т: таких n не существует. На самом деле тут имеется три класса эквивалентных расстановок. Но мы проверим лишь то, что существует инвариант, принимающий три значения.

Будем считать, что люди стоят в шеренгу (двух крайних при этом считаем соседями). Определим вес каждой семьи: рассмотрим, как эти трое стоят в шеренге, если ребенок стоит первым, полагаем вес равным 1, если вторым — 2, если третьим — 0. Нетрудно проверить, что при выполнении операций смены мест суммарный вес семей по модулю 3 не меняется. В частности, из любой расстановки нам не удастся получить расстановку, где ребенок поменялся с одним из родителей, а все остальные люди остались на тех же местах.

3.6. [6, Lemma 2.7] О т в е т: Граф $\mathsf{FS}(C_n, K_{k,n-k})$ имеет НОД$(k, n-k)\cdot(k-1)!(n-k-1)!$ компонент связности.

Пусть A и B — это доли графа $K_{k,n-k}$, а e — фиксированное ребро цикла. Очевидно, что при несовпадающих парах циклических упорядочений множеств A и B расстановки лежат в разных компонентах графа $\mathsf{FS}(C_n, K_{k,n-k})$. Таких пар имеется $(k-1)!(n-k-1)!$. Расстановки с одинаковой парой циклических упорядочений множеств A и B разобьём на $k(n-k)$ множеств, определяемых парой («первая по часовой стрелке от e вершина из A», «первая против часовой стрелки от e вершина из B»). Каждое из этих множеств лежит в одной компоненте связности графа $\mathsf{FS}(C_n, K_{k,n-k})$ — расстановки из этих множеств получаются друг из друга с помощью обменов, не затрагивающих ребро e, это фактически проверяется в задаче 3.2. С помощью обменов через ребро e совокупность этих множеств можно разбить на классы по НОК$(k, n-k)$ множеств в каждом (потому что дружеский обмен на ребре e сдвигает оба элемента пары на 1 по циклу). Поскольку имеется $k(n-k)$ множеств, мы получаем НОД$(k, n-k)$ классов.

3.7. Д о к а з а т е л ь с т в о 1 ([5, Proposition 4.4]). Допустим, что существует расстановка людей σ, из которой с помощью цепочки обменов удается получить расстановку σ_k, где все люди (циклически) сдвинулись на k по часовой стрелке ($1 \leqslant k \leqslant n-1$). Зададим вес каждому человеку: пусть в расстановке σ вес каждого равен нулю, при сдвиге человека на одну позицию по часовой стрелке вес увеличивается на 1, а при сдвиге против часовой стрелки — уменьшается на 1. Тогда в расстановке σ_k вес каждого человека сравним с k по модулю n, в частности, вес не будет равен 0. Поскольку каждый обмен изменяет вес одного человека на 1, а другого на -1, суммарный вес всех людей в расстановке σ_k остался равен 0. Следовательно, часть людей имеет положительный вес, а часть — отрицательный. Обозначим через Y^+ множество людей в расстановке σ_k, имеющих положительный вес, а через Y^- — множество людей в расстановке σ_k, имеющих отрицательный вес. Ясно, что при выполнении обменов любой человек $y^+ \in Y^+$ и любой человек $y^- \in Y^-$ должны были совершить обмен. Значит, каждый человек из Y^+ дружит с каждым человеком из Y^-. Но это противоречит связности графа $\overline{Y}$, поскольку $Y^+ \cup Y^- = V(Y)$.

Д о к а з а т е л ь с т в о 2. Разорвём круг в любом месте, а также перенумеруем людей числами от 1 до n. Для каждой расстановки людей рассмотрим ациклическую ориентацию α графа $\overline{Y}$: каждое ребро ориентируем от левого человека к правому. Весом ориентированного ребра $e : a \to b$ назовём количество вершин графа $\overline{Y}$ после удаления ребра e в компоненте связности, содержащей вершину a. *Весом* ациклической ориентации $w(\alpha)$ графа $\overline{Y}$ будем называть сумму весов всех ориентированных рёбер, которые идут от человека с меньшим номером к человеку к бóльшим номером.

Тогда при любом обмене, кроме обмена друзей на первом и n-м местах, ациклическая ориентация, а, следовательно, и её вес не меняются.

Л е м м а. Если в ациклической ориентации α выбрать сток v и изменить направление всех рёбер, входящих в v, то для веса полученной ориентации α' верно сравнение $w(\alpha') \equiv w(\alpha) - 1 \pmod{n}$.

Доказательство. Пусть $a_1, \ldots, a_s$ и $b_1, \ldots, b_r$ — вершины, соединённые с v, причём $a_i < v < b_j$. Обозначим через c_i и d_j веса рёбер $v \to a_i$ и $v \to b_j$ соответственно. Тогда при изменении ребра $v \to a_i$ оно учитывалось с весом c_i, а станет учитываться с весом 0. А ребро $v \to b_i$ учитывалось с весом 0, а станет — с весом $n - d_i \equiv -d_i \pmod n$. В итоге суммарно вес изменится на

$$c_1 + \dots c_s + d_1 + \dots + d_r = n - 1 \equiv -1 \pmod n.$$

$\square$

Таким образом, при обменах друзей, стоящих на первом и n-м местах один сток превращается в исток, а один исток — в сток. По лемме первое превращение вычтет 1 из веса, второе — прибавит 1, в результате вес ориентации по модулю n сохраняется.

Наконец, при циклическом сдвиге на k мест по очереди k стоков превращаются в истоки. Следовательно, вес ориентации изменится на k, и получится расстановке, не эквивалентная исходной.

3.8. Условие задачи взято из [5, Proposition 4.4]. Мы приводим более простое решение.

Пронумеруем людей из Y числами от 1 до n. Докажем, что произвольную расстановку людей на C_n можно привести к *стандартной* расстановке, где, начиная с первого человека, все люди стоят по возрастанию по часовой стрелке (в какой именно вершине находится первый человек, мы при этом не отслеживаем). Это утверждение доказывается индукцией по n. База для $n = 3$ очевидна. Для перехода от $n - 1$ к n рассмотрим висячую вершину K графа $\overline{Y}$, и, «притворившись что её не существует», расставим оставшиеся $n - 1$ вершин по возрастанию. Это делается с помощью цепочки перестановок, которая существует по предположению индукции. Если в процессе перестановок соседям K (стоящим по обе стороны от K) требуется поменяться местами, применим «ТРЮК»: сначала поменяем K с тем из соседей, с которым K дружит (это возможно, поскольку K — висячая вершина в $\overline{Y}$, и значит, ей запрещено меняться лишь с одной из остальных вершин). Теперь, когда все вершины, кроме K, стоят по возрастанию, приведем K на своё место, двигая ее либо по, либо против часовой стрелки. Таким образом, любую расстановку можно привести обменами к стандартной. Заметим, что все расстановки по возрастанию отличаются циклическими сдвигами и по задаче 3.7 являются представителями различных компонент связности графа $\mathsf{FS}(C_n, Y)$.

3.9. Мы взяли это утверждение в [5, Corollary 4.12.], но предлагаем более элементарное решение.

Пронумеруем людей из Y, причем людям из T_i выдадим номера от $\left(\sum_{j=1}^{i-1} |V(T_j)|\right) + 1$ до $\sum_{j=1}^{i} |V(T_j)|$. Назовем расстановку людей *стандартной*, если, начиная с первого человека, все люди стоят по возрастанию номеров по часовой стрелке. В какой именно вершине цикла находится первый человек, мы всё ещё не отслеживаем. Таким образом, располагая людей по циклу и внося какие-либо изменения в их циклический порядок, мы допускаем, что в результате проводимых обменов могут происходить циклические сдвиги всей конфигурации. Отметим еще, что в стандартной расстановке все вершины каждого множества T_i стоят по кругу подряд.

Аналогично решению задачи 3.8 докажем, что произвольную расстановку людей на цикле C_n можно привести к *стандартной* расстановке. Действительно, мы можем дословно повторить рассуждения задачи 3.8, мысленно достроив $\overline{Y}$ до дерева. Заметим однако, что теперь некоторые циклические сдвиги стандартной расстановки могут лежать в одной компоненте. Если мы последовательно проведём $n - |V(T_i)|$ обменов против часовой стрелки для каждой вершины множества T_i, начиная с наименьшего по номеру и идя по возрастанию номеров (заметим, что любые два человека из разных компонент T_i и T_j всегда могут меняться местами), мы получим стандартную расстановку циклически сдвинутую на $|V(T_i)|$ позиций по часовой стрелке. Оперируя сдвигами такого типа, мы можем получить сдвиг на любую целочисленную комбинацию $\sum \alpha_i |V(T_i)|$. Поскольку ν является такой целочисленной комбинацией, в графе $\mathsf{FS}(C_n, Y)$ не более ν компонент.

Теперь докажем, что количество компонент не меньше ν. Рассмотрим стандартную расстановку σ и получаемую из неё цепочкой обменов расстановку σ_k, где все люди (циклически) сдвинулись на k по часовой стрелке. Зададим вес каждому человеку: пусть в расстановке σ вес каждого человека равен нулю, при сдвиге человека на одну позицию по часовой стрелке его вес увеличивается на 1, а при сдвиге против часовой стрелки — уменьшается на 1. Тогда в расстановке σ_k вес каждого человека сравним с k по модулю n, а сумма всех весов равна 0. Более того, у людей, соединённых ребром в $\overline{Y}$, веса одинаковые. Отсюда нетрудно получить, что для всех i все вершины множества T_i имеют одинаковый вес, пусть этот вес равен $\alpha_i n + k$. Запишем в этих обозначениях, что сумма всех весов равна 0:

$$\sum_{i=1}^{r}\Big(|V(T_i)|(\alpha_i n + k)\Big) = 0$$

или, эквивалентно,

$$k\sum_{i=1}^{r}|V(T_i)| = -\sum_{i=1}^{r}\Big(|V(T_i)|\alpha_i n\Big).$$

Поскольку $\sum|V(T_i)| = n$, последнее равенство можно записать в виде

$$kn = -n\sum_{i=1}^{r}|V(T_i)|\alpha_i$$

Сократив обе части равенства на n, получим что k — целочисленная комбинация чисел $|V(T_i)|$, а значит, k кратно ν.

3.10. Для связного графа Y определим граф $\mathsf{FS}'(Y)$. Вершины этого графа совпадают с вершинами графа $\mathsf{FS}(C_{|V(Y)|}, Y)$. Две вершины σ и τ соединены ребром, если они соединены в графе $\mathsf{FS}(C_{|V(Y)|}, Y)$, или же эти две расстановки отличаются циклическим сдвигом. Тогда любая расстановка и все её циклические сдвиги лежат в одной компоненте связности графа $\mathsf{FS}'(Y)$, но, как следует из задачи 3.7, в разных компонентах связности графа $\mathsf{FS}(C_{|V(Y)|}, Y)$. Следовательно, граф $\mathsf{FS}'(Y)$ состоит ровно из $\dfrac{\mathsf{fs}(C_{|V(Y)|}, Y)}{|V(Y)|}$ компонент связности.

Оценка снизу. Во-первых, посмотрим на всех людей из $V(Y_i)$ и выпишем их в порядке обхода цикла C_n по часовой стрелке, начиная с кого-нибудь. Получится расстановка людей из компоненты Y_i по циклу. Заметим, что компонента связности полученной расстановки в графе $\mathsf{FS}'(Y_i)$ не зависит от начала обхода и не меняется при обменах, а потому является инвариантом для каждого i.

Во-вторых, из решения задачи 3.9 следует, что если взять произвольную расстановку людей из графа Y по циклу и провернуть её на $0, 1, \ldots, \nu-1$ позиций, то получить эти ν расстановок друг из друга с помощью дружеских обменов невозможно. Таким образом, у нас имеется r инвариантов: компоненты связности соответствующих расстановок в графе $\mathsf{FS}'(Y_i)$, и для каждого выбора этих инвариантов найдется не менее ν попарно неэквивалентных расстановок. Следовательно,

$$\mathsf{fs}(C_n, Y) \geqslant \nu\prod_{i=1}^{r}\frac{\mathsf{fs}(C_{|V(Y_i)|}, Y_i)}{|V(Y_i)|}.$$

Оценка сверху. Покажем, что если компоненты связности соответствующих расстановок в графе $\mathsf{FS}'(Y_i)$ фиксированы, то неэквивалентных расстановок не более ν. Делается аналогично задаче 3.9.

4 Гарантированная связность

4.1. Пусть $a \in V(X)$, $A \in V(Y)$ — вершины степени не меньше $\frac{n}{2}$. Пусть $\sigma\colon V(X) \to V(Y)$ — произвольная расстановка людей. т. е. вершина графа $\mathsf{FS}(X, Y)$. Докажем, что в графе $\mathsf{FS}(X, Y)$ вершина σ не изолированная. Обозначим через U множество людей, стоящих в соседних с a вершинах графа X, тогда $U \subset V(Y)\setminus\{A\}$, $|U| \geqslant \frac{n}{2}$. И пусть W — множество друзей A, тогда $W \subset V(Y)\setminus\{A\}$, $|W| \geqslant \frac{n}{2}$. Ясно, что множества U и W пересекаются, т.е. существует человек B, который является другом A и стоит в соседней с A вершине. Это значит, что для расстановки σ возможен обмен AB.

4.2. [2, Proposition 5.1] Построим графы X и Y, у которых множество вершин — это множество чисел от 1 до n. Для удобства считаем, что n делится на 5. Разобьем множество чисел от 1 до n на пять непересекающихся подмножеств A_1, A_2, A_3, A_4, A_5. Ребра в графах X и Y зададим следующим образом. Пусть $x \in A_i$, $y \in A_j$ и $x \neq y$. В графе X вершины x и y соединим ребром только если $i - j \not\equiv \pm 2 \pmod 5$, а в графе Y эти вершины соединены ребром только в случае $i - j \not\equiv \pm 1 \pmod 5$. Как нетрудно видеть, все вершины имеют степень $\frac{3}{5}n - 1$. Проверим, что граф $\mathsf{FS}(X, Y)$ несвязный.

Рассмотрим множество расстановок людей, при которой люди из каждой части $A_i \subset V(Y)$ занимают в каком-то порядке вершины, заданные той же частью $A_i \subset V(X)$. Для любой такой расстановки дружеский обмен двух человек u и v возможен только лишь в случае, когда оба принадлежат одной и той же части $A_i \subset V(Y)$. В результате такого обмена получится расстановка из того же множества расстановок.

Если же n не делится на 5, следует выбрать «почти» равные части A_i, и тогда приведенное рассуждение даст чуть худшую оценку $d_n \geqslant \frac{3}{5}n - 2$.

4.3. Решение 1 ([3, theorem 1.5]). Рассмотрим произвольную расстановку людей на графе X и возьмем двух произвольных человек U и V, стоящих в соседних вершинах u и v. Докажем, что U и V образуют перестановочную пару. По утверждению задачи 2.4 отсюда следует, что граф $\mathsf{FS}(X, Y)$ связный.

Рассмотрим подграф в X, состоящий из вершины u, всех ее соседей и ребер, соединяющих u с соседними вершинами, обозначим этот подграф $Star$. Пусть $Q \subset V(Y)$ — это множество людей, стоящих в вершинах графа $Star$. Обозначим через Y_Q индуцированный подграф в Y на множестве вершин Q. Докажем, что $\delta(Y_Q) > \frac{1}{2}|Q|$. Для этого возьмем вершину $y \in Q$ минимальной степени (в графе Y_Q) и проверим, что ее степень больше $\frac{1}{2}|Q|$. Обозначим через $N(y)$ множество друзей y в графе Y. Тогда степень вершины y в графе Y_Q равна

$$\delta(Y_Q) = |N(y) \cap Q| = |N(y)| + |Q| - |N(y) \cup Q| \geqslant |N(y)| + |Q| - n.$$

Таким образом, достаточно проверить, что $|N(y)| + |Q| - n > \frac{1}{2}|Q|$ или, эквивалентно,

$$2|N(y)| + |Q| > 2n.$$

Это так, поскольку $|N(y)| \geqslant \delta(Y)$, $|Q| \geqslant \delta(X) + 1$.

Итак, $\delta(Y_Q) > \frac{1}{2}|Q|$. Тогда по утверждению задачи 1.1 а) на графе Y_Q собирается игра «15». Это значит, что граф $\mathsf{FS}(Y_Q, Star)$ связный! Но тогда и граф $\mathsf{FS}(Star, Y_Q)$ тоже связный, значит пользуясь дружескими связями из графа Y_Q и ребрами графа $Star$ мы сможем поменять местами U и V. Эта цепочка обменов выполнима и в более широких графах X и Y, т.е. вершины U и V образуют перестановочную пару.

Решение 2. Воспользуемся симметричностью графа $\mathsf{FS}(X, Y)$: покажем, что если X и Y — связные графы, $\delta(Y) \leqslant \delta(X)$ и $2\delta(X) + \delta(Y) \geqslant 2n$, то граф $\mathsf{FS}(X, Y)$ связный. Для этого достаточно проверить условие задачи 2.10. Возьмём $k = \delta(Y)$ и проверим, что каждый индуцированный k-вершинный подграф в X связен. Из каждой вершины графа X максимум $n - k$ рёбер ведёт вне индуцированного подграфа. А поэтому степень каждой вершины индуцированного подграфа $\delta(X) - (n - \delta(Y)) \geqslant \frac{\delta(X)}{2}$ не менее половины числа вершин подграфа, поэтому индуцированный подграф связен.

Далее проверим условие наличия k-вершинного подграфа X_0, на котором игра 15 собирается. Заметим, что во втором доказательстве задачи 1.4 б мы доказали более сильный факт: если в графе X каждый индуцированный k-вершинный подграф в X связен, а степень каждой вершины не меньше k, то среди индуцированных подграфов на k вершинах найдется такой подграф $_0$, котором игра «15» собирается. Воспользовавшись этим утверждением, мы заканчиваем проверку условий задачи 2.10, которая утверждает, что граф $\mathsf{FS}(X, Y)$ связный.

4.4. Этот результат доказан в [3, theorem 1.4].

4.5. a) [2, Proposition 6.1] Считаем, что r делится на 4. Построим двудольные графы X и Y, имеющие по r вершин в каждой доле. Пусть A_X, B_X, C_X, D_X — попарно непересекающиеся множества, состоящие из $\frac{r}{2}$ элементов каждое. Пусть множества $A_X \cup B_X$ и $C_X \cup D_X$ будут долями графа X. Аналогично зададим $A_Y \cup B_Y$ и $C_Y \cup D_Y$ — доли графа Y. Зафиксируем произвольную биекцию $\sigma\colon V(X) \to V(Y)$, для которой $\sigma(A_X) = A_Y$, $\sigma(B_X) = B_Y$, $\sigma(C_X) = C_Y$, $\sigma(D_X) = D_Y$.

Зададим множество ребер графа X. Каждую вершину A_X соединим с каждой вершиной C_X, а каждую вершину B_X соединим с каждой вершиной D_X. Между вершинами из множеств A_X и D_X проведем лишь половину всех возможных ребер — так, чтобы из каждой вершины множества A_X выходило $\frac{r}{4}$ ребер и в каждую вершину множества D_X входило $\frac{r}{4}$ ребер. Это нетрудно сделать.

Теперь зададим множество ребер графа Y. Каждую вершину A_Y соединим с каждой вершиной множества B_Y, а каждую вершину C_Y соединим с каждой вершиной D_Y. Между вершинами из множеств A_Y и D_Y проведем лишь половину всех возможных ребер, находящихся в «противофазе ребрам графа X относительно биекции σ», а именно: вершины $u \in A_Y$ и $v \in D_Y$ соединены ребром в том и только том случае, когда в графе X вершины $\sigma^{-1}(u)$ и $\sigma^{-1}(v)$ НЕ соединены. Аналогично вершины $s \in B_Y$ и $t \in C_Y$ соединены ребром в том и только том случае, когда в графе X вершины $\sigma^{-1}(s)$ и $\sigma^{-1}(t)$ не соединены.

В результате все вершины графов X и Y имеют степень $\frac{3}{4}r$. Проведенная конструкция гарантирует, что σ — изолированная вершина графа $\mathsf{FS}(X,Y)$. Тогда в силу утверждения задачи 2.6, граф $\mathsf{FS}(X,Y)$ имеет не меньше трех компонент связности.

В случае, когда r не делится на 4, следует взять множества A_X, D_X, состоящие из $\lceil\frac{r}{2}\rceil$ вершин, и множества B_X, C_X, состоящие из $\lfloor\frac{r}{2}\rfloor$ вершин, а также надлежащим образом поправить однородность: из каждой вершины A_X должно выходить $\left\lfloor\frac{\lceil r/2\rceil}{2}\right\rfloor$ ребер к вершинам части D_X и в каждую вершину множества D_X входит столько же ребер; а между частями B_X, C_X — по $\left\lfloor\frac{\lfloor r/2\rfloor}{2}\right\rfloor$ ребер из каждой вершины. Тогда степени всех вершин построенных графов будут не меньше $\lceil\frac{3r+1}{4}\rceil - 1$.

b) Пусть r делится на 8. Докажем оценку $b_{r,r} \leqslant \frac{7}{8}r + 1$. Нам понадобится следующее «двудольное» обобщение задачи 2.4.

Лемма 1. Пусть X и Y — двудольные графы с долями по r вершин и любые два человека из разных долей графа Y, находящиеся в разных долях графа X, образуют перестановочную пару. Тогда граф $\mathsf{FS}(X,Y)$ содержит ровно две компоненты.

Доказательство. Это так, потому что условие леммы предоставляет нам такую же свободу в обмене людей, как если бы речь шла о графе $\mathsf{FS}(K_{r,r}, K_{r,r})$, который, как мы знаем из задачи 2.7, имеет две компоненты. $\square$

Лемма 2. Пусть X — граф, получающийся из графа $K_{3,3}$ с долями $\{x_1, x_3, x_5\}$ и $\{x_2, x_4, x_6\}$ удалением ребер x_1x_2 и x_5x_6, и Y — граф, получающийся из графа $K_{3,3}$ с долями $\{y_1, y_3, y_5\}$ и $\{y_2, y_4, y_6\}$ удалением ребер y_1y_2 и y_5y_6. Пусть $\sigma\colon V(X) \to V(Y)$ — «тождественная» расстановка $x_i \mapsto y_i$. Тогда вершины y_1 и y_2 графа Y образуют перестановочную пару. То же утверждение верно для расстановки σ' которая переводит вершины x_1, x_2, ..., x_6 соответственно в y_1, y_2, y_4, y_3, y_6, y_5.

Доказательство. Для расстановки σ подойдет последовательность обменов

$$y_1y_6,\ y_3y_4,\ y_3y_6,\ y_2y_5,\ y_4y_5,\ y_5y_6,\ y_2y_5,\ y_2y_3,\ y_1y_6,\ y_1y_4,\ y_3y_4.$$

Расстановка σ' легко сводится к σ. $\square$

Для доказательства утверждения задачи достаточно проверить, что при $b_r = \frac{7}{8}r + 1$ графы X и Y удовлетворяют лемме 1. Рассмотрим двух человек из разных долей Y_1 и Y_2 графа Y, находящиеся в разных долях X_1 и X_2 графа X. Обозначим этих людей y_1 и y_2, а вершины, в которых они стоят, обозначим x_1 и x_2. Докажем, что в графе X можно так выбрать еще четыре вершины x_3, x_4, x_5, x_6, и в графе Y — четырех человек y_3, y_4, y_5, y_6, что подграфы, определяемые этими вершинами, удовлетворяют лемме 2. Это будет означать, что y_1 и y_2 образуют перестановочную пару, что нам и требуется.

Рассмотрим людей, стоящих в вершинах доли $X_1 \setminus \{x_1\}$. Пусть не меньше $\frac{r}{2}$ из них принадлежат множеству Y_1, обозначим множество этих людей через $\widetilde{Y}_1$. Тогда не меньше $\frac{r}{2}$ человек, находящихся в вершинах из множества $X_2 \setminus \{x_2\}$, принадлежат множеству Y_2, обозначим множество этих людей через $\widetilde{Y}_2$. Поскольку из вершин x_1, y_1 выходит не более $\frac{r}{8} - 1$ антиребер, мы сможем выбрать $\frac{r}{4}+2$ вершины из $\widetilde{Y}_2$, так что выбранные люди дружат с y_1 и находятся при этом в вершинах графа X, соединенных с x_1. Нам на самом деле не нужно столько народу, достаточно того, что можно выбрать одного человека, обозначим его y_4, а вершину, где он стоит, — x_4. Теперь, поскольку из вершин y_2, y_4, x_2 и x_4 выходит не более $\frac{r}{8} - 1$ антиребер, мы сможем выбрать 4 вершины из $\widetilde{Y}_1$, так что выбранные люди дружат с y_2 и y_4 и находятся при этом в вершинах графа X, соединенных с x_2 и x_4. Здесь нам опять достаточно того, что мы можем выбрать одного человека (а не четырех), обозначим его y_3, а вершину, где он стоит, — x_3. Далее аналогично мы выберем человека $y_6 \in \widetilde{Y}_2 \setminus \{y_2\}$, который дружит с y_1, y_3, а стоит в вершине x_6, соединенной с x_1 и x_3. И наконец, аналогично выберем человека $x_5 \in \widetilde{Y}_1 \setminus \{x_3\}$, который дружит с y_2 и y_4, а стоит в вершине x_5, соединенной с x_2 и x_4. Мы получили требуемую конфигурацию.

Если в рассуждении в начале предыдущего абзаца не меньше $\frac{r}{2}$ человек принадлежат множеству Y_2, мы, действуя аналогично, придем ко второй расстановке из леммы 2.

В статье [2, Proposition 6.2] доказана оптимальная оценка $b_{r,r} \leqslant \lceil \frac{3r+2}{4} \rceil$.

4.6. Этот результат доказан в [3, theorem 1.11].

Список литературы

[1] Кохась К. Игра в 15. // Квант, 2022, №5. С. 14–20.

[2] Alon N., Defant C., Kravitz N. Typical and Extremal Aspects of Friends-and-Strangers Graphs. https://arxiv.org/abs/2009.07840

[3] Bangachev K. On the Asymmetric Generalizations of Two Extremal Questions on Friends-and-Strangers Graphs. arXiv:2107.06789v1

[4] Defant C., Dong D., Lee A., Wei M. Connectedness and cycle spaces of friends-and-strangers graphs. arXiv:2209.01704v1

[5] Defant C., Kravitz N. Friends and strangers walking on graphs. arXiv:2009.05040v2

[6] Wang L., Lu J., Chen Y. Connectedness of friends-and-strangers graphs of complete bipartite graphs and others. arXiv:2302.00900

Friends wander on graph

Project team: O. Bursian, D. Kokhas, K. Kokhas, V. Retinskiy

In this problem we consider finite undirected graphs without loops and multiple edges. If G is a graph, then we denote by $V(G)$ the set of its vertices and by $E(G)$ the set of its edges, denote by $\delta(G)$ the minimum degree of its vertex. Besides that, we use standard graph notation: P_n is the path with n vertices, C_n is the cycle with n vertices, $K_{m,n}$ is the complete bipartite graph with parts of sizes m and n, a graph $K_{1,n-1}$ is called a *star* and is denoted by $Star_n$. A vertex x_0 of graph G is called a *cut vertex*, if the number of components of connectivity increases when we remove this vertex from graph G. Connected graph without cut vertices is called *biconnected*. A *bridge* is an edge uv, whose removal would disconnect the graph. If none of vertices u, v is a leaf vertex of graph G, we call the bridge *essential*. Graph H is called *induced* subgraph of graph G, if $V(H) \subset V(G)$ and $E(H) = \{uv \in E(G) : u \in V(H), v \in V(H)\}$.

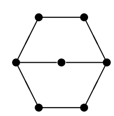
1 15-puzzle

15-puzzle has been invented approximately 150 years ago. You can read about it in journal [?], where a generalization of this game to arbitrary graphs is given (this generalization we also call 15-puzzle, though the number of graph vertices may be arbitrary, not only 16) and Wilson's theorem is proved, which describes all the graphs, on which 15-puzzle is solvable.

Wilson's theorem. Let graph G satisfies the following four conditions:

1) it is not cycle C_n, $n \geqslant 4$, 2) it is not bipartite,

3) it does not contain cut vertices, 4) it does not coincide with graph «Θ» (see fig. to the right).



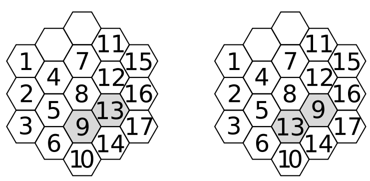
Then 15-puzzle on graph G is solvable!

Actually Wilson proved a stronger statement: if $G \neq \Theta$, $G \neq C_n$ is biconnected bipartite graph, then in 15-puzzle on this graph there exist exactly two classes of nonequivalent permutations. And for $G = \Theta$ there are 6 classes.

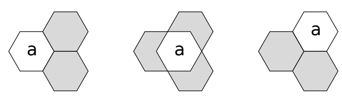
1.1. a) Check that if $\delta(G) > n/2$, then 15-puzzle is solvable on graph G.

b) Is 15-puzzle solvable on an arbitrary graph if we allow two empty vertices?

1.2. Hexagonal pieces numbered by positive integers are placed on the cells of a hexagonal board with side n. Two adjacent cells are left empty, and thanks to it some pieces can be moved. Two pieces with common sides exchanged places (see an example in the figure). Prove that if $n \geqslant 3$ the second arrangement cannot be obtained from the first one by moving pieces.



Note. Moving a piece a requires two adjacent empty cells. For instance, if they are on the right of a (left figure), a can be moved right till it touches an angle (middle figure), and then it can be moved upward right or downward right (right figure).



1.3. Prove that for any biconnected graph G (where $|V(G)| \geqslant 4$) any tile may be moved to any graph vertex in 15-puzzle on G.

1.4. In 100-vertex graph G any induced subgraph on 30 vertices is connected. Prove that there exists a 30-vertex subgraph of G, for which 15-puzzle is always solvable.

2 Friends wander on the graph

Let a group of n people be given, any two of them are friends or strangers, which people are friends with each other is encoded in a graph Y. And let another one graph X on n vertices be given, we call it «geographic» conditionally, the people of company $V(Y)$ are standing at its vertices, always one person is at each vertex. Two friends standing at adjacent vertices of graph X, may swap places. Such operation is called *friendly swap*. Construct a new graph $\mathsf{FS}(X,Y)$, whose vertex set is the set of all possible people arrangements on graph X, the two arrangements are connected by edge, if they are obtained from each other by one swap operation. Speaking more formally, people *arrangement* on graph X is the bijection $\tau\colon V(X)\to V(Y)$ that for each vertex $u\in V(X)$ shows, which person $\tau(u)\in V(Y)$ has to occupy this vertex. We say that the set of all possible people arrangements on graph X is *connected*, if graph $\mathsf{FS}(X,Y)$ is connected. For any people arrangement at vertices of connected graph X we say that two persons $u,v\in Y$ are an *exchangeable pair*, if there exists a sequence of swaps, as a result of which u and v swap their places, and all the others are on the previous places.

If S is an arbitrary set, we denote by $|S|$ the number of the elements of set S.

2.1. Prove that graph $\mathsf{FS}(X,Y)$ is isomorphic to graph $\mathsf{FS}(Y,X)$.

2.2. Prove that graph $\mathsf{FS}(X,Y)$ is always bipartite.

2.3. Let $|V(X)|=|V(Y)|\geqslant 3$. Let x_0 be a cut vertex of graph X and graph X falls into components $X_1,\ldots,X_r$ after removing it; y_0 be a cat vertex of graph Y and graph Y falls into components $Y_1,\ldots,Y_s$ after removing it. Let $\mathcal{M}$ be the set of $r\times s$ matrices with non-negative integer entries in which the i-th row sums to $|V(X_i)|$, and j-th column sums to $|V(Y_j)|$. Prove that the number of connected components of graph $\mathsf{FS}(X,Y)$ is at least the number of such matrices.

2.4. Prove that if for each people arrangement on graph X any two persons of Y located at adjacent vertices form an exchangeable pair, then graph $\mathsf{FS}(X,Y)$ is connected.

2.5. Let X and Y be connected graphs on n vertices, and at least one person of Y has at least k friends ($k\geqslant 2$), and each induced k-vertex subgraph of X is connected. Let one of the vertices of X be called «corner», and some person of Y have name Vasya. Prove that for any people arranegment on graph X Vasya can be placed in the corner by friendly swaps.

The following problems generalize the theorem about 15-puzzle.

2.6. a) If X and Y are bipartite graphs on n vertices ($n\geqslant 3$), then graph $\mathsf{FS}(X,Y)$ is disconnected.

b) Let X and Y be bipartite graphs, $V(X)=A_X\cup B_X$, $V(Y)=A_Y\cup B_Y$ be partitions of sets of their vertices into parts. Prove that if two arrangements of people $\sigma,\tau\colon V(X)\to V(Y)$ belong to the same connected component of graph $\mathsf{FS}(X,Y)$, then the sign of the permutation $\sigma^{-1}\circ\tau$ coincides with the parity of number $|\tau(A_X)\cap A_Y|-|\sigma(A_X)\cap A_Y|$.

2.7. Prove that graph $\mathsf{FS}(K_{r,r},K_{r,r})$ has two components of connectivity.

2.8. Let bipartite graph X satisfies conditions 1), 3), 4) of Wilson's theorem, graph Y is the star graph $K_{1,n}$ to which one edge has been added. Prove that graph $\mathsf{FS}(X,Y)$ is connected.

2.9. Let X be a graph with $n\geqslant 4$ vertices. Prove that graph $\mathsf{FS}(X,K_{2,n-2})$ is connected if and only if, when X is connected not bipartite graph without essential bridges and $X\neq C_n$.

a) $\Rightarrow$ b) $\Leftarrow$

2.10. Let X and Y be connected graphs on n vertices, and at least one person from Y has at least k friends ($k\geqslant 2$), and each induced k-vertex subgraph of X is connected. Let there exist k-vertex induced subgraph X_0 of graph X, for which 15-puzzle is solvable. Prove that graph $\mathsf{FS}(X,Y)$ is connected.

2.11. Let X and Y be connected graphs on n vertices, and let the vertices $x_1, x_2, \ldots, x_d$ ($d\geqslant 1$) form a «long bridge» in X, i. e. a path in X, which endpoints are cut vertices, and all the intermediate vertices $x_2,\ldots,x_{d-1}$ have degree exactly 2. Let $\delta(Y)\leqslant d$. Prove that graph $\mathsf{FS}(X,Y)$ is disconnected.

3 Friends walk along the circles

3.1. First, let the friends go along a line. Let graph Y be pentagon $ABCDE$ with diagonals AC and AD. How many components of connectivity has graph $\mathsf{FS}(P_5, Y)$?

Let graph $\overline{Y}$ be given. Define an orientation on it by choosing a direction for each edge. An orientation α is called *acyclic*, if it does not contain a directed cycle. If orientation α is given, consider all the possible placements of vertices of graph $\overline{Y}$ on the line (= at the vertices of graph P_n), for which all the arrows are directed from left to right. The set of such placements is denoted by $\mathcal{L}(\alpha)$.

The next problem is an example of «mathematical zoology». If all terms are accurately and correctly defined, then there is nothing to prove.

3.2. Let $X = P_n$, $|V(Y)| = n$. Prove that for each acyclic orientation α of the complement graph $\overline{Y}$ the set $\mathcal{L}(\alpha)$ is a component of connectivity of graph $\mathsf{FS}(P_n, Y)$.

3.3. *The Lollipop graph* $L_{k,m}$ is the graph with $k + m$ vertices, consisting of m-clique and a tail of k vertices (i. e. just a path K_k) hanged to one of the vertices of the clique.

a) Let Y be a graph on n vertices such that graph $\mathsf{FS}(L_{n-m,m}, Y)$ is connected. Prove that $\delta(Y) \geqslant n - m + 1$.

b) Let Y be a graph on n vertices. Prove that graph $\mathsf{FS}(L_{n-3,3}, Y)$ is connected if and only if $\delta(Y) \geqslant n - 2$.

c) Let D_n be the graph obtained from path P_{n-1} (with vertices numbered from 1 to $n - 1$) by adding new vertex with number n and new edge $(n-2) - n$. (This graph can be obtained from lollipop $L_{n-3,3}$ by removing one edge on 3-cycle). Let Y be a graph on n vertices. Prove that graph $\mathsf{FS}(D_n, Y)$ is connected if and only if, when $\delta(Y) \geqslant n - 2$.

3.4. $2n$ people are standing around in a cycle, they form n married pairs. The neighbours may interchange, if they are not husband and wife. Is it true that it is possible to rearrange the people in an arbitrary order?

3.5. $3n$ people forming n families of a mother, a father and a child, stand in a circle. Every two neighbours can exchange places except the case when a parent exchanges places with his/her child (this is forbidden). For what n is it possible to obtain every arrangement of those people by such exchanges? The arrangements differing by a circular shift are considered distinct.

3.6. Let $Y = K_{k,n-k}$. How many components of connectivity has graph $\mathsf{FS}(C_n, Y)$?

3.7. Let $X = C_n$, $n \geqslant 3$, and the complement graph $\overline{Y}$ is a connected graph on n vertices. Prove that any two people arrangements differing by a circular shift belong to distinct connected components of graph $\mathsf{FS}(C_n, Y)$, in particular, it has at least n components of connectivity.

Циклы в графах и в гиперграфах

Э. АЛКИН, А. ВОРОПАЕВ, С. ДЖЕНЖЕР, О. НИКИТЕНКО, А. СКОПЕНКОВ

Содержание

Введение

Назовём 1**-циклом** (симплициальным, по модулю 2) в графе множество C ребер такое, что каждая вершина принадлежит четному числу ребер из C. Например, цикл в смысле теории графов — это 1-цикл, но не наоборот. Легко проверить, что сумма (по модулю 2) 1-циклов тоже является 1-циклом.

В этом тексте мы изучаем следующие задачи: найти

• количество всех 1-циклов в данном графе;

• небольшое количество 1-циклов в данном графе таких, что любой 1-цикл является суммой нескольких из них.

Мы также рассматриваем обобщения (этих задач) на графы с симметрией и на 2-*циклы* в *двумерных гиперграфах* (все выделенные курсивом понятия определены ниже). Основные задачи — это 1.1.f, 1.3.e, 1.4.b, 1.5.ab, и 3.1.cf, 3.2.cf. Наивысшие достижения этого текста — результаты об 1- и 2-циклах в *квадрате графа* (задачи 2.5.c, 5.5.cd, 5.6.ab и 5.10.d).

Понятие 1-цикла и его обобщения имеют многочисленные приложения в топологии, наиболее простые из них см., например в [Sk20, §§4.11, 6, 9], [Sk, §§1, 8, 9]. Хотя этот текст элементарен, он мотивирован передним краем науки, см. [FH10, MS17, SS23] и ссылки в этих работах. Открытыми проблемами являются 2.9.cdfg и 5.10.f.

Изучение путём решения задач

Задачи пронумерованы, слово «задача» опускается. Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. **Загадкой** называется не сформулированный чётко вопрос; здесь нужно придумать и чёткую формулировку, и доказательство. Если задача выделена словом «теорема» («лемма», «следствие» и т. д.), 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

Э. Алкин, С. Дженжер, А. Скопенков: Московский физико-технический институт.
О. Никитенко: Алтайский технический университет.
А. Скопенков: Независимый московский университет, https://users.mccme.ru/skopenko/.

Данный текст (за исключением задач, отмеченных звёдочкой) был представлен в 2023 на Международной Летней Конференции Турнира Городов, см. https://ru.wikipedia.org/wiki/Турнир_городов. Мы благодарны И. Богданову, А. Рябичеву и О. Стырту за полезные обсуждения, а также А. Рябичеву за подготовку электронных версий некоторых рисунков.

могут потребоваться последующие задачи. Мы даем подсказки об этом после утверждений, но мы не лишаем Вас удовольствия самостоятельно найти момент, когда Вы наконец-то сможете доказать такое утверждение. Вообще, если Вы застряли на какой-то задаче, попробуйте перейти к следующим, они могут оказаться полезными.

В тексте определения важных понятий помечены **жирным шрифтом**, чтобы их было проще найти.

К представлению на летней конференции

Приглашаем Вас *обсуждать* с жюри возникающие вопросы. Те, кто успешно работают над проектом, завоюют право получить интересные *дополнительные задачи для исследования.*

Команда, работающая над проектом, может состоять из любого числа участников. За каждое решение, **написанное для пользователя**, оцененное в «+» или «+.», команда получает пять «бобов» (см. рекомендации https://www.mccme.ru/circles/oim/home/pism.pdf). Дополнительные бобы могут выдаваться за красивые решения, решения сложных задач или оформление некоторых решений в системе TEX. У жюри бесконечно много бобов. У каждого участника (или каждой команды) в начале пять бобов. Решения можно сдавать и *устно*, и как *написанные для соавтора*, если у команды есть бобы. Команда отдает один боб за каждую попытку сдачи (удачную или нет).

1. Одномерные циклы в графах

Строгое определение графа дано в начале §2. До этого можно работать с графами на интуитивном уровне.

Обозначим через

- $[n] := \{1, 2, \ldots, n\}$;
- K_n полный граф на множестве $[n]$ вершин;
- $K_{m,n}$ полный двудольный граф с долями $[m]$ и $[n]'$ (мы обозначаем через A' копию объекта A).

Простым циклом $v_1v_2\ldots v_k$ **длины** k в графе называется множество $\{v_1v_2, v_2v_3, \ldots, v_kv_1\}$ ребер такое, что вершины $v_1, \ldots, v_k$ попарно различны. *Простым циклом* называется простой цикл произвольной длины. Мы пропускаем слово «простой», если оно понятно из контекста. Очевидно, что любой простой цикл является 1-циклом. Определение 1-цикла дано во введении.

Суммой (суммой по модулю 2, или симметрической разностью) множеств A и B называется

$$A + B := (A \cup B) \setminus (A \cap B).$$

1.1. (a) Сумма 1-циклов является 1-циклом.
(b) Любой 1-цикл в K_n является суммой нескольких циклов длины 3.
(c) Если каждое ребро некоторого 1-цикла в K_n содержит вершину n, то этот 1-цикл пустой.
(d) Сколько имеется 1-циклов в K_n?
(e) Для любых вершин a, b, c, d в K_n выполнено равенство $abc + abd + acd + bcd = 0$ (мы обозначаем $0 := \varnothing$).
(f) Любое линейное соотношение между циклами длины 3 является суммой нескольких соотношений из п. (e).

Например,

- соотношение $123 + 124 + 134 + 235 + 245 + 345 = 0$ является суммой соотношений $123 + 124 + 134 + 234 = 0$ и $234 + 235 + 245 + 345 = 0$;
- сумма границ треугольников любой триангуляции сферы или тора (рис. 1) равна 0.

Строго говоря, *линейное соотношение* — это множество циклов длины 3 в K_n такое, что каждое ребро графа K_n содержится в четном числе циклов из этого множества. Поэтому строгая формулировка п. (f) такова (мы отождествляем циклы длины 3 в K_n с 3-элементными подмножествами множества $[n]$). Пусть R — набор 3-элементных подмножеств множества $[n]$ такой, что любое 2-элементное подмножество множества $[n]$ содержится в четном количестве

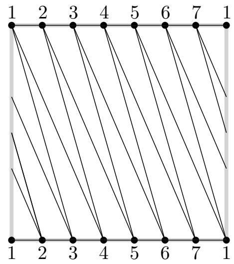


Рис. 1. Триангуляция тора (7-вершинная)

3-элементных подмножеств, являющихся элементами набора R. Тогда существует семейство R', состоящее из 4-элементных подмножеств множества $[n]$ такое, что 3-элементное подмножество B множества $[n]$ содержится в R тогда и только тогда, когда B содержится в нечетном количестве 4-элементных подмножеств, являющихся элементами семейства R'.

1.2. (a) Любой 1-цикл в графе является суммой нескольких простых циклов.
(b) Любой 1-цикл в графе является суммой нескольких простых циклов, не содержащих хорд. *Хордой* в простом цикле называется ребро графа, которое не принадлежит данному циклу (т. е. ребро между двумя непоследовательными вершинами цикла).
(c) Любой 1-цикл в K_n является суммой нескольких из следующих циклов: 123 и циклы длины 4.
(d) Цикл 123 не является суммой никаких циклов длины 4 в K_n.

1.3. (a) Любой 1-цикл в $K_{n,n}$ является суммой нескольких циклов длины 4.
(b) Если каждое ребро некоторого 1-цикла в $K_{n,n}$ содержит по крайней мере одну из вершин n или n', то этот 1-цикл пустой.
(c) Сколько имеется 1-циклов в $K_{n,n}$?
(d) Для любого набора попарно различных $a, b, c \in [n]$ и различных $u', v' \in [n]'$ выполнено $au'bv' + bu'cv' + cu'av' = 0$.
(e) Любое линейное соотношение между циклами длины 4 в $K_{n,n}$ является суммой нескольких соотношений из п. (d), и аналогичных соотношений $a'ub'v + b'uc'v + c'ua'v = 0$. (Строго говоря, *линейное соотношение* — это множество циклов длины 4 в $K_{n,n}$ такое, что каждое ребро графа $K_{n,n}$ содержится в четном количестве циклов из этого множества.)

1.4. Сколько имеется 1-циклов
(a) в дереве?
(b) в связном графе с V вершинами и E ребрами?

Обозначим через $\widetilde{K_n}$ граф, полученный из $K_{n,n}$ удалением всех «диагональных» ребер jj', $j \in [n]$. Например, $\widetilde{K_3}$ — это цикл $12'31'23'$ длины 6. Этот граф естественно появляется в задаче 5.8.

1.5. (a) Если $n \geqslant 4$, то любой 1-цикл в $\widetilde{K_n}$ является суммой нескольких циклов длины 4.
(b) Любой 1-цикл в $\widetilde{K_n}$ является суммой нескольких циклов $C_{ij'} := 12'31'ij'$ для ребер ij' из $\widetilde{K_n}$ таких, что $i, j > 1$ и $(i, j) \neq (3, 2)$.
(c) Представление из п. (b) единственно.

Множество $B \subset H_1(K)$ называется *базисом* множества $A \subset H_1(K)$, если каждый 1-цикл из A имеет единственное представление в виде суммы нескольких 1-циклов из B.

1.6 (симметричные 1-циклы)**.** * Обозначим через $t\colon \widetilde{K_n} \to \widetilde{K_n}$ симметрию (инволюцию), переставляющую доли графа, то есть переставляющую j и j' для каждого $j \in [n]$. Через tQ обозначим 1-цикл, симметричный 1-циклу Q. Например, $t\widetilde{K_3} = \widetilde{K_3}$ и $t(12'31'ij') = 1'23'1i'j$, 1-цикл Q называется *t-симметричным*, если $tQ = Q$. Например, $\widetilde{K_3}$ является t-симметричным.

(a) Сколько имеется t-симметричных 1-циклов в $\widetilde{K_n}$?

(b) Любой t-симметричный 1-цикл в $\widetilde{K_n}$ является суммой нескольких из следующих 1-циклов: $\widetilde{K_3}$ и $Q + tQ$ для циклов Q длины 4.

(c) Множество всех 1-циклов в $\widetilde{K_n}$ имеет базис, состоящий из (t-симметричного 1-цикла) $\widetilde{K_3}$ и пар взаимно симметричных (относительно t) 1-циклов.

1.7 (целочисленные 1-циклы)**.** * Пусть K — граф с ориентированными ребрами. Расстановка целых чисел на всех ребрах графа называется (симплициальным) *целочисленным 1-циклом*, если для каждой вершины сумма значений на входящих ребрах равна сумме значений на исходящих ребрах (правило Кирхгофа).

(a,b) Сформулируйте и докажите аналоги задач 1.4.a,b для целочисленных 1-циклов.

(c) Для данного набора ω ориентаций на ребрах графа K обозначим через $H_1^\omega(K;\mathbb{Z})$ множество целочисленных 1-циклов, с операцией покомпонентной суммы. Для различных наборов ω, ω' ориентаций существует взаимно однозначное соответствие $\varphi\colon H_1^\omega(K;\mathbb{Z}) \to H_1^{\omega'}(K;\mathbb{Z})$ такое, что $\varphi(x+y) = \varphi(x) + \varphi(y)$ для всех пар $x, y \in H_1^\omega(K;\mathbb{Z})$ (т. е. *группы* $H_1(K;\mathbb{Z})$ для различных наборов ориентаций ребер *изоморфны*).

1.8 (когомологии)**.** * Пусть на ребрах графа задана некоторая расстановка знаков $+$ или $-$. Определим на графе следующую операцию: выбираем произвольную вершину и инвертируем знаки у всех ребер, которым она принадлежит.

(a) Для дерева, применяя описанную выше операцию несколько раз (к различным вершинам), мы можем из любой расстановки знаков получить любую другую.

(b) Рассмотрим связный граф с V вершинами и E ребрами. Найдите наибольшее количество таких расстановок знаков $+$ или $-$ на ребрах графа, что ни одна из них не может быть получена ни из какой другой описанными выше операциями.

2. Одномерные циклы в квадрате графа

Граф — это пара (V, E) из конечного множества V и множества E, состоящего из 2-элементных подмножеств (называемых «ребрами») множества V.

В этом тексте K — граф. Иногда мы обозначаем ребро $\{a, b\}$ коротко через ab.

Определим *конфигурацию* (на интуитивном уровне) как пару муравьев (один красный и один синий), расположенных в двух вершинах графа (муравьи могут занимать одну и ту же вершину). Назовём две конфигурации *смежными*, если одна из них может быть получена из другой перемещением одного из муравьев вдоль какого-либо (одного) ребра. Вот строгое определение. Вершины графа $K^{\square 2}$ — это упорядоченные пары (a, b) вершин графа K. Если вершины b и c графа K соединены ребром, то вершины (a, b) и (a, c) графа $K^{\square 2}$ соединены ребром, обозначаемым (a, bc), а вершины (b, a) и (c, a) соединены ребром, обозначаемым (bc, a). Других ребер в графе $K^{\square 2}$ нет.

Вот примеры простых циклов в $K^{\square 2}$ (напомним из §1, что простой цикл обозначается вершинами, через которые он проходит):

• *граница*

$$ab \,\square\, uv := (a, u)(b, u)(b, v)(a, v),$$

для ребер ab и uv в K (произведение $ab \times uv$ является прямоугольником, см. §4, а $ab \,\square\, uv = \partial(ab \times uv)$ является его границей);

• *диагональные*, *внедиагональные* и *антидиагональные циклы*

$$\operatorname{diag}(123) := (1,1)(1,2)(2,2)(2,3)(3,3)(3,1), \quad (1,2)(1,3)(2,3)(2,1)(3,1)(3,2),$$

$$\text{и} \quad (1,1)(2,1)(2,3)(3,3)(3,2)(1,2) \quad \text{в} \quad K_3^{\square 2};$$

• *левые*, *правые*, *диагональные*, *внедиагональные*, и *антидиагональные циклы*

$$a \times C := (a, v_1) \dots (a, v_k), \quad C \times a := (v_1, a) \dots (v_k, a),$$

$$\operatorname{diag} C := (v_1, v_1)(v_1, v_2)(v_2, v_2) \ldots (v_k, v_k)(v_k, v_1), \quad (v_1, v_2)(v_1, v_3)(v_2, v_3) \ldots (v_k, v_1)(v_k, v_2),$$
$$\text{и} \quad (v_1, v_1)(v_2, v_1)(v_2, v_k) \ldots (v_k, v_2)(v_1, v_2)$$

для вершины a и простого цикла $C = v_1 \ldots v_k$ в K;

• *триодический цикл* $(1,3)(1,1')(1,2)(1',2)(3,2)(3,1')\ldots$ в $K_{3,1}^{\square 2}$, где точками обозначена часть, симметричная выписанной части; *триодическим циклом* также называется аналогичный цикл, соответствующий $K_{3,1}$-подграфу графа K.

Мы рассматриваем симметрию (инволюцию) графа $K^{\square 2}$, переставляющую компоненты (т. е. переставляющую точки (x, y) и (y, x)), и соответствующее отображение на 1-циклах. (О применении симметричных 1-циклов см. [Sk23, §1.6], [Sk, §1.6].)

2.1 (загадка)**.** Какие графы $K^{\square 2}$ получатся, если
(a) $K = K_{2,1}$ путь на трех вершинах; (b) $K = K_3$ цикл на трех вершинах;
(c) $K = K_{3,1}$ триод; (d) $K = K_4$.

2.2. (a) Любой 1-цикл в $K_{2,1}^{\square 2}$ является суммой нескольких границ.

(b) Триодический цикл в $K_{3,1}^{\square 2}$ является суммой нескольких границ.

(c) Любой 1-цикл в $K_{3,1}^{\square 2}$ является суммой нескольких границ.

(d) Если K — дерево, то любой 1-цикл в $K^{\square 2}$ является суммой нескольких границ.

Подсказка. Докажите, что *если K и L суть деревья, то любой 1-цикл в графе $K \square L$* (определенном ниже) *является суммой нескольких границ.* Докажите это по индукции, используя удаление висячей вершины.

(e) Является ли какой-либо левый цикл суммой нескольких границ?

(f) Является ли какой-либо диагональный цикл суммой нескольких границ?

Следующие понятия полезны, в частности, для задач 2.2.def.

Пусть K и L суть графы. Вершинами *графа произведения* $K \square L$ являются упорядоченные пары (a, b) вершин a графа K и b графа L. Если вершины b и c графа L соединены ребром, тогда вершины (a, b) и (a, c) графа $K \square L$ соединены ребром, обозначаемым как (a, bc). Если вершины b и c графа K соединены ребром, тогда вершины (b, a) и (c, a) графа $K \square L$ соединены ребром, обозначаемым как (bc, a). Других ребер в $K \square L$ нет.

Левой проекцией C_y для 1-цикла C в $K \square L$ называется множество всех ребер σ в L такое, что имеется нечетное количество вершин a в K таких, что $a \times \sigma \in C$. (Если C является циклом, то C_y является множеством всех ребер, по которым синий муравей проходит нечетное число раз.) *Правая проекция* C_x определяется аналогично.

2.3. (a) Диагональный цикл в $K_3^{\square 2}$ является суммой левого цикла, правого цикла, и нескольких границ.

(b) Внедиагональный цикл в $K_3^{\square 2}$ является суммой диагонального цикла и нескольких границ.

(c) Антидиагональный цикл в $K_3^{\square 2}$ является суммой диагонального цикла и нескольких границ.

(d) *Симметризованный цикл* $a \times C + C \times a$ является суммой цикла $\operatorname{diag} C$ и нескольких границ.

(e) Является ли для $K = K_4$ левый цикл 1×234 суммой нескольких диагональных циклов и границ?

2.4. Найдите количество 1-циклов по модулю границ в:
(a) $K_3^{\square 2}$; (b) $K_{2,2}^{\square 2}$; (c) $K_{2,3}^{\square 2}$; (d) $K_4^{\square 2}$.

Подсказка. Количество 1-циклов по модулю границ — это максимальное количество 1-циклов, ни один из которых не является суммой каких-либо других, и нескольких границ. Для некоторых пунктов этой задачи будет полезна теорема Кюннета 2.5.c.

Два 1-цикла C, C' в $K^{\square 2}$ называются *гомологичными* (или сравнимыми по модулю границ), если $C + C'$ является суммой нескольких границ. Обозначение: $C \sim C'$.

2.5. (a) Если граф K связен и T — дерево, то для любых 1-цикла C в $K \square T$ и вершины a в T существует единственный 1-цикл C_1 в K такой, что $C \sim C_1 \times a$. Более того, $C \sim C_x \times a$.

(b) Если Z является 1-циклом в $K^{\square 2}$ таким, что $Z_x = 0$, то $Z \sim a \times Z_y$ для любой вершины a.

(c) (теорема Кюннета) Если граф K связен, то для любых 1-цикла C в $K^{\square 2}$ и вершины a в K существуют единственные 1-циклы C_1, C_2 в K такие, что $C \sim C_1 \times a + a \times C_2$. Более того, $C \sim C_x \times a + a \times C_y$.

Следующее (как и $K^{\underline{2}}$, определенный в §5) является теоретико-графовым аналогом множества размещений. Рассмотрим двух муравьев на K, как описано выше, которым теперь запрещено находиться в одной вершине. Строго говоря, вершинами графа $K^{\square\underline{2}}$ являются упорядоченные пары различных вершин графа K. Вершины графа $K^{\square\underline{2}}$ соединены ребром в $K^{\square\underline{2}}$, если они соединены ребром в $K^{\square 2}$.

2.6. (загадка) Какие графы $K^{\square\underline{2}}$ получатся в случаях (a,b,c,d) из задачи 2.1?

2.7. Найдите количество 1-циклов в

(a) $K_3^{\square\underline{2}}$; (b) $K_{2,2}^{\square\underline{2}}$; (c) $K_{2,3}^{\square\underline{2}}$; (d) $K_4^{\square\underline{2}}$; (e) $K_{3,3}^{\square\underline{2}}$; (f) $K_5^{\square\underline{2}}$.

(a'-f') Найдите количество 1-циклов в $K^{\square\underline{2}}$ по модулю границ (содержащихся) в $K^{\square\underline{2}}$ (т. е. по модулю границ, соответствующих парам несмежных ребер).

Подсказки. (a'-d') Если множество границ в $K^{\square\underline{2}}$ имеет нулевую сумму, то это множество пусто.

(e'), (f') Сумма всех границ в $K^{\square\underline{2}}$ равна нулю. Это единственный непустой набор границ в $K^{\square\underline{2}}$, суммма которых равна нулю.

2.8. * (a) Если сумма границ симметрична, то она является *симметризованной границей*, т. е. суммой нескольких сумм $B + B'$ для некоторых взаимно симметричных пар границ B, B'.

(b) Любой симметричный 1-цикл в $K^{\square 2}$ является суммой нескольких симметризованных циклов и нескольких симметризованных границ. (Следовательно, это сумма нескольких диагональных циклов и нескольких границ; обратите внимание, что диагональный цикл симметричен по модулю границ.)

Подсказка. Следует из п. (a) и теоремы Кюннета 2.5.c.

(c) Для связного графа K отображение $C \mapsto C \times a + a \times C$ определяет взаимно однозначное соответствие между 1-циклами в K и симметричными 1-циклами в $K^{\square 2}$ по модулю симметричных границ. Обратное соответствие задается формулой $C \mapsto C_x = C_y$.

(d) Однозначно ли определяется количеством V вершин и количеством E ребер (для связных графов K) количество симметричных 1-циклов в $K^{\square 2}$? (Мы не знаем решения этой задачи.)

2.9. * Пусть K — связный граф.

(a) Триодический цикл не является суммой никаких границ в $K_{3,1}^{\square\underline{2}}$.

(b) Является ли антидиагональный цикл суммой 1-цикла в $K^{\square\underline{2}}$ и границ в $K^{\square 2}$.

(c) (гипотеза) В $K^{\square\underline{2}}$ никакой внедиагональный цикл не является суммой никаких симметризованных циклов, и границ.

(d) Любой ли внедиагональный в цикл $K_4^{\square\underline{2}}$ является суммой некоторых симметризованных циклов, триодических циклов, и границ?

(e) В $K^{\square\underline{2}}$ любой симметризованный цикл является суммой внедиагональных циклов, триодических циклов, и границ.

(f) (гипотеза) В $K^{\square\underline{2}}$ любой 1-цикл является суммой левых циклов, правых циклов, внедиагональных циклов, триодических циклов, и границ.

(g) (гипотеза) Является ли любой симметричный 1-цикл в $K^{\square\underline{2}}$ суммой внедиагональных циклов, триодических циклов, и границ (в $K^{\square 2}$)? То же с «...границами в $K^{\square\underline{2}}$»? То же, если «границы» заменить «симметризованными границами»?

Дополнительную информацию см. в [CPG].

3. Циклы в гиперграфах

Многомерные циклы в гиперграфах появляются, в частности, как соотношения между 1-циклами в графе, см. утверждения 1.1.ef.

3.1 (ср. задача 1.1)**.** Назовём 2-*циклом* множество C, состоящее из 3-элементных подмножеств (называемых «гранями») множества $[n]$, такое, что каждое 2-элементное подмножество множества $[n]$ содержится в четном количестве подмножеств множества C. Например, пустое множество является 2-циклом. Для 4-элементного подмножества $A \subset [n]$ назовём *тетраэдром* T_A множество всех 3-элементных подмножеств множества A. Другими словами, для попарно различных $a, b, c, d \in [n]$ определим *тетраэдр*

$$T_{\{a,b,c,d\}} := \big\{\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}\big\}.$$

Очевидно, что любой тетраэдр является 2-циклом.

(a) Сумма 2-циклов является 2-циклом.

(b) Если каждая грань 2-цикла содержит число n, то этот 2-цикл пустой.

(c) Любой 2-цикл является суммой нескольких тетраэдров.

(d) Сколько имеется 2-циклов для $[n]$?

(e) Для любого 5-элементного подмножества $A \subset [n]$ выполнено $\sum\limits_{j \in A} T_{A-\{j\}} = 0$.

(f) Любое линейное соотношение между тетраэдрами является суммой нескольких соотношений из п. (e). (Дайте строгую формулировку, аналогичную утверждению 1.1.f.)

3.2. Назовём *рядом* подмножество множества $[n]^\ell$ векторов длины ℓ, получаемое фиксацией всех координат, кроме одной. Определим *ладейный цикл* как подмножество множества $[n]^\ell$, содержащее четное количество вершин в каждом ряду. Например, пустое множество является ладейным циклом. Назовём *параллелепипедом* подмножество $P_1 \times \ldots \times P_\ell \subset [n]^\ell$, где P_i суть 2-элементные подмножества множества $[n]$. Очевидно, что любой параллелепипед является ладейным циклом.

(a) Сумма ладейных циклов является ладейным циклом.

(b) Если в ладейном цикле нет элементов из $[n-1]^\ell$, то этот ладейный цикл пустой.

(c) Любой ладейный цикл является суммой нескольких параллелепипедов.

(d) Сколько имеется ладейных циклов в $[n]^\ell$?

(e) Для любых попарно различных $a, b, c \in [n]$ и параллелепипеда $P \subset [n]^{\ell-1}$ выполнено $P \times \{a,b\} + P \times \{b,c\} + P \times \{c,a\} = 0$.

(f) Любое линейное соотношение между параллелепипедами в $[n]^\ell$ является суммой нескольких соотношений из (e), и соотношений, получаемых из (e) перестановками координат. (Строгая формулировка аналогична утверждениям 1.3.e и 3.1.f.)

Подсказка. Сначала разберите случай $\ell = 2$, ср. задача 1.3.

3.3 (загадка)**.** Придумайте и докажите многомерный аналог задачи 3.1.

3.4. * Назовём 2-*гиперграфом* (двумерным гиперграфом, или 3-однородным гиперграфом) пару (V, F) из конечного множества V и множества F, состоящего из нескольких 3-элементных подмножеств («граней») множества V. Назовём 2-*циклом* (симплициальным, по модулю 2) в 2-гиперграфе (V, F) множество C граней такое, что каждое 2-элементное подмножество множества V содержится в четном количестве подмножеств множества C.

(a) Существуют два *связных* гиперграфа, имеющие одинаковое количество вершин, ребер (т. е. 2-элементных подмножеств граней), и граней, но разное количество 2-циклов. (Ср. задача 1.4.b.)

(b) Пусть $L = (V, F)$ — гиперграф. Обозначим через E множество ребер, через b_0 количество компонент связности, через 2^{b_1} количество 1-циклов с по модулю границ граней, через 2^{b_2} количество 2-циклов. Тогда $b_0 - b_1 + b_2 = |V| - |E| + |F|$.

4. Геометрическое отступление: декартово произведение графов

Сначала мы дадим интуитивное определение цилиндра, а затем строгое.

Возьмем прямоугольники-ленточки $aa'b'b$, соответствующие ребрам ab графа K. Склеим концевые отрезки ленточек, соответствующие одной и той же вершине, так, чтобы штрихованные буквы склеивались бы со штрихованными. Полученная двумерная фигура называется *цилиндром* над графом K.

Напомним, что $\mathbb{R}^d$ — это d-мерное евклидово пространство (для $d = 2$ и $d = 3$ это обычные плоскость и пространство, которые проходят на уроках геометрии). *Цилиндром* над подмножеством $U \subset \mathbb{R}^d$ называется

$$U \times K_2 := \{(x,t) \in \mathbb{R}^{d+1} \ : \ x \in U,\ t \in [-1,1]\}.$$

Например, цилиндры над K_2, K_3, $K_{3,1}$, и K_5 показаны на рис. 2; цилиндр над $K_{k,1}$ «выглядит» как книга с k листами.

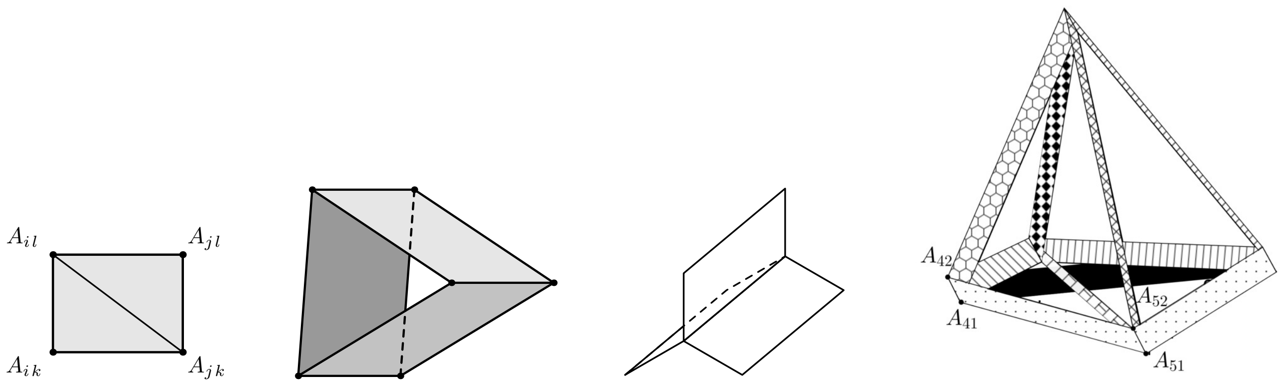


Рис. 2. Цилиндры над K_2, K_3, $K_{3,1}$, K_5

4.1. Любой граф можно нарисовать без пересечения ребер на книге с некоторым количеством листов (рис. 2, $K_{3,1}$), зависящим от графа. Более строго, для любого n существует целое число k, а также n точек и $n(n-1)/2$ несамопересекающихся ломаных на книге с k листами таких, что

- каждая пара точек соединена ломаной, и
- никакая ломаная не пересекает внутренность другой ломаной.

4.2 (загадка)**.** Цилиндр над любым графом реализуем без самопересечений в $\mathbb{R}^3$.

Для подмножеств $U, V \subset \mathbb{R}^d$ их *(геометрическим) произведением* называется

$$U \times V := \{(x,y) \in \mathbb{R}^{2d} \ : \ x \in U,\ y \in V\}.$$

В частности, *квадрат* подмножества $U \subset \mathbb{R}^d$ — это $U^2 = U \times U$. Например, квадрат K_2^2 — это обычный квадрат на плоскости, а квадрат K_3^2 (называемый *тором*) показан на рис. 4, в центре.

4.3 (загадка)**.** Нарисуйте в $\mathbb{R}^3$

(a) произведение $K_3 \times K_{3,1}$ без самопересечений.

(b) квадрат $K_{3,1}^2$; самопересечения допускаются.

Замечание. Иногда слово «граф» используется для понятия «тело графа», определяемого следующим образом. Пусть некоторое подмножество в $\mathbb{R}^3$ находится во взаимно однозначном соответствии с множеством вершин графа K, причем ни один отрезок, соответствующий какому-либо ребру графа K, не пересекает внутренность никакого другого такого отрезка. *Телом* графа K является объединение этого подмножества, а также всех таких отрезков.

На этом языке $K^{\square 2}$ — это множество (конфигурационное пространство) упорядоченных пар (x,y) точек графа K (точнее, его тела) таких, что x или y является вершиной графа K. Множество $K^{\square 2}$ является объединением конечного числа отрезков, т. е. является графом.

Аналогично, $K^{\square\underline{2}}$ — это множество (конфигурационное пространство) упорядоченных пар (x,y) точек графа K (точнее, его тела) таких, что x или y является вершиной графа K, и x,y не принадлежат одному ребру. Множество $K^{\square\underline{2}}$ является объединением конечного числа отрезков, т. е. является графом.

5. Двумерные циклы в квадрате графа

(Комбинаторным) произведением графов K и L называется

$$K \times L := \{(\sigma,\tau)\ :\ \sigma,\tau \text{ являются ребрами графа } K, L \text{ соответственно}\}.$$

Клетки (α,β) и (σ,τ) в $K\times L$ называются *смежными*, если
- либо $\alpha=\sigma$ и β,τ имеют общую вершину,
- либо $\beta=\tau$ и α,σ имеют общую вершину

(т. е. если они имеют общее ребро в $K \square L$).

Если склеить смежные клетки по их «общим рёбрам» в $K\square L$, получится геометрическое произведение, обсуждаемое в §4.

Квадратом графа K называется $K^2 := K\times K$. **Клеточным 2-циклом** (в K^2) называется подмножество $C\subset K^2$ такое, что для каждой вершины a и ребра β графа K
- имеется четное количество ребер α в K таких, что $\alpha\ni a$ и $(\alpha,\beta)\in C$, а также
- имеется четное количество ребер α в K таких, что $\alpha\ni a$ и $(\beta,\alpha)\in C$.

Иными словами, $C\subset K^2$ является клеточным 2-циклом, если к любому ребру «примыкает» чётное число клеток из C.

5.1. (a) Для подмножества $C\subset K^2$ сумма границ $\sigma\square\tau$ по всем $(\sigma,\tau)\in C$ равну нулю тогда и только тогда, когда C является клеточным 2-циклом.

(b) Подмножество $C\subset K^2$ является клеточным 2-циклом тогда и только тогда, когда для каждого ребра σ в K оба множества («вертикальное сечение» и «горизонтальное сечение»)

$$C_{\sigma,\cdot} := \big\{\tau\ :\ (\sigma,\tau)\in C\big\} \quad \text{и} \quad C_{\cdot,\sigma} := \big\{\tau\ :\ (\tau,\sigma)\in C\big\}$$

являются 1-циклами в K.

5.2. (a) Произведение любых простых циклов в K (*тор*) является клеточным 2-циклом.

(b) Сумма по модулю 2 клеточных 2-циклов является клеточным 2-циклом.

(c) Существует ли дерево T и непустой клеточный 2-цикл в T^2?

(d) Существуют ли граф K, дерево $T\subset K$ и непустой клеточный 2-цикл, содержащийся в $\overline{T} := T\times K\cup K\times T$?

5.3. Найдите количество клеточных 2-циклов в

(a) K_3^2; (b) $K_{2,2}^2$; (c) $K_{2,3}^2$; (d) K_4^2.

Подсказка. Для некоторых пунктов этой задачи будут полезны следующие задачи.

Говоря нестрого (и неточно), **комбинаторный взрезанный квадрат** $K^{\underline{2}}$ графа K — это множество упорядоченных пар (x,y) точек графа K таких, что x,y не принадлежат соседним ребрам. Множество $K^{\underline{2}}$ можно представить в виде объединения прямоугольников. Строго говоря, **комбинаторный взрезанный квадрат** графа K — это

$$K^{\underline{2}} := \{(\sigma,\tau)\ :\ \sigma,\tau \text{ суть несмежные ребра графа } K\}.$$

Замечание. Множество $K^{\underline{2}}$ и его обобщения имеют многочисленные приложения, в частности, для алгоритма распознавания реализуемости гиперграфов в многомерных евклидовых пространствах, см. обзоры [Sk06, Sk18]. Подмножество $K^{\underline{2}}\subset K^2$ меньше, чем K^2, поэтому иногда его легче нарисовать. Например, $K_2^{\underline{2}} = K_3^{\underline{2}} = K_{n,1}^{\underline{2}} = \varnothing$.

Склеим смежные клетки вдоль их «общего ребра». Тогда комбинаторные взрезанные квадраты пути на 5 вершинах, цикла на 5 вершинах, графа K_4, графа $K_{3,3}$, и графа K_5 выглядят как несвязное объединение двух дисков, кольцо, кубооктаэдр без треугольных граней (рис. 5), сфера с четырьмя ручками, и сфера с шестью ручками соответственно. (Для $K = K_{3,3}$ и $K = K_5$ можно доказать, что $K^{\underline{2}}$ выглядит как связная ориентируемая двумерная поверхность, и применить теорему о классификации двумерных поверхностей; см. подробности в [Sa91, текст после 3.4.1].)

5.4. (a) Существуют ли непустые клеточные 2-циклы в $K^{\underline{2}}$ для *цикла* K?

(b) Аналогичный вопрос для *колеса* K, т. е. для графа с множеством $\{0\} \cup [n]$ вершин, и ребрами $\{n, 1\}$, $\{0, j\}$ и $\{j, j+1\}$ для $j \in [n-1]$.

(c) Подмножество $K^{\underline{2}}_{3,3}$ в $K^{2}_{3,3}$ является клеточным 2-циклом.

(d) Аналогичное утверждение для K_5.

(e) Существует граф K такой, что $K^{\underline{2}}$ имеет непустое собственное подмножество, являющееся клеточным 2-циклом.

5.5. (a) Представьте $K^{\underline{2}}_{3,3}$ в виде суммы нескольких торов.

(b) Представьте $K^{\underline{2}}_5$ в виде суммы нескольких торов.

(c) Любой клеточный 2-цикл (в K^2) является суммой нескольких торов.

(d) Сколько имеется клеточных 2-циклов в K^2 для связного графа K с V вершинами и E ребрами?

Подсказка к (c, d). 1-цикл $\widehat{\varphi}\sigma$ определен в решении задачи 1.4.b. Воспользовавшись ответом на задачу 5.2.d, получим, что любой клеточный 2-цикл C в K^2 равен $\sum\limits_{(\sigma,\tau)\in C-\overline{T}} \widehat{\varphi}\sigma \times \widehat{\varphi}\tau$ и однозначно определяется своими клетками вне $\overline{T}$.

Обозначим через $H_1(K)$ множество всех 1-циклов в K, с операцией сложения.

Обозначим через $H_2(K^2)$ множество всех клеточных 2-циклов в K^2, с операцией сложения.

5.6 (Теорема Кюннета)**.** (a) Существует базис $C_1, \ldots, C_q$ в $H_1(K)$ такой, что $C_i \times C_j$, $i, j \in [q]$ — базис в $H_2(K^2)$.

(b) Если $C_1, \ldots, C_q$ — базис в $H_1(K)$, то $C_i \times C_j$, $i, j \in [q]$, — базис в $H_2(K^2)$.

(Т. е. $H_2(K^2) \cong H_1(K) \otimes H_1(K)$. *Базис* множества клеточных 2-циклов определяется аналогично случаю 1-циклов.)

5.7. (a) Произведение любых вершинно-непересекающихся циклов в K является клеточным 2-циклом в $K^{\underline{2}}$.

(b) Является ли любой клеточный 2-цикл в $K^{\underline{2}}$ суммой нескольких произведений вершинно-непересекающихся циклов?

5.8. (a) Сколько имеется клеточных 2-циклов в $K^{\underline{2}}_{n,n}$?

(b) Существует взаимно однозначное соответствие $H_2(K^{\underline{2}}_{n,n}) \to H_2(\widetilde{K_n}^2)$.

(c) Существует взаимно однозначное соответствие между $K^{\underline{2}}_{n,n}$ и $\widetilde{K_n}^2$, сохраняющее смежность.

Подсказка: решайте п. (a-c) в обратном порядке.

Рассмотрим симметрию (инволюцию) на K^2, переставляющую компоненты (т. е. переставляющую точки (x, y) и (y, x)), и соответствующее отображение на клеточных 2-циклах.

5.9. * (a) Для любых простых циклов Q, R в K *симметризованный тор* $Q \times R + R \times Q$ является симметричным клеточным 2-циклом.

(b) Сумма по модулю 2 симметричных клеточных 2-циклов является симметричным клеточным 2-циклом.

(c) Является ли любой симметричный клеточный 2-цикл суммой нескольких симметризованных торов?

(e) Однозначно ли определяется количеством V вершин и количеством E ребер (для связных графов K) количество симметричных клеточных 2-циклов в K^2?

5.10. * (a) Любой симметричный клеточный 2-цикл, содержащийся в $K^{\underline{2}}$, является суммой нескольких симметризованных торов.

(b) Сколько имеется симметричных клеточных 2-циклов в $K^{\underline{2}}_{n,n}$?

(c) взаимно однозначное соответствие из утверждения 5.8.b отображает клеточные 2-циклы в $K^{\underline{2}}_{n,n}$, переставляемые симметрией, в клеточные 2-циклы в $\widetilde{K_n}^2$, переставляемые симметрией t^2. Здесь симметрия $t\colon \widetilde{K_n} \to \widetilde{K_n}$ определена в задаче 1.6, и $t^2(x,y) := (tx, ty)$.

(d) Любой симметричный клеточный 2-цикл в $K^{\underline{2}}_{n,n}$ является суммой нескольких из следующих циклов:

• симметризованные торы $Q\times R+R\times Q$ для вершинно-непересекающихся циклов Q, R длины 4 в $K_{n,n}$;

• комбинаторный взрезанный квадрат $K^{\underline{2}}_{3,3}$ подграфа $K_{3,3}$ графа $K_{n,n}$.

(e) Любой t^2-симметрический клеточный 2-цикл в $\widetilde{K_n}^2$ является суммой нескольких из следующих: t^2-симметричных торов $Q \times R + tQ \times tR$ и $\widetilde{K_3}^2$.

(f) Верен ли аналог п. (d) для K_n и подграфа (гомеоморфного) K_5 графа K_n?

Подсказки. (d) Требуется теорема Кюннета 5.6, утверждение 5.8.b и п. (e).

(e) Требуется утверждение 1.6.c.

5.11. * (a) Следующее утверждение [Sa91, 3.4.2] неверно, даже для связных графов: существует клеточный 2-цикл C в $K^{\underline{2}}$ такой, что любой клеточный 2-цикл в $K^{\underline{2}}$ является суммой нескольких из следующих клеточных 2-циклов: C и произведения вершинно-непересекающихся циклов.

(b) (открытая проблема) Верно ли утверждение из п. (a) для 3-связных графов?

(c) Любой клеточный 2-цикл в $K^{\underline{2}}$ является суммой нескольких произведений вершинно-непересекающихся циклов, и нескольких комбинаторных взрезанных квадратов подграфов, гомеоморфных графу K_5 или $K_{3,3}$.

(d) (загадка) Сколько имеется клеточных 2-циклов в $K^{\underline{2}}$ для связного графа K с V вершинами и E ребрами (используйте дополнительные данные о графе, если нужно)?

Подсказки. (a) Возьмите дизъюнктное объединение двух копий графа K_5. Сделайте это объединение связным, соединив две копии ребром.

(c) Это следует из [Sa91, 3.4.1], потому что минимальные по включению 2-циклы порождают группу $H_2(K^{\underline{2}})$ (ср. [Sa91, начало п. (3.3)]). См. план доказательства в обновленном [SS23].

6. Ответы, подсказки и решения

1.1. (a) Пусть C_1 и C_2 — 1-циклы в графе. Возьмем произвольную вершину v. Назовем степенью $d_C(v)$ вершины v в наборе C ребер количество ребер набора C, которым принадлежит вершина v. Тогда $d_{C_1+C_2}(v) = d_{C_1}(v) + d_{C_2}(v) - 2d_{C_1\cap C_2}(v)$ четно. Поэтому $C_1 + C_2$ — 1-цикл.

(b) Любой простой цикл без хорд в графе K_n имеет длину 3. Поэтому (b) следует из утверждения 1.2.b.

Замечание. Конкретное представление 1-цикла в виде суммы нескольких циклов длины 3 дано в п. (d).

(c) Если в этом 1-цикле есть хотя бы одно ребро, то в нем есть висячая вершина.

(d) *Ответ:* $2^{\frac{(n-1)(n-2)}{2}}$.

Подсказка. Произвольный 1-цикл C в K_n равен сумме $\widehat{C} := \sum\limits_{ij\in C,\ i,j<n} ijn$ циклов ijn по всем ребрам $ij \in C$, не содержащим вершину n. Это следует из того, что каждое ребро в $C + \widehat{C}$ содержит вершину n, поэтому в силу п. (c) мы имеем $C + \widehat{C} = 0$, т. е. $C = \widehat{C}$.

Более того, такое представление единственно, см. подробности в доказательстве утверждения 1.4.b.

(f) В строгой формулировке это утверждение эквивалентно утверждению 3.1.c.

1.2. (a) Докажем, что любой 1-цикл в графе является суммой нескольких реберно непересекающихся простых циклов, принадлежащих данному 1-циклу. Поскольку все вершины 1-цикла имеют четную степень, ребер в нем не меньше, чем вершин. Следовательно, в любом 1-цикле есть простой цикл. Удаляя из 1-цикла ребра простого цикла, также получаем 1-цикл. Продолжая, получим набор реберно непересекающихся простых циклов, сумма которых равна исходному 1-циклу.

(b) Любой 1-цикл является суммой нескольких простых циклов. Любая хорда простого цикла длины l дает представление цикла в виде суммы двух простых циклов длины меньше l.

(c) Сумма двух циклов длины 3, имеющих общее ребро, является циклом длины 4. Поэтому, если цикл α длины 3 является суммой цикла 123 и циклов длины 4, то это верно и для любого цикла длины 3, имеющего общее ребро с α. Следовательно, все циклы длины 3 имеют это свойство. Теперь (c) следует по утверждению 1.1.b.

(d) Для конечного множества X обозначим через $|X|_2$ количество элементов в множестве X по модулю 2. Тогда для любых 1-циклов C, C' выполнено $|C + C'|_2 = |C|_2 + |C'|_2$.

Мы часто сокращаем $\varphi(x)$ до φx для образа x под действием отображения φ, и $\{\sigma\}$ до σ для 1-элементного множества.

1.3. (a) Данное утверждение следует из утверждения 1.2.b.

Замечание. Другой способ представления 1-цикла C в виде суммы нескольких циклов длины 4 — это $\widehat{\varphi}\varphi C$, определенный в нашем решении п. (c).

(c) *Ответ:* $2^{(n-1)^2}$.

Замечание. Сравните с утверждением 1.4.b.

Доказательство. Достаточно доказать, что существует взаимно однозначное соответствие между 1-циклами в $K_{n,n}$ и подмножествами[1] $K_{n-1,n-1}$. Определим отображение

$$\varphi\colon H_1(K_{n,n}) \to 2^{K_{n-1,n-1}} \quad \text{формулой} \quad \varphi C := C \cap K_{n-1,n-1}.$$

Для любого ребра $\sigma = ab'$ в $K_{n-1,n-1}$ обозначим через $\widehat{\varphi}\sigma$ цикл $ab'nn'$ длины 4. Определим отображение

$$\widehat{\varphi}\colon 2^{K_{n-1,n-1}} \to H_1(K_{n,n}) \quad \text{формулой} \quad \widehat{\varphi}D := \sum_{\sigma\in D} \widehat{\varphi}\sigma.$$

Поскольку $\varphi\widehat{\varphi}\sigma = \{\sigma\}$, имеем $\varphi\widehat{\varphi}D = D$ для любого $D \subset K_{n-1,n-1}$.

Возьмем любой 1-цикл $C \in H_1(K_{n,n})$. Так как $\widehat{\varphi}\varphi C$ и C являются 1-циклами, то $C' := \widehat{\varphi}\varphi C + C$ тоже является 1-циклом. Применяя $\varphi\widehat{\varphi}D = D$ для $D = \varphi C$, получаем $\varphi C' = 0$. Поэтому $C' \subset K_{n,n} \setminus K_{n-1,n-1}$. Отсюда, по (b), имеем $C' = 0$, поэтому $\widehat{\varphi}\varphi C = C$.

Таким образом, φ является взаимно однозначным соответствием.

(e) См. утверждение 3.2.f.

Замечание. Задача 1.3 эквивалентна частному случаю задачи 3.2 для $\ell = 2$. Ребро $ab' \in K_{n,n}$ соответствует паре $(a, b) \in [n]^2$. Вершина $a \in [n]$ соответствует ряду $x = a$, вершина $b' \in [n]'$ соответствует ряду $y = b$. Ребро, содержащее вершину, соответствует элементу множества $[n]^2$, принадлежащему ряду. Тогда 1-циклы в $K_{n,n}$ соответствуют ладейным циклам в $[n]^2$. В частности, циклы длины 4 соответствуют параллелепипедам (которые при $\ell = 2$ можно назвать параллелограммами).

1.4. *Ответ:* (a) 1; (b) 2^{E-V+1}.

(b) *Доказательство.* Пусть T — максимальное дерево связного графа K. Достаточно доказать, что существует взаимно однозначное соответствие между $H_1(K)$ и множеством 2^{K-T} подмножеств ребер из $K - T$.

Определим отображение

$$\varphi\colon H_1(K) \to 2^{K-T} \quad \text{формулой} \quad \varphi C := C \cap (K - T).$$

[1]Иногда обозначение графа K используется для множества ребер этого графа (или, напротив, обозначение «$\cap K$» используется для операции «ограничение на K» на множестве ребер).

Для любого ребра $\sigma \in K - T$ обозначим через $\widehat{\varphi}\sigma$ простой цикл в K, образованный σ, и простым путем в T, соединяющим концы σ. Определим отображение

$$\widehat{\varphi}\colon 2^{K-T} \to H_1(K) \quad \text{формулой} \quad \widehat{\varphi}D := \sum_{\sigma\in D} \widehat{\varphi}\sigma.$$

Поскольку $\varphi\widehat{\varphi}\sigma = \{\sigma\}$, имеем $\varphi\widehat{\varphi}D = D$ для любого $D \in 2^{K-T}$.

Выберем любой 1-цикл $C \in H_1(K)$. Так как $\widehat{\varphi}\varphi C$ и C являются 1-циклами, $C' := \widehat{\varphi}\varphi C + C$ тоже является 1-циклом. Применяя $\varphi\widehat{\varphi}D = D$ для $D = \varphi C$, получаем $\varphi C' = 0$. Поэтому $C' \subset T$. Отсюда, по (a) имеем $C' = 0$, поэтому $\widehat{\varphi}\varphi C = C$.

Таким образом, φ является взаимно однозначным соответствием.

1.5. (a) Простой цикл в $\widetilde{K_n}$ образован l-элементной циклической последовательностью вершин такой, что

- число l четное и больше 2;
- в последовательности чередуются вершины из разных долей;
- внутри каждой отдельной доли вершины не повторяются;
- не существует двух последовательных вершин m и m'.

Предположим, что такой цикл не имеет хорд. Тогда любые две непоследовательные вершины не являются смежными, т. е. либо находятся в одной доле, либо являются m и m'. Любая вершина имеет $\frac{l}{2} - 2$ непоследовательных вершин из другой доли. Тогда $\frac{l}{2} - 2 \leqslant 1$, так что $l \in \{4, 6\}$.

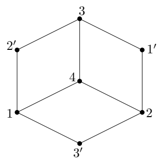


Рис. 3. Цикл длины 6 является суммой трех циклов длины 4

В простом цикле длины 6 без хорд любые две противоположные вершины равны m и m'. Следовательно, цикл равен $(m_1, m_2', m_3, m_1', m_2, m_3')$ для некоторых попарно различных m_1, m_2, m_3. Так как $n \geqslant 4$, то существует $a \in [n] - \{m_1, m_2, m_3\}$. Тогда цикл равен

$$(m_1, m_2', m_3, a') + (m_2, m_3', m_1, a') + (m_3, m_1', m_2, a'),$$

см. рис. 3. Теперь требуемый результат выполняется по утверждению 1.2.b.

(b,c) Пусть S — множество всех ребер ij' в $\widetilde{K_n}$ таких, что $i, j > 1$ и $(i, j) \neq (3, 2)$. Утверждения логически вытекают (аналогично задаче 1.4.b) из того, что

- ребро $e' \in S$ содержится в цикле C_e тогда и только тогда, когда $e = e'$;
- граф $\widetilde{K_n} - S$, полученный из $\widetilde{K_n}$ удалением всех ребер из S, является деревом.

Второе из этих утверждений следует из того, что ребра $\widetilde{K_n} - S$ равны именно $32'$ и $1i', i1'$, где $i > 1$, поэтому $\widetilde{K_n} - S$ получается соединением ребром $32'$ «звездных» деревьев, состоящих из ребер $1i'$ при $i > 1$ и ребер $1'i$ при $i > 1$.

2.1. (a) Сеточный граф 3×3, см. рис 4, слева.

(b) См. рис 4, по центру (где граничные циклы закрашены серым цветом). Другим способом граф $K_3^{\square 2}$ можно получить из графа в п. (a), добавив ребра между соответствующими вершинами:

- 1-й и 3-й строк;
- 1-го и 3-го столбцов.

(Сравните с получением графа K_3 из пути 123 добавлением ребра между 1 и 3.)

(c) См. рис 4, справа.

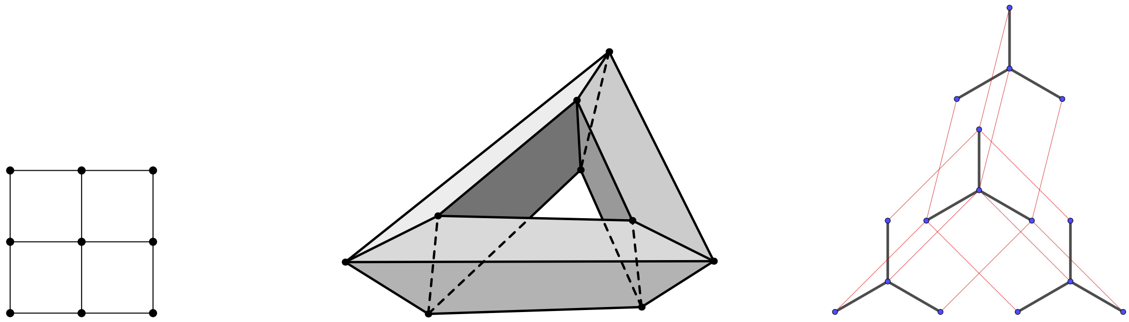


Рис. 4. Слева: $K_{2,1}^{\square 2}$, т. е. сеточный граф 3×3. Центр: $K_3^{\square 2}$ на торе K_3^2. Справа: $K_{3,1}^{\square 2}$

(d) Вершины — это узлы сетки 4×4. Две вершины соединены ребром тогда и только тогда, когда они находятся в одной строке или в одном столбце.

2.2. (b) Триодический цикл в $K_{3,1}^{\square 2}$ равен $\sum\limits_{i,j\in[3],i\neq j} i1'\square j1'$.

(e,f) *Ответы:* нет.

(e) *Подсказка.* Левая проекция любой границы (и, следовательно, любой суммы границ) пуста.

2.3. (a) Выполнено равенство $\mathrm{diag}(123) = 1\times(123)+(123)\times 1+12\square 23+12\square 31+23\square 31$.
(b) Внедиагональный цикл в $K_3^{\square 2}$ равен $1\times K_3+K_3\times 1+12\square 31+31\square 12$.
(c) Антидиагональный цикл в $K_3^{\square 2}$ равен $1\times K_3+K_3\times 1+23\square 31+31\square 23+31\square 31$.
(d) Выполнено равенство $1\times C+C\times 1=\mathrm{diag}\,C+\sum\limits_{i,j\in[n],i<j} i(i+1)\square j(j+1)$, где $n+1:=1$.

(e) *Ответ:* нет.

2.4. *Ответы:* (a) 2^2; (b) 2^2; (c) 2^4; (d) 2^6.

2.5. (a) Докажите это индукцией по количеству вершин в T, используя удаление висячей вершины.

(b) Это можно доказать индукцией по числу пар ребер в Z, проецируемых слева на одно и то же ребро в K. База индукции при нулевом числе может быть доказана индукцией по количеству вершин b в K таких, что $Z\cap(b\times K)\neq\varnothing$. Для индуктивного перехода возьмем такую пару $\{(\sigma,v_1),(\sigma,v_k)\}$, возьмем путь $v_1\dots v_k$ в K и заменим Z на $Z+\sigma\square v_1v_2+\ldots+\sigma\square v_{k-1}v_k$.

(c) Согласно (b), если $Z_x=Z_y=0$, то $Z\sim 0$. Применяя это к $Z=C+C_x\times a+a\times C_y$, мы получаем представление из (c). Единственность следует из того, что левая и правая проекции суммы границ равны 0.

2.6. *Ответы.*
(a) Объединение двух непересекающихся копий графа $K_{2,1}$.
(b) Цикл на 6 вершинах.
(c) Цикл на 12 вершинах.
(d) Объединение рёбер кубооктаэдра, см. рис. 5.

2.7. *Ответы.*
(a) 2^1; (b) 2^5; (c) 2^{17}; (d) 2^{13}; (e) 2^{43}; (f) 2^{41}.
(a') 2^1; (b') 2^1; (c') 2^5; (d') 2^7; (e') 2^8; (f') 2^{12}.
Указание. Примените задачу 1.4.b, чтобы получить (a)-(f).

3.1. (c) Достаточно доказать, что произвольный 2-цикл C равен сумме $\widehat{C} := \sum\limits_{\{i,j,k\}\in C,\ i,j,k<n} T_{i,j,k,n}$ тетраэдров $T_{i,j,k,n}$ над 3-элементными подмножествами $\{i,j,k\}\in C$, не содержащими n . Это следует из того, что каждая грань в $C+\widehat{C}$ содержит n, поэтому, в силу (b) имеем $C+\widehat{C}=0$, т. е. $C=\widehat{C}$.

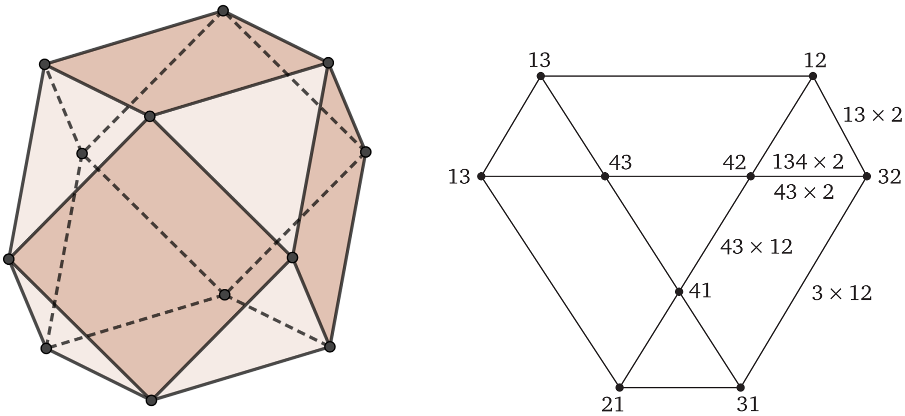


Рис. 5. Слева: кубооктаэдр; объединение ребер есть $K_4^{\square 2}$ (выделены три из шести границ); дополнение к треугольным граням есть $K_4^{\underline{2}}$. Справа: то же с некоторыми пояснениями; на рисунке не показана невидимая часть, проекция которой получается из изображенной проекции поворотом на $\pi/3$

(f) Строгая формулировка такова (мы отождествляем тетраэдры в $[n]$ с 4-элементными подмножествами $[n]$). Пусть R — набор 4-элементных подмножеств множества $[n]$ такой, что любое 3-элементное подмножество множества $[n]$ содержится в четном количестве 4-элементных подмножеств, являющихся элементами набора R. Тогда существует семейство R', состоящее из 5-элементных подмножеств множества $[n]$ такое, что 4-элементное подмножество B множества $[n]$ содержится в R тогда и только тогда, когда B содержится в нечетном количестве 5-элементных подмножеств, являющихся элементами семейства R'.

Это утверждение является многомерным аналогом утверждения 3.1.c; доказательство аналогично.

3.2. (c) Для $a \in [n-1]^\ell$ обозначим через $P(a) := \{n, a_1\} \times \ldots \times \{n, a_\ell\}$ параллелепипед с противоположными вершинами a и $(n, \ldots, n)$. Достаточно доказать, что любой ладейный цикл $C \subset [n]^\ell$ равен сумме $\widehat{C}$ параллелепипедов $P(a)$ над $a \in C \cap [n-1]^\ell$. Сумма $C + \widehat{C}$ является ладейным циклом. Поскольку $P(a) \cap [n-1]^\ell = \{a\}$, мы имеем $(C + \widehat{C}) \cap [n-1]^\ell = \varnothing$. По (b) имеем $C + \widehat{C} = \varnothing$, т. е. $C = \widehat{C}$.

(f) *Подсказка.* Любой параллелепипед P с некоторым $P_i \subset [n-1]$ является суммой нескольких заданных соотношений и двух параллелепипедов, полученных из P заменой на n одного из двух элементов в P_i. Значит, в каждом из этих двух параллелепипедов количество пар P_j, не содержащих n, меньше, чем в P. Следовательно, любое соотношение между параллелепипедами является суммой нескольких заданных соотношений и соотношения $P(a_1) + \ldots + P(a_s) = 0$, для некоторых попарно различных $a_1, \ldots, a_s \in [n-1]^\ell$.

Последнее соотношение тривиально, поскольку

$$\varnothing = (P(a_1) + \ldots + P(a_s)) \cap [n-1]^\ell = \{a_1, \ldots, a_s\}.$$

Здесь выполняется второе равенство, так как $P(a) \cap [n-1]^\ell = \{a\}$.

4.2. Пусть $O, V, A_{11}, \ldots A_{1n}$ — точки в $\mathbb{R}^3$, никакие 4 из которых не лежат в одной плоскости. Для каждого $p \in [n]$ возьмем точку A_{2p} такую, что $\overrightarrow{OA_{2p}} = \overrightarrow{OV} + \overrightarrow{OA_{1p}}$. Если V достаточно близка к O, то точки A_{jp}, $j \in \{1, 2\}$, $p \in [n]$ — искомые, т. е. объединение параллелограммов $A_{1p}A_{2p}A_{2q}A_{1q}$ дает изображение цилиндра над K_n в $\mathbb{R}^3$.

4.3. (b) См. рис. 6.

5.1. (b) В этом решении σ, τ — ребра графа K, v — вершина графа K:

$$C \text{ — 2-цикл} \quad \Leftrightarrow \quad \begin{cases} |\{\sigma :\ \sigma \ni v,\ (\sigma, \tau) \in C\}| \text{ четно для любых } v \text{ и } \tau \\ |\{\tau :\ \tau \ni v,\ (\sigma, \tau) \in C\}| \text{ четно для любых } v \text{ и } \sigma \end{cases} \quad \Leftrightarrow$$

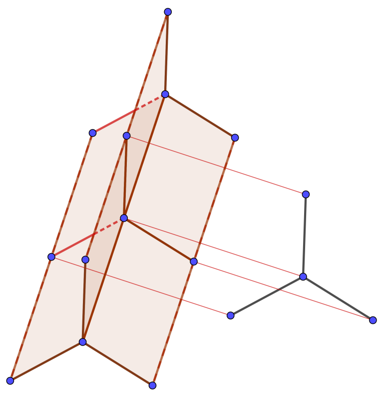


Рис. 6. Изображение графа $K^2_{3,1}$ в трехмерном пространстве

$$\Leftrightarrow \begin{cases} |\{\sigma \in C_{\cdot,\tau}\ :\ \sigma \ni v\}| \text{ четно для любых } v \text{ и } \tau \\ |\{\tau \in C_{\sigma,\cdot}\ :\ \sigma \ni v\}| \text{ четно для любых } v \text{ и } \sigma \end{cases} \Leftrightarrow \begin{cases} C_{\cdot,\tau} \text{ — 1-цикл для любого } \tau \\ C_{\sigma,\cdot} \text{ — 1-цикл для любого } \sigma. \end{cases}$$

5.2. (a) Пусть $C := \widetilde{C}_1 \times \widetilde{C}_2 \subset K^2$ — произведение простых циклов $\widetilde{C}_1$ и $\widetilde{C}_2$ в K. Для любого ребра σ графа K множество $C_{\sigma,\cdot}$ либо равно $\widetilde{C}_2$, либо пусто. Для любого ребра τ графа K множество $C_{\cdot,\tau}$ либо равно $\widetilde{C}_1$, либо пусто. Используя утверждение 5.1.b, получим, что C — клеточный 2-цикл.

(c) *Ответ:* нет.

Решение. Пусть C — клеточный 2-цикл в T^2. Поскольку T — дерево, из утверждения 5.1.b получаем, что $C_{\sigma,\cdot} = 0$ для любого ребра σ дерева T. Следовательно, $C = 0$.

(d) *Ответ:* нет.

Решение. Пусть C — клеточный 2-цикл в $\overline{T}$. Поскольку T — дерево, из утверждения 5.1.b получаем, что $C_{\sigma,\cdot} = 0$ для любого ребра σ графа $K \setminus T$. Следовательно, $C \subset T \times K$. Поскольку T — дерево, из утверждения 5.1.b получаем, что $C_{\cdot,\sigma} = 0$ для любого ребра σ графа K. Следовательно, $C = 0$.

5.3. *Ответы:* (a) 2; (b) 2; (c) 2^4; (d) 2^9.

Решения.

(a, b) Пусть C — клеточный 2-цикл в K^2 такой, что $C \neq K$, т. е. $(\sigma,\tau) \notin C$ для некоторых ребер σ,τ графа K. По утверждению 5.1.b, множество $C_{\sigma,\cdot}$ является 1-циклом. Так как K — граф-цикл, то $C_{\sigma,\cdot} = 0$. Тогда $(\sigma,\sigma) \notin C$. Следовательно, $C \subset \overline{K-\sigma}$. Используя ответ на задачу 5.2.d, получаем, что $C = 0$.

(c) Используя ответ на задачу 5.5.d, получаем, что количество 2-циклов в $K^2_{2,3}$ равно $2^{(E-V+1)^2} = 2^{2^2} = 16$.

(d) Используя ответ на задачу 5.5.d, получаем, что количество 2-циклов в K^2_4 равно $2^{(E-V+1)^2} = 2^{3^2} = 2^9 = 512$.

5.4. (a) *Ответ:* нет.

Решение. Пусть C — клеточный 2-цикл в $K^{\underline{2}}$. Возьмем ребро σ графа K. По утверждению 5.1.b, множество $C_{\sigma,\cdot}$ является 1-циклом. Поскольку $C_{\sigma,\cdot}$ — подмножество ребер графа-пути $K-\sigma$, то $C_{\sigma,\cdot} = 0$. Следовательно, $C = 0$.

(b) *Ответ:* нет.

Решение. Пусть C — клеточный 2-цикл в $K^{\underline{2}}$. По утверждению 5.1.b, множества $C_{\sigma,\cdot}$, $C_{\cdot,\sigma}$ являются 1-циклами для любого ребра σ графа K. Так как и $C_{0j,\cdot}$, и $C_{\cdot,0j}$ — подмножества ребер графа-пути $K-0-j$ для любого $j \in [n]$, то $C_{0j,\cdot} = C_{\cdot,0j} = 0$ для любого $j \in [n]$. Тогда $C \subset (K-0)^{\underline{2}}$ для графа-цикла $K-0$. Отсюда, по (a), имеем $C = 0$.

(c) Положим $C := K^{\underline{2}}_{3,3}$. Для произвольного ребра σ графа $K_{3,3}$ и $C_{\sigma,\cdot}$, и $C_{\cdot,\sigma}$ — циклы длины 4. Тогда требуемый результат следует из утверждения 5.1.b.

(d) Положим $C := K_5^{\underline{2}}$. Для произвольного ребра σ графа K_5 и $C_{\sigma,\cdot}$, и $C_{\cdot,\sigma}$ — циклы длины 3. Тогда требуемый результат следует из утверждения 5.1.b.

(e) Возьмем $K := K_6$ и $C := 123 \times 456$. Так как $(12, 34) \notin C$, произведение простых циклов C есть непустое собственное подмножество комбинаторного взрезанного квадрата $K^{\underline{2}}$. По утверждению 5.2.a, множество C является клеточным 2-циклом.

5.5. (a, b) *Подсказка:* требуемые представления можно получить из доказательства п. (c).

(c) Этот пункт легко следует из частного случая для связного графа K, что мы далее и предполагаем.

Пусть T — максимальное дерево связного графа K. Определим отображение

$$\varphi\colon H_2(K^2) \to 2^{K^2-\overline{T}} \quad \text{формулой} \quad \varphi C := C \cap (K^2 - \overline{T}).$$

Для любого ребра $\sigma \in K \setminus T$ в доказательстве утверждения 1.4.b определен 1-цикл $\widehat{\varphi}\sigma$. Определим отображение

$$\widehat{\varphi}\colon 2^{K^2-\overline{T}} \to H_2(K^2) \quad \text{формулой} \quad \widehat{\varphi}D := \sum_{(\sigma,\tau)\in D} \widehat{\varphi}\sigma \times \widehat{\varphi}\tau.$$

Используя ответ на задачу 5.2.d, получим, что $\widehat{\varphi}\varphi C = C$ для любого $C \in H_2(K^2)$, т. е. произвольный клеточный 2-цикл C в K^2 есть сумма торов $\widehat{\varphi}\sigma \times \widehat{\varphi}\tau$ по всем парам $(\sigma, \tau) \in \varphi C$.

(d) *Ответ:* $2^{(E-V+1)^2}$.

Решение. В п. (c) мы определили отображения $\varphi : H_2(K^2) \to 2^{K^2-\overline{T}}$ и $\widehat{\varphi} : 2^{K^2-\overline{T}} \to H_2(K^2)$ для максимального дерева T связного графа K и доказали, что $\widehat{\varphi}\varphi C = C$ для любого $C \in H_2(K^2)$. Также $\varphi\widehat{\varphi}D = D$ для любого $D \in 2^{K^2-\overline{T}}$. Таким образом, φ — взаимно однозначное соответствие. Следовательно,

$$|H_2(K^2)| = |2^{K^2-\overline{T}}| = |2^{(K\setminus T)^2}| = 2^{(E-V+1)^2}.$$

5.6. (b) Обозначим $B := \{C_i \times C_j \ : \ i, j \in [q]\}$. В следующих двух абзацах мы докажем, что каждый 2-цикл в K^2 есть сумма некоторых 2-циклов из B и что такое представление единственно, соответственно.

Применим утверждение 5.5.c. Каждый тор $\widetilde{C}_1 \times \widetilde{C}_2 \subset K^2$, в свою очередь, есть сумма некоторых 2-циклов из B, потому что каждый из простых циклов $\widetilde{C}_1, \widetilde{C}_2$ представляется в виде суммы некоторых 1-циклов из $C_1, \ldots, C_q$.

Обозначим через N количество компонент связности графа K. Аналогично утверждению 1.4.b, $|H_1(K)| = 2^{E-V+N}$. Поскольку $C_1, \ldots, C_q$ — базис в $H_1(K)$, то $2^q = |H_1(K)|$, значит $q = E-V+N$. Следовательно, $|B| = q^2 = (E - V + N)^2$. Обобщая утверждение 5.5.d для произвольного графа K, мы получаем $|H_2(K^2)| = 2^{(E-V+N)^2}$, где последнее значение совпадает с числом линейных комбинаций 2-циклов из B. Последнее влечет единственность представлений.

5.7. (a) *Подсказка:* это следует из утверждения 5.1.b.

(b) *Ответ:* нет.

Решение. Возьмем $K := K_5$ (или $K := K_{3,3}$) и $C := K^{\underline{2}}$. По утверждению 5.4.c (или 5.4.d), C — клеточный 2-цикл. Поскольку в графе K не существует двух непустых вершинно-непересекающихся циклов, то 2-цикл C не является суммой некоторых произведений вершинно-непересекающихся циклов.

5.8. (a) *Ответ:* $2^{(n^2-3n+1)^2}$.

(c) *Подсказка.* Взаимно однозначное соответствие определяется формулой $f(\sigma_1\sigma_2', \tau_1\tau_2') := (\sigma_1\tau_1', \sigma_2\tau_2')$ для несмежных рёбер $\sigma, \tau \in [n]^2$. (Напомним, что для $a, b \in [n]$ через ab' мы обозначаем ребро, соединяющее вершины a и b'.) Клетки $\alpha, \beta \in [n] \times [n]' \times [n] \times [n]'$ смежны в $K_{n,n}^{\underline{2}}$ тогда и только тогда, когда они различаются ровно по одной из четырех координат. Поскольку $K_{n,n}^{\underline{2}}, \widetilde{K_n}^{\underline{2}} \subset K_{n,n}^2$, то α и β в $K_{n,n}^{\underline{2}}$ смежны тогда и только тогда, когда $f\alpha$ и $f\beta$ в $\widetilde{K_n}^{\underline{2}}$ смежны, т. е. f сохраняет смежность.

Замечание. Определим взаимно однозначное соответствие $\widehat{f}$ между ребрами графа $K_{n,n}^{\square 2}$ и ребрами графа $\widetilde{K_n}^{\square 2}$, опустив одну из переменных $\sigma_1, \sigma_2', \tau_1, \tau_2'$ в формуле отображения f (например, $\widehat{f}(\sigma_1, \tau_1\tau_2') = (\sigma_1\tau_1', \tau_2'))$. Нетрудно доказать, что соответствия $f, \widehat{f}$ сохраняют инцидентность. (Напомним, что ребро η и 2-клетка $\alpha = (\xi, \zeta)$ *инцидентны*, если $\eta = \xi$ или $\eta = \zeta$.) При этом не существует взаимно однозначного соответствия между вершинами, которое бы сохраняло инцидентность. Действительно, не существует взаимно однозначного соответствия между 1-циклами в $K_{n,n}^{\square 2}$ и в $\widetilde{K_n}^{\square 2}$. Например, для $n = 3$ имеем $|H_1(\widetilde{K_3}^{\square 2})| = 2^{37}$, в отличие от ответа на задачу 2.7.e; кроме того, в $\widetilde{K_3}^{\square 2}$ четыре цикла по модулю границ, в отличие от ответа на задачу 2.7.e'.

Для набора квадратов с ориентированными сторонами разобьём эти стороны на пары. Склеим как-то стороны в соответствии с разбиением. Оказывается, это можно сделать разными способами, получив тем самым разные поверхности. Например, как было обосновано выше в решении, при одной склейке можно получить $K_{3,3}^2$, являющийся сферой с четырьмя ручками, а при другой склейке — тор $\widetilde{K_3}^2$.

Список литературы

[CPG] https://ru.wikipedia.org/wiki/Прямое_произведение_графов

[FH10] *M. Farber, E. Hanbury.* Topology of Configuration Space of Two Particles on a Graph, II. Algebr. Geom. Topol. 10 (2010) 2203–2227. arXiv:1005.2300.

[MS17] *T. Maciazek, A. Sawicki.* Homology groups for particles on one-connected graphs J. Math. Phys. 58, 062103 (2017). arXiv:1606.03414.

[Sa91] *K. S. Sarkaria.* A one-dimensional Whitney trick and Kuratowski's graph planarity criterion, Israel J. Math. 73 (1991), 79–89. http://kssarkaria.org/docs/One-dimensional.pdf.

[Sk06] * *A. Skopenkov,* Embedding and knotting of manifolds in Euclidean spaces, London Math. Soc. Lect. Notes, 347 (2008) 248–342. arXiv:math/0604045.

[Sk14] * *А. Скопенков,* Реализуемость гиперграфов и неотъемлемая зацепленность, Мат. Просвещение, в печати. arXiv:1402.0658.

[Sk18] * *A. Skopenkov.* Invariants of graph drawings in the plane. Arnold Math. J., 6 (2020) 21–55; full version: arXiv:1805.10237.

[Sk20] * *A. Skopenkov,* Algebraic Topology From Geometric Standpoint (in Russian), MCCME, Moscow, 2020 (2nd edition). Part of the book: http://www.mccme.ru/circles/oim/obstruct.pdf . Part of the English translation: https://www.mccme.ru/circles/oim/obstructeng.pdf.

[Sk23] * *A. Skopenkov.* Инварианты изображений графов на плоскости. Мат. Просвещение (2023).

[Sk] * *A. Skopenkov.* Algebraic Topology From Algorithmic Standpoint, draft of a book, mostly in Russian, http://www.mccme.ru/circles/oim/algor.pdf.

[SS23] A. Skopenkov and O. Styrt, Embeddability of join powers and minimal rank of partial matrices, arXiv:2305.06339.

CYCLES IN GRAPHS AND IN HYPERGRAPHS

E. ALKIN, S. DZHENZHER, O. NIKITENKO, A. SKOPENKOV, A. VOROPAEV

Contents

Introduction

A (simplicial) 1-**cycle** (modulo 2) in a graph is a set C of edges such that every vertex is contained in an even number of edges from C. E.g., a cycle in the sense of graph theory is a 1-cycle, but not vice versa. It is easy to check that the sum (modulo 2) of 1-cycles is a 1-cycle.

In this text we study the following problems: to find

• the number of all 1-cycles in a given graph;

• a small number of 1-cycles in a given graph such that any 1-cycle is the sum of some of them.

We also consider generalizations (of these problems) to graphs with symmetry, and to 2-*cycles* in 2-*dimensional hypergraphs* (all the italicized notions are defined later). Main problems are 1.1.f, 1.3.e, 1.4.b, 1.5.ab, and 3.1.cf, 3.2.cf. The peaks of this text are results on 1- and 2-cycles in *the square of a graph* (Problems 2.5.c, 5.5.cd, 5.6.ab and 5.10.d).

The notion of a 1-cycle and its generalizations have many applications in topology, for simpler ones see e.g. [Sk20, §§4.11, 6, 9], [Sk, §§1, 8, 9]. However elementary, this text is motivated by frontline of research, see [FH10, MS17, SS23] and the references therein. Open problems are 2.9.cdfg and 5.10.f.

Learning by doing problems

In this text we expose a theory as a sequence of problems, see e.g. [Sk21m, Introduction, Learning by doing problems] and the references therein. Most problems are useful theoretical facts. So this text could in principle be read even without solving problems or looking to §6 'Answers, hints and solutions'.

Problems are numbered, the words 'problem' are omitted. If a mathematical statement is formulated as a problem, then the objective is to prove this statement. Open-ended questions are called **riddles**; here one must come up with a clear wording, and a proof. If a problem is named 'theorem' ('lemma', 'corollary', etc.), then this statement is considered to be more important. Usually we *formulate* beautiful or important statement *before* giving a sequence of results (lemmas, assertions,

---

E. Alkin, S. Dzhenzher, A. Skopenkov: Moscow Institute of Physics and Technology.

O. Nikitenko: Altay Technical University.

A. Skopenkov: Independent University of Moscow, https://users.mccme.ru/skopenko/.

This text (except for problems marked by star) was presented in 2023 at the International Summer Conferences of the Tournament of Towns, see https://en.wikipedia.org/wiki/Tournament_of_the_Towns. We are grateful to I. Bogdanov, A. Ryabichev and O. Styrt for useful discussions, and to A. Ryabichev for preparing computer versions of some figures.

etc.) which constitute its *proof*. We give hints on that after the statements but we do not want to deprive you of the pleasure of finding the right moment when you finally are ready to prove the statement. In general, if you are stuck on a certain problem, try looking at the next ones; they may turn out to be helpful.

Important definitions are highlighted in **bold** for easy navigation.

On presentation at the Summer conference

Participants are welcomed to *consult* the jury on any questions on the project. If they successfully work on the project, they can get interesting *extra problems*.

A *team* working on this project may consist of any number of participants. For every solution *written for a user* marked with either '+' or '+.' a team gets five 'beans' (see recommendations in p. 3, 'How to write a proof for a user' of https://www.mccme.ru/circles/oim/multicomb.pdf). The jury may also award extra beans for beautiful solutions, solutions of hard problems, or solutions typeset in TEX. The jury has infinitely many beans. Every team initially has five beans. A team may submit a solution *in oral form* or as *written for a developer* if the team has some beans. A team loses a bean with every attempt (successful or not).

1. One-dimensional cycles in graphs

The rigorous definition of a graph is given at the beginning of §2. Before that you can work with graphs at an intuitive level.

Denote by

- $[n] := \{1, 2, \dots, n\}$;
- K_n the complete graph on the set $[n]$ of vertices;
- $K_{m,n}$ the complete bipartite graph with parts $[m]$ and $[n]'$ (we denote by A' a copy of A).

A **simple cycle** $v_1v_2\dots v_k$ **of length** k in a graph is a set $\{v_1v_2, v_2v_3, \dots, v_kv_1\}$ of edges such that the vertices $v_1, \dots, v_k$ are pairwise distinct. A *simple cycle* is a simple cycle of some length. We omit 'simple' if this word is clear from the context. Clearly, any simple cycle is a 1-cycle. The definition of a 1-cycle is given in the introduction.

The **sum** (the sum modulo 2, or the symmetric difference) of sets A, B is

$$A + B := (A \cup B) \setminus (A \cap B).$$

1.1. (a) The sum of 1-cycles is a 1-cycle.

(b) Any 1-cycle in K_n is a sum of some cycles of length 3.

(c) If every edge of a 1-cycle in K_n contains the vertex n, then the 1-cycle is empty.

(d) How many 1-cycles in K_n are there?

(e) For any vertices a, b, c, d in K_n we have $abc + abd + acd + bcd = 0$ (we denote $0 := \varnothing$).

(f) Any linear relation on cycles of length 3 in K_n is a sum of some relations from (e).

E.g.

- the relation $123 + 124 + 134 + 235 + 245 + 345 = 0$ is the sum of relations $123 + 124 + 134 + 234 = 0$ and $234 + 235 + 245 + 345 = 0$;
- the sum of boundaries of triangles from any triangulation of the sphere or of the torus (Figure 1) is zero.

Rigorously, a *linear relation* is a set of cycles of length 3 in K_n such that every edge of K_n is contained in an even number of cycles from this set. Thus a rigorous formulation of (f) is as follows (we identify cycles of length 3 in K_n with 3-element subsets of $[n]$). Suppose that R is a set of 3-element subsets of $[n]$ such that any 2-element subset of $[n]$ is contained in an even number of those 3-element subsets that are elements of R. Then there is a family R' of 4-element subsets of $[n]$ such that a 3-element subset B of $[n]$ is contained in R if and only if B is contained in an odd number of those 4-element subsets that are elements of R'.

1.2. (a) Any 1-cycle in a graph is a sum of some simple cycles.

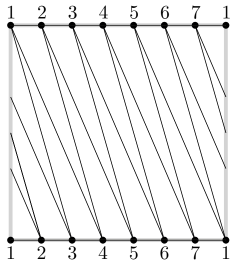


FIGURE 1. A 7-vertices triangulation of the torus

(b) Any 1-cycle in a graph is a sum of some simple cycles for which there are no chords. A *chord* in a simple cycle is an edge of the graph which does not belong to the cycle (i.e., an edge between two non-consecutive vertices).
(c) Any 1-cycle in K_n is a sum of some of the following cycles: 123 and cycles of length 4.
(d) The cycle 123 is not a sum of some cycles of length 4 in K_n.

1.3. (a) Any 1-cycle in $K_{n,n}$ is a sum of some cycles of length 4.
(b) If every edge of a 1-cycle in $K_{n,n}$ contains at least one of the vertices n or n', then the 1-cycle is empty.
(c) How many 1-cycles in $K_{n,n}$ are there?
(d) For any pairwise distinct $a, b, c \in [n]$ and distinct $u', v' \in [n]'$ we have $au'bv'+bu'cv'+cu'av' = 0$.
(e) Any linear relation on cycles of length 4 in $K_{n,n}$ is a sum of some relations from (d), and analogous relations $a'ub'v + b'uc'v + c'ua'v = 0$. (Rigorously, a *linear relation* is a set of cycles of length 4 in $K_{n,n}$ such that every edge of $K_{n,n}$ is contained in an even number of cycles from this set.)

1.4. How many 1-cycles are there
(a) in a tree?
(b) in a connected graph with V vertices and E edges?

Denote by $\widetilde{K_n}$ the graph obtained from $K_{n,n}$ by deleting all 'diagonal' edges jj', $j \in [n]$. E.g., $\widetilde{K_3}$ is the cycle $12'31'23'$ of length 6. This graph naturally appears in Problem 5.8.

1.5. (a) If $n \geqslant 4$, then any 1-cycle in $\widetilde{K_n}$ is a sum of some cycles of length 4.
(b) Any 1-cycle in $\widetilde{K_n}$ is a sum of some of the cycles $C_{ij'} := 12'31'ij'$ for edges ij' of $\widetilde{K_n}$ such that $i, j > 1$ and $(i, j) \neq (3, 2)$.
(c) The representation of (b) is unique.

1.6 (symmetric 1-cycles)**.** * Denote by $t\colon \widetilde{K_n} \to \widetilde{K_n}$ the symmetry (involution) switching the parts, i.e., switching j and j' for every $j \in [n]$. Denote by tQ the 1-cycle symmetric to a 1-cycle Q. E.g. $t\widetilde{K_3} = \widetilde{K_3}$ and $t(12'31'ij') = 1'23'1i'j$. A 1-cycle Q is called *t-symmetric* if $tQ = Q$. E.g. $\widetilde{K_3}$ is t-symmetric.

(a) How many t-symmetric 1-cycles are there in $\widetilde{K_n}$?

(b) Any t-symmetric 1-cycle in $\widetilde{K_n}$ is the sum of some of the following 1-cycles: $\widetilde{K_3}$ and $Q + tQ$ for cycles Q of length 4.

(c) The set of all 1-cycles in $\widetilde{K_n}$ has a base consisting of (the t-symmetric 1-cycle) $\widetilde{K_3}$ and pairs of 1-cycles going to each other under t.

1.7 (integer 1-cycles)**.** * Let K be a graph with oriented edges. An assignment of integers to oriented edges of K is a (simplicial) *integer* 1-*cycle* if for every vertex the sum of integers assigned to incoming edges equals the sum of integers assigned to outcoming edges (Kirchhoff rule).

(a,b) State and prove the analogues of Problems 1.4.a,b for integer 1-cycles.

(c) For given set ω of orientations on edges of K denote by $H_1^\omega(K;\mathbb{Z})$ the set of the integer 1-cycles, with the componentwise sum operation. For different sets ω,ω' of orientations there is a 1–1 correspondence $\varphi\colon H_1^\omega(K;\mathbb{Z})\to H_1^{\omega'}(K;\mathbb{Z})$ such that $\varphi(x+y)=\varphi(x)+\varphi(y)$ for every $x,y\in H_1^\omega(K;\mathbb{Z})$ (i.e., the *groups* $H_1(K;\mathbb{Z})$ for different sets of orientations are *isomorphic*).

1.8 (cohomology)**.** * Fix an assignment of + or − to edges of a graph. For any vertex one can inverse the sign of every edge containing this vertex.

(a) For a tree, by the above operations for different vertices one can obtain any assignment from any other assignment.

(b) Consider a connected graph with V vertices and E edges. Find a maximal number of assignments of + or − to edges such that none of these assignments can be obtained from any other by the above operations.

2. One-dimensional cycles in the square of a graph

A **graph** is a pair (V,E) of a finite set V and a set E of 2-element subsets (called 'edges') of V.

In this text K is a graph. We sometimes denote edge $\{a,b\}$ shortly by ab.

Intuitively, a *configuration* is a pair of ants (one red and one blue) sitting at two vertices of a graph (ants may occupy the same vertex). Configurations are called *adjacent* if one can be obtained from the other by one of the ants moving along one edge. This is rigorized as follows. Vertices of the graph $K^{\square 2}$ are ordered pairs (a,b) of vertices of the graph K. If vertices b and c of K are joined by an edge, then the vertices (a,b) and (a,c) of $K^{\square 2}$ are joined by an edge denoted by (a,bc), and vertices (b,a) and (c,a) are joined by an edge denoted by (bc,a). There are no other edges in $K^{\square 2}$.

E.g., the following are simple cycles in $K^{\square 2}$ (recall from §1 that a simple cycle is denoted by vertices it passes through):

• the *boundary*

$$ab\,\square\, uv := (a,u)(b,u)(b,v)(a,v),$$

for edges ab and uv in K (the product $ab\times uv$ is a rectangle, see §4, and $ab\,\square\,uv=\partial(ab\times uv)$ is its boundary);

• the *diagonal*, *off-diagonal* and *antidiagonal cycles*

$$\operatorname{diag}(123) := (1,1)(1,2)(2,2)(2,3)(3,3)(3,1),\quad (1,2)(1,3)(2,3)(2,1)(3,1)(3,2),$$

$$\text{and}\quad (1,1)(2,1)(2,3)(3,3)(3,2)(1,2)\quad\text{in}\quad K_3^{\square 2};$$

• the *left*, *right*, *diagonal*, *off-diagonal*, and *antidiagonal cycles*

$$a\times C := (a,v_1)\dots(a,v_k),\qquad C\times a := (v_1,a)\dots(v_k,a),$$

$$\operatorname{diag} C := (v_1,v_1)(v_1,v_2)(v_2,v_2)\dots(v_k,v_k)(v_k,v_1),\quad (v_1,v_2)(v_1,v_3)(v_2,v_3)\dots(v_k,v_1)(v_k,v_2),$$

$$\text{and}\quad (v_1,v_1)(v_2,v_1)(v_2,v_k)\dots(v_k,v_2)(v_1,v_2)$$

for a vertex a and a simple cycle $C=v_1\dots v_k$ in K;

• the *triodic cycle* $(1,3)(1,1')(1,2)(1',2)(3,2)(3,1')\dots$ in $K_{3,1}^{\square 2}$, where dots denote the part symmetric to the written part; a *triodic cycle* is also the analogous cycle corresponding to a $K_{3,1}$-subgraph of K.

We consider the symmetry (involution) of $K^{\square 2}$ switching the factors (i.e., switching points (x,y) and (y,x)), and the corresponding map on 1-cycles. (For an application of symmetric 1-cycles see e.g. [Sk, §1.6].)

2.1 (riddle)**.** Find graphs $K^{\square 2}$ for

(a) $K=K_{2,1}$ a path on three vertices; (b) $K=K_3$ a cycle on three vertices;

(c) $K=K_{3,1}$ a triod; (d) $K=K_4$.

2.2. (a) Any 1-cycle in $K_{2,1}^{\square 2}$ is a sum of some boundaries.

(b) The triodic cycle in $K_{3,1}^{\square 2}$ is a sum of some boundaries.

(c) Any 1-cycle in $K_{3,1}^{\square 2}$ is a sum of some boundaries.

(d) If K is a tree, then any 1-cycle in $K^{\square 2}$ is a sum of some boundaries.

Hint. Prove that *if K and L are trees, then any* 1*-cycle in the graph* $K \square L$ (defined below) *is a sum of some boundaries.* Prove this by induction, using deletion of a leaf vertex.

(e) Is some left cycle a sum of some boundaries?

(f) Is some diagonal cycle a sum of some boundaries?

The following notions are useful, in particular, for Problems 2.2.def.

Let K and L be graphs. Vertices of the *product graph* $K \square L$ are ordered pairs (a, b) of vertices a of K and b of L. If vertices b and c of L are joined by an edge, then the vertices (a, b) and (a, c) of $K \square L$ are joined by an edge denoted by (a, bc). If vertices b and c of K are joined by an edge, then the vertices (b, a) and (c, a) of $K \square L$ are joined by an edge denoted by (bc, a). There are no other edges in $K \square L$.

The left projection C_y of a 1-cycle C in $K \square L$ is the set of all edges σ in L such that there is an odd number of vertices a in K such that $a \times \sigma \in C$. (If C is a cycle, then C_y is the set of all edges passed by the blue ant an odd number of times.) *The right projection* C_x is defined analogously.

2.3. (a) The diagonal cycle in $K_3^{\square 2}$ is a sum of a left cycle, a right cycle, and some boundaries.

(b) The off-diagonal cycle in $K_3^{\square 2}$ is a sum of the diagonal cycle and some boundaries.

(c) The antidiagonal cycle in $K_3^{\square 2}$ is a sum of the diagonal cycle and some boundaries.

(d) The *symmetrized cycle* $a \times C + C \times a$ is the sum of $\operatorname{diag} C$ and some boundaries.

(e) For $K = K_4$ is the left cycle 1×234 a sum of some diagonal cycles and some boundaries?

2.4. Find the number of 1-cycles up to boundaries in

(a) $K_3^{\square 2}$; (b) $K_{2,2}^{\square 2}$; (c) $K_{2,3}^{\square 2}$; (d) $K_4^{\square 2}$.

Hint. The number of 1-cycles up to boundaries is the maximal number of 1-cycles such that none of them is the sum of any other and some boundaries. For some parts of this problem the Künneth theorem 2.5.c will be useful.

Two 1-cycles C, C' in $K^{\square 2}$ are said to be *homologous* (or congruent modulo boundaries) if $C + C'$ is a sum of some boundaries. Notation: $C \sim C'$.

2.5. (a) If K is connected and T is a tree, then for any 1-cycle C in $K \square T$ and vertex a in T there is a unique 1-cycle C_1 in K such that $C \sim C_1 \times a$. Moreover, $C \sim C_x \times a$.

(b) If Z is a 1-cycle in $K^{\square 2}$ such that $Z_x = 0$, then $Z \sim a \times Z_y$ for any vertex a.

(c) (Künneth theorem) If K is connected, then for any 1-cycle C in $K^{\square 2}$ and vertex a in K there are unique 1-cycles C_1, C_2 in K such that $C \sim C_1 \times a + a \times C_2$. Moreover, $C \sim C_x \times a + a \times C_y$.

The following (and $K^{\underline{2}}$ defined in §5) is a graph-theoretical analogue of the set of arrangements. Consider two ants on K as above, but now forbidden to sit in the same vertex. Rigoriously speaking, vertices of the graph $K^{\square\underline{2}}$ are ordered pairs of distinct vertices of K. Vertices of $K^{\square\underline{2}}$ are joined by an edge in $K^{\square\underline{2}}$ if they are joined by an edge in $K^{\square 2}$.

2.6. (riddle) Find graphs $K^{\square\underline{2}}$ in cases (a,b,c,d) of Problem 2.1.

2.7. Find the number of 1-cycles in

(a) $K_3^{\square\underline{2}}$; (b) $K_{2,2}^{\square\underline{2}}$; (c) $K_{2,3}^{\square\underline{2}}$; (d) $K_4^{\square\underline{2}}$; (e) $K_{3,3}^{\square\underline{2}}$; (f) $K_5^{\square\underline{2}}$.

(a'-f') Find the number of 1-cycles in $K^{\square\underline{2}}$ up to boundaries (contained) in $K^{\square\underline{2}}$ (i.e., up to boundaries corresponding to pairs of non-adjacent edges).

Hints. (a'-d') If a set of boundaries in $K^{\square\underline{2}}$ has zero sum, then the set is empty.

(e'), (f') The sum of all boundaries in $K^{\square\underline{2}}$ is zero. This is the only non-empty set of boundaries in $K^{\square\underline{2}}$ that has zero sum.

2.8. * (a) If a sum of boundaries is symmetric, it is a *symmetrized boundary*, i.e., a sum of $B+B'$ for some pairs of boundaries B, B' symmetric to each other.

(b) Any symmetric 1-cycle in $K^{\square 2}$ is a sum of some symmetrized cycles and some symmetrized boundaries. (Hence it is a sum of some diagonal cycles and some boundaries; note that a diagonal cycle is symmetric up to adding boundaries.)

Hint. Follows by (a) and the Künneth Theorem 2.5.c.

(c) For K connected, the map $C \mapsto C \times a + a \times C$ defines a 1–1 correspondence between 1-cycles in K and symmetric 1-cycles in $K^{\square 2}$ up to symmetrized boundaries. The inverse correspondence is given by $C \mapsto C_x = C_y$.

(d) For K connected, is the number of symmetric 1-cycles in $K^{\square 2}$ uniquely defined by the number V of vertices and the number E of edges? (We do not know solution of this problem.)

2.9. * Let K be a connected graph.

(a) A triodic cycle is not a sum of some boundaries in $K_{3,1}^{\underline{\square 2}}$.

(b) Is an antidiagonal cycle a sum of a 1-cycle in $K^{\underline{\square 2}}$ and some boundaries (in $K^{\square 2}$)?

(c) (conjecture) In $K^{\underline{\square 2}}$ any off-diagonal cycle is not a sum of symmetrized cycles, and boundaries.

(d) In $K_4^{\underline{\square 2}}$ is any off-diagonal cycle a sum of symmetrized cycles, triodic cycles, and boundaries?

(e) In $K^{\underline{\square 2}}$ any symmetrized cycle is a sum of off-diagonal cycles, triodic cycles, and boundaries.

(f) (conjecture) In $K^{\underline{\square 2}}$ any 1-cycle is a sum of left cycles, right cycles, off-diagonal cycles, triodic cycles, and boundaries.

(g) (conjecture) Any symmetric 1-cycle in $K^{\underline{\square 2}}$ is a sum of off-diagonal cycles, triodic cycles, and boundaries (in $K^{\square 2}$)? The same with '…boundaries in $K^{\underline{\square 2}}$'. The same with 'boundaries' replaced by 'symmetrized boundaries'.

See more information in [CPG].

3. Cycles in hypergraphs

Higher-dimensional cycles in hypergraphs appear, in particular, as relations on 1-cycles in a graph, see Assertions 1.1.ef.

3.1 (cf. Problem 1.1)**.** A 2-*cycle* is a set C of 3-element subsets (called 'faces') of $[n]$ such that every 2-element subsets of $[n]$ is contained in an even number of subsets from C. E.g. the empty set is a 2-cycle. For a 4-element subset $A \subset [n]$ let the *tetrahedron* T_A be the set of all 3-element subsets of A. In other words, for pairwise distinct $a, b, c, d \in [n]$ define the *tetrahedron*

$$T_{\{a,b,c,d\}} := \big\{\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}\big\}.$$

Clearly, any tetrahedron is a 2-cycle.

(a) The sum of 2-cycles is a 2-cycle.

(b) If every face of a 2-cycle contains the number n, then the 2-cycle is empty.

(c) Any 2-cycle is a sum of some tetrahedra.

(d) How many 2-cycles for $[n]$ are there?

(e) For any 5-element subset $A \subset [n]$ we have $\sum\limits_{j \in A} T_{A-\{j\}} = 0$.

(f) Any linear relation on tetrahedra is a sum of some relations from (e). (Give a rigorous formulation analogous to Assertion 1.1.f.)

3.2. Recall that $[n]^\ell$ is the set of all vectors of length ℓ whose entries are numbers from $[n]$. A *line* is a subset of $[n]^\ell$ given by fixing all coordinates except one. A *rook cycle* is a subset of $[n]^\ell$ containing an even number of vertices of every line. E.g. the empty set is a rook cycle. A *parallelepiped* is a subset $P_1 \times \ldots \times P_\ell \subset [n]^\ell$, where P_i are 2-element subsets of $[n]$. Clearly, any parallelepiped is a rook cycle.

(a) The sum of rook cycles is a rook cycle.

(b) If a rook cycle contains no elements from $[n-1]^\ell$, then the rook cycle is empty.

(c) Any rook cycle is a sum of some parallelepipeds.

(d) How many rook cycles for $[n]^\ell$ are there?

(e) For pairwise distinct $a, b, c \in [n]$ and parallelepiped $P \subset [n]^{\ell-1}$ we have $P \times \{a,b\} + P \times \{b,c\} + P \times \{c,a\} = 0$.

(f) Any linear relation on parallelepipeds in $[n]^\ell$ is a sum of some relations from (e), and relations obtained from that by permutations of coordinates. (A rigorous formulation is analogous to Assertions 1.3.e and 3.1.f.)

Hint. First try the case $\ell = 2$, cf. Problem 1.3.

3.3 (riddle)**.** Invent and prove a higher-dimensional analogue of Problem 3.1.

3.4. * A 2-*hypergraph* (a two-dimensional hypergraph, or a 3-uniform hypergraph) is a pair (V,F) of a finite set V and a set F of 3-element subsets ('faces') of V. A (simplicial) 2-*cycle* (modulo 2) in a 2-hypergraph (V,F) is a set C of faces such that every 2-element subset of V is contained in an even number of subsets from C.

(a) There are two *connected* hypergraphs having the same numbers of vertices, edges (i.e., 2-element subsets of faces), and faces, but different numbers of 2-cycles. (Cf. Problem 1.4.b.)

(b) Let $L = (V,F)$ be a hypergraph. Denote by E the set of edges, by b_0 the number of connected components, by 2^{b_1} the number of 1-cycles up to sums of some boundaries of faces, by 2^{b_2} the number of 2-cycles. Then $b_0 - b_1 + b_2 = |V| - |E| + |F|$.

4. Geometric digression: Cartesian products of graphs

First we give an intuitive definition of a cylinder, and then a rigorous one.

Take rectangle bands $aa'bb'$ correponding to edges ab of a graph K. Glue the end segments of the bands corresponding to the same vertex, so that the hatched letters would stick together with the hatched ones. The obtained two-dimensional figure is called a *cylinder* over graph K.

Recall that $\mathbb{R}^d$ is the d-dimensional Euclidean space (for $d = 2$ and $d = 3$ this is the usual plane and space which one studies in elementary geometry class). The *cylinder* over a subset $U \subset \mathbb{R}^d$ is

$$U \times K_2 := \{(x,t) \in \mathbb{R}^{d+1} \ : \ x \in U,\ t \in [-1,1]\}.$$

For instance, the cylinders over K_2, K_3, $K_{3,1}$, and K_5 are shown in Figure 2; the cylinder over $K_{k,1}$ 'looks like' the book with k sheets.

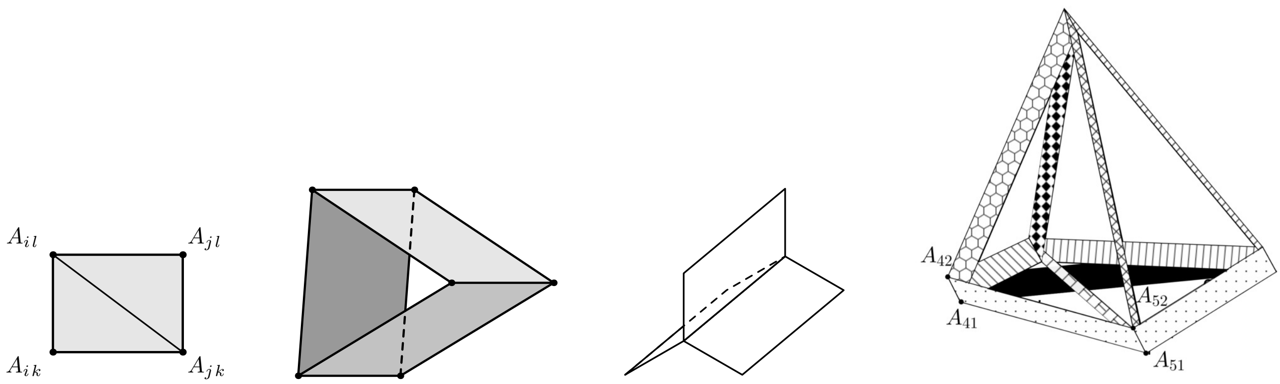


Figure 2. The cylinders over K_2, K_3, $K_{3,1}$, K_5

4.1. Any graph can be drawn without edges crossing on a book with a certain number of sheets (Figure 2, $K_{3,1}$) depending on the graph. More precisely, for any n there exists an integer k, as well as n points and $n(n-1)/2$ non-self-intersecting polygonal lines on a book with k sheets such that

- every pair of points is joined by a polygonal line, and
- no polygonal line intersects the interior of another polygonal line.

4.2 (riddle)**.** The cylinder over any graph is realizable without self-intersections in $\mathbb{R}^3$.

The *(geometric) product* of subsets $U, V \subset \mathbb{R}^d$ is

$$U \times V := \{(x, y) \in \mathbb{R}^{2d} \ : \ x \in U, \ y \in V\}.$$

In particular, the *square* of a subset $U \subset \mathbb{R}^d$ is $U^2 = U \times U$. For instance, the square K_2^2 is the ordinary square in the plane, and the square K_3^2 (called the *torus*) is shown in Figure 4, middle.

4.3 (riddle)**.** Draw in $\mathbb{R}^3$
(a) the product $K_3 \times K_{3,1}$ without self-intersections.
(b) the square $K_{3,1}^2$; self-intersections are allowed.

Remark. Sometimes the word 'graph' is used for 'the body of a graph' defined as follows. Suppose that a subset of $\mathbb{R}^3$ is in 1–1 correspondence with the set of vertices of K, and no segment corresponding to an edge of K intersects the interior of any other such segment. The *body* of K is the union of the subset, and of all such segments.

In this language $K^{\square 2}$ is the set (the configuration space) of ordered pairs (x, y) of points of a graph K (or rather of its body) such that either x or y is a vertex of K. The set $K^{\square 2}$ is a union of a finite number of segments, i.e., is a graph.

Analogously, $K^{\underline{\square 2}}$ is the set (the configuration space) of ordered pairs (x, y) of points of a graph K (or rather of its body) such that either x or y is a vertex of K, and x, y do not belong to the same edge. The set $K^{\underline{\square 2}}$ is a union of a finite number of segments, i.e., is a graph.

5. Two-dimensional cycles in the square of a graph

Let *the (combinatorial) product* of graphs K and L be

$$K \times L := \{(\sigma, \tau) \ : \ \sigma \text{ is an edge of } K, \ \tau \text{ is an edge of } L\}.$$

Cells (σ, τ) and (γ, δ) in $K \times L$ are said to be *adjacent* if either
- $\sigma = \gamma$, and τ, δ have a common vertex, or
- $\tau = \delta$, and σ, γ have a common vertex.

(i.e., if the cells 'share a common edge' in $K \square L$). If we glue adjacent cells along their 'common edges' in $K \square L$, we obtain the geometric product discussed in §4.

Let *the square* of K be $K^2 := K \times K$.

A **cellular 2-cycle** (in K^2) is a subset $C \subset K^2$ such that for every vertex a and edge β of K
- there is an even number of edges α of K such that $\alpha \ni a$ and $(\alpha, \beta) \in C$, and
- there is an even number of edges α of K such that $\alpha \ni a$ and $(\beta, \alpha) \in C$.

In other words, $C \subset K^2$ is a cellular 2-cycle if every edge in $K^{\square 2}$ is 'contained' in an even number of cells $(\alpha, \beta) \in C$.

5.1. (a) For subset C of K^2, the sum of boundaries $\sigma \square \tau$ over $(\sigma, \tau) \in C$ is zero if and only if C is a cellular 2-cycle.

(b) A subset $C \subset K^2$ is a cellular 2-cycle if and only if for every edge σ of K both sets ('column section' and 'row section')

$$C_{\sigma,\cdot} := \big\{\tau \ : \ (\sigma, \tau) \in C\big\} \quad \text{and} \quad C_{\cdot,\sigma} := \big\{\tau \ : \ (\tau, \sigma) \in C\big\}$$

are 1-cycles in K.

5.2. (a) The product of any two simple cycles in K (the *torus*) is a cellular 2-cycle.
(b) The sum modulo 2 of cellular 2-cycles is a cellular 2-cycle.
(c) Does there exist a tree T, and a non-empty cellular 2-cycle in T^2?
(d) Does there exist a graph K, a tree $T \subset K$, and a non-empty cellular 2-cycle contained in $\overline{T} := T \times K \cup K \times T$?

5.3. Find the number of cellular 2-cycles in
(a) $K_3^{\underline{2}}$; (b) $K_{2,2}^{\underline{2}}$; (c) $K_{2,3}^{\underline{2}}$; (d) $K_4^{\underline{2}}$.
Hint. For some parts of this problem the following problems will be useful.

Intuitively (and not precisely) speaking, the *combinatorial deleted product* $K^{\underline{2}}$ of K is a set of ordered pairs (x,y) of points in the graph K such that x,y do not belong to adjacent edges. The set $K^{\underline{2}}$ could be represented as a union of rectangles. Rigorously, let the *combinatorial deleted product* of K be

$$K^{\underline{2}} := \{(\sigma,\tau)\ :\ \sigma,\tau \text{ are non-adjacent edges of } K\}.$$

Remark. This set and its generalizations have many applications, notably to algorithm recognizing realizability of hypergraphs in higher-dimensional Euclidean spaces, see surveys [Sk06, Sk18]. The subset $K^{\underline{2}} \subset K^2$ is smaller than K^2, and so is sometimes easier-to-draw. E.g. $K_2^{\underline{2}} = K_3^{\underline{2}} = K_{n,1}^{\underline{2}} = \varnothing$.

Glue adjacent cells along their 'common edges' in $K^{\square 2}$. Then the combinatorial deleted product of the path on 5 vertices, of the cycle on 5 vertices, of K_4, of $K_{3,3}$, and of K_5 look like the disjoint union of two disks, the annulus, the cuboctahedron without triangular faces (Figure 5), the sphere with 4 handles, and the sphere with 6 handles, respectively.

(For $K = K_{3,3}$ and $K = K_5$ one proves that $K^{\underline{2}}$ looks like a connected orientable two-dimensional surface, and uses the classification theorem for two-dimensional surfaces; see details in [Sa91, the text after 3.4.1].)

5.4. (a) Are there any non-empty cellular 2-cycles in $K^{\underline{2}}$ for a *cycle* K?

(b) Analogous question for a *wheel* K, i.e., for the graph with the set $\{0\} \cup [n]$ of vertices, and edges $\{n,1\}$, $\{0,j\}$ and $\{j,j+1\}$ for $j \in [n-1]$.

(c) The subset $K_{3,3}^{\underline{2}}$ of $K_{3,3}^2$ is a cellular 2-cycle.

(d) Analogous statement for K_5.

(e) There is a graph K such that $K^{\underline{2}}$ has a non-empty proper subset that is a cellular 2-cycle.

5.5. (a) Express $K_{3,3}^{\underline{2}}$ as a sum of some tori.

(b) Express $K_5^{\underline{2}}$ as a sum of some tori.

(c) Any cellular 2-cycle (in K^2) is a sum of some tori.

(d) How many cellular 2-cycles in K^2 are there, for a connected graph K with V vertices and E edges?

Hint to (c, d). The 1-cycle $\widehat{\varphi}\sigma$ is defined in the solution of Problem 1.4.b. By answer to Problem 5.2.d any cellular 2-cycle C in K^2 equals $\sum\limits_{(\sigma,\tau)\in C-\overline{T}} \widehat{\varphi}\sigma \times \widehat{\varphi}\tau$, and is uniquely defined by its cells outside $\overline{T}$.

Denote by $H_1(K)$ the set of all 1-cycles in K, with the sum operation.

Denote by $H_2(K^2)$ the set of all cellular 2-cycles in K^2, with the sum operation.

A set B of 1-cycles is called a *base* of a set A of 1-cycles, if every 1-cycle from A has a unique representation as a sum of some 1-cycles from B (cf. Assertions 1.5.bc). Analogously one defines a *base* of a set of cellular 2-cycles.

5.6 (Künneth theorem)**.** (a) There is a base $C_1,\dots,C_q$ in $H_1(K)$ such that $C_i \times C_j$, $i,j \in [q]$, is a base in $H_2(K^2)$.

(b) If $C_1,\dots,C_q$ is a base in $H_1(K)$, then $C_i \times C_j$, $i,j \in [q]$, is a base in $H_2(K^2)$.

(I.e., $H_2(K^2) \cong H_1(K) \otimes H_1(K)$.)

5.7. (a) The product of any two vertex-disjoint cycles in K (i.e., two cycles which do not have common vertices) is a cellular 2-cycle in $K^{\underline{2}}$.

(b) Is any cellular 2-cycle in $K^{\underline{2}}$ a sum of some products of vertex-disjoint cycles?

5.8. (a) How many cellular 2-cycles in $K_{n,n}^{\underline{2}}$ are there?

(b) There is a 1–1 correspondence $H_2(K^{\underline{2}}_{n,n}) \to H_2(\widetilde{K_n}^2)$.

(c) There is a 1–1 correspondence between $K^{\underline{2}}_{n,n}$ and $\widetilde{K_n}^2$ that respects the adjacence.

Hint: solve parts (a-c) in the reverse order.

Consider the symmetry (involution) of K^2 switching the factors (i.e., switching points (x, y) and (y, x)), and the map induced by this symmetry on cellular 2-cycles.

5.9. * (a) For any simple cycles Q, R in K the *symmetrized torus* $Q \times R + R \times Q$ is a symmetric cellular 2-cycle.

(b) The sum modulo 2 of symmetric cellular 2-cycles is a symmetric cellular 2-cycle.

(c) Is any symmetric cellular 2-cycle a sum of some symmetrized tori?

(e) For K connected, is the number of symmetric cellular 2-cycles in K^2 uniquely defined by the number V of vertices and the number E of edges?

5.10. * (a) Any symmetric cellular 2-cycle contained in $K^{\underline{2}}$ is a sum of some symmetrized tori.

(b) How many symmetric cellular 2-cycles in $K^{\underline{2}}_{n,n}$ are there?

(c) The 1–1 correspondence of Assertion 5.8.b moves cellular 2-cycles in $K^{\underline{2}}_{n,n}$ transposed by the symmetry to cellular 2-cycles in $\widetilde{K_n}^2$ transposed by the symmetry t^2. Here the symmetry $t : \widetilde{K_n} \to \widetilde{K_n}$ is defined in Problem 1.6, and $t^2(x, y) := (tx, ty)$.

(d) Any symmetric cellular 2-cycle in $K^{\underline{2}}_{n,n}$ is a sum of some of the following ones:

- symmetrized tori $Q \times R + R \times Q$ for vertex-disjoint cycles Q, R of length 4 in $K_{n,n}$;
- the combinatorial deleted product $K^{\underline{2}}_{3,3}$ of the subgraph $K_{3,3}$ of $K_{n,n}$.

(e) Any t^2-symmetric cellular 2-cycle in $\widetilde{K_n}^2$ is a sum of some of the following ones: t^2-symmetrized tori $Q \times R + tQ \times tR$, and $\widetilde{K_3}^2$.

(f) Is the analogue of (d) for K_n and the subgraph (homeomorphic to) K_5 of K_n correct?

Hints. (d) One needs Künneth Theorem 5.6, Assertion 5.8.b and (e).

(e) One needs Assertion 1.6.c.

5.11. * (a) The following assertion [Sa91, 3.4.2] is wrong, even for connected graphs: there is a cellular 2-cycle C in $K^{\underline{2}}$ such that any cellular 2-cycle in $K^{\underline{2}}$ is a sum of some of the following cellular 2-cycles: C and products of vertex-disjoint cycles.

(b) (open problem) Is the assertion of (a) correct for 3-connected graphs?

(c) Any cellular 2-cycle in $K^{\underline{2}}$ is a sum of some products of vertex-disjoint cycles, and some combinatorial deleted products of subgraphs homeomorphic to K_5 or to $K_{3,3}$.

(d) (riddle) How many cellular 2-cycles in $K^{\underline{2}}$ are there, for a connected graph K with V vertices and E edges (use additional data of K, if required)?

Hints. (a) Take disjoint union of two copies of K_5. Make the disjoint union connected by joining the copies by an edge.

6. Answers, hints and solutions

1.1. (b) The assertion follows from Assertion 1.2.b.

Remark. A specific representation of a 1-cycle as a sum of some cycles of length 3 is given in (d).

(d) *Answer:* $2^{\frac{(n-1)(n-2)}{2}}$.

Hint. An arbitrary 1-cycle C in K_n equals the sum $\widehat{C} := \sum\limits_{ij \in C,\ i,j<n} ijn$ of cycles ijn over all edges $ij \in C$ not containing the vertex n. This follows because every edge in $C + \widehat{C}$ contains the vertex n, so by (c) we have $C + \widehat{C} = 0$, i.e., $C = \widehat{C}$.

Moreover, such a representation is unique, see details in the proof of Assertion 1.4.b.

(f) In the rigorous formulation this is equivalent to Assertion 3.1.c.

1.2. (b) Any 1-cycle is a sum of some simple cycles. Any chord for a simple cycle of length l gives a representation of the cycle as the sum of two simple cycles of lengths less than l.

(c) The sum of two cycles of length 3 having a common edge is a cycle of length 4. So if a cycle α of length 3 is a sum of 123 and cycles of length 4, then any cycle of length 3 having a common edge with α is such. Therefore, all cycles of length 3 are such. Now (c) follows by Assertion 1.1.b.

(d) For a finite set X denote by $|X|_2$ the size of X modulo 2. Then for any 1-cycles C, C' we have $|C + C'|_2 = |C|_2 + |C'|_2$.

We often shorten $\varphi(x)$ to φx for the image of x under φ, and $\{\sigma\}$ to σ for 1-element subset.

1.3. (a) The assertion follows from Assertion 1.2.b.

Remark. Another way of representing 1-cycle C as a sum of some cycles of length 4 is $\widehat{\varphi}\varphi C$ defined in our solution of (c).

(c) *Answer:* $2^{(n-1)^2}$.

Remark. Compare to Assertion 1.4.b.

Proof. It suffices to prove that there exists a 1–1 correspondence between 1-cycles in $K_{n,n}$ and subsets[1] of $K_{n-1,n-1}$. Define a map

$$\varphi\colon H_1(K_{n,n}) \to 2^{K_{n-1,n-1}} \quad \text{by} \quad \varphi C := C \cap K_{n-1,n-1}.$$

For any edge $\sigma = ab'$ in $K_{n-1,n-1}$ denote by $\widehat{\varphi}\sigma$ the cycle $ab'nn'$ of length 4. Define a map

$$\widehat{\varphi}\colon 2^{K_{n-1,n-1}} \to H_1(K_{n,n}) \quad \text{by} \quad \widehat{\varphi}D := \sum_{\sigma\in D} \widehat{\varphi}\sigma.$$

Since $\varphi\widehat{\varphi}\sigma = \sigma$, we have $\varphi\widehat{\varphi}D = D$ for any $D \subset K_{n-1,n-1}$.

Take any $C \in H_1(K_{n,n})$. Since both $\widehat{\varphi}\varphi C$ and C are 1-cycles, $C' := \widehat{\varphi}\varphi C + C$ is a 1-cycle. Applying $\varphi\widehat{\varphi}D = D$ for $D = \varphi C$, we obtain $\varphi C' = 0$. So $C' \subset K_{n,n} \setminus K_{n-1,n-1}$. Hence by (b) we have $C' = 0$, so $\widehat{\varphi}\varphi C = C$.

Thus, φ is a 1–1 correspondence.

(e) See Assertion 3.2.f.

Remark. Problem 1.3 is equivalent to a particular case of Problem 3.2 for $\ell = 2$. An edge $ab' \in K_{n,n}$ corresponds to $(a, b) \in [n]^2$. A vertex $a \in [n]$ corresponds to the line $x = a$, a vertex $b' \in [n]'$ corresponds to the line $y = b$. An edge containing a vertex corresponds to an element of $[n]^2$ belonging to a line. Then 1-cycles in $K_{n,n}$ correspond to rook cycles in $[n]^2$. In particular, cycles of length 4 correspond to parallelepipeds (which for $\ell = 2$ may be called parallelograms).

1.4. *Answers:* (a) 1; (b) 2^{E-V+1}.

(b) *Proof.* Let T be a maximal tree of a connected graph K. It suffices to prove that there exists a 1–1 correspondence between $H_1(K)$ and subsets of $K \setminus T$.

Define a map

$$\varphi\colon H_1(K) \to 2^{K\setminus T} \quad \text{by} \quad \varphi C := C \cap (K \setminus T).$$

For any edge $\sigma \in K \setminus T$ denote by $\widehat{\varphi}\sigma$ the simple cycle in K formed by σ and the simple path in T joining ends of σ.

Define a map

$$\widehat{\varphi}\colon 2^{K\setminus T} \to H_1(K) \quad \text{by} \quad \widehat{\varphi}D := \sum_{\sigma\in D} \widehat{\varphi}\sigma.$$

Since $\varphi\widehat{\varphi}\sigma = \sigma$, we have $\varphi\widehat{\varphi}D = D$ for any $D \in 2^{K\setminus T}$.

Take any $C \in H_1(K)$. Since both $\widehat{\varphi}\varphi C$ and C are 1-cycles, $C' := \widehat{\varphi}\varphi C + C$ is a 1-cycle. Applying $\varphi\widehat{\varphi}D = D$ for $D = \varphi C$, we obtain $\varphi C' = 0$. So $C' \subset T$. Hence by (a) we have $C' = 0$, so $\widehat{\varphi}\varphi C = C$.

Thus, φ is a 1–1 correspondence.

1.5. (a) A simple cycle in $\widetilde{K_n}$ is formed by an l-element cyclic sequence of vertices such that

[1] Sometimes the notation for a graph K is used for the set of edges of K (or, alternatively, the notation '$\cap K$' is used for the 'restriction to K' operation on the sets of edges).

- the number l is even and greater than 2;
- the parts of vertices alternate in the sequence;
- within each separate part, the vertices are not repeated;
- there are no two consecutive vertices m and m'.

Assume that such a cycle has no chords. Then any two non-consecutive vertices are not adjacent, i.e., they either are in the same part or are m and m'. Any vertex has $\frac{l}{2}-2$ non-consecutive vertices from the other part. Then $\frac{l}{2}-2\leqslant 1$, so $l\in\{4,6\}$.

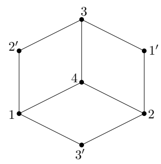


FIGURE 3. A cycle of length 6 is the sum of three cycle of length 4

In a simple cycle of length 6 having no chords, any two opposite vertices are m and m'. Hence the cycle is $(m_1,m_2',m_3,m_1',m_2,m_3')$ for some pairwise distinct m_1,m_2,m_3. Since $n\geqslant 4$, there is $a\in[n]-\{m_1,m_2,m_3\}$. Then the cycle equals

$$(m_1,m_2',m_3,a')+(m_2,m_3',m_1,a')+(m_3,m_1',m_2,a'),$$

see Figure 3. Now the required result holds by Assertion 1.2.b.

(b,c) Let S be the set of all edges ij' of $\widetilde{K_n}$ such that $i,j>1$ and $(i,j)\neq(3,2)$. The assertions follow (analogously to Problem 1.4.b) because

- an edge $e'\in S$ is contained in the cycle C_e if and only if $e=e'$;
- the graph $\widetilde{K_n}-S$ obtained from $\widetilde{K_n}$ by deleting all edges of S is a tree.

The second of these assertions follows because the edges of $\widetilde{K_n}-S$ are exactly $32'$ and $1i',i1'$, where $i>1$, so $\widetilde{K_n}-S$ is obtained by connecting with edge $32'$ the 'star' trees consisting of edges $1i'$ with $i>1$, and of edges $1'i$ with $i>1$.

1.6. (a,b) The natural projection $\widetilde{K_n}\to K_n$ gives a 1–1 corespondence between t-symmetric 1-cycles in $\widetilde{K_n}$ and 1-cycles in K_n. Use Assertions 1.1.d and 1.2.c.

(c) Take the base given by Assertions 1.5.bc. Then the 1-cycles

$$\widetilde{K_3}=C_{23'},\quad C_{ij'},\quad C_{23'}-C_{ji'},\quad\text{where}\quad i>j>1\quad\text{and}\quad (i,j)\neq(3,2),$$

also form a base. This base is as required because $C_{23'}-C_{ji'}=1i'j1'32'12'31'23'=1i'j1'23'=tC_{ij'}$.

Alternatively, one can take the cycles $\widetilde{K_3}$, $1j'i2'$, $1'ji'2$, where $j>i>2$, and $1i'23'$, $1'i2'3$, where $i>3$.

1.7. (a) *Statement.* There is only one integer 1-cycle in a tree. It assigns 0 to all edges.

Hint. Start with proving that any integer 1-cycle on a tree assigns 0 to all terminal edges.

(b) *Statement.* Let T be a maximal tree of a connected graph K. Every assignment of integers to edges of $K\setminus T$ has a unique extension to integer 1-cycle in K.

Proof. Note that the sum of integer 1-cycles is an integer 1-cycle.

Denote by $\widehat{\varphi}_{\mathbb Z}(\sigma)$ the integer 1-cycle in K

- assigning 1 to all edges of $\widehat{\varphi}\sigma$ oriented in $\widehat{\varphi}\sigma$ in the same way as σ,
- assigning -1 to all edges of $\widehat{\varphi}\sigma$ oriented in $\widehat{\varphi}\sigma$ the opposite way, and
- assigning 0 to all edges in $K\setminus\widehat{\varphi}\sigma$.

For every assignment D of integers to edges of $K\setminus T$ denote $\widehat{\varphi}D:=\sum\limits_{\sigma\in K\setminus T}D(\sigma)\widehat{\varphi}_{\mathbb Z}(\sigma)$. Then $\widehat{\varphi}D$ is an integer 1-cycle extending D.

Take any integer 1-cycle C in K extending D. Then $C-\widehat{\varphi}D$ is an integer 1-cycle that assigns 0's to all edges in $K\setminus T$. So by (a) integer 1-cycle $C-\widehat{\varphi}D$ also assigns 0's to all edges in T. So $C=\widehat{\varphi}D$.

1.8. (b) *Answer:* 2^{E-V+1}.

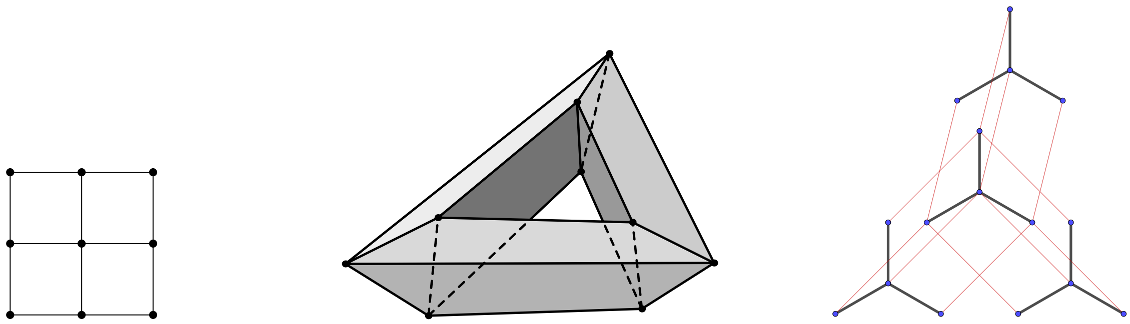


FIGURE 4. Left: $K_{2,1}^{\square 2}$ is the 3×3 grid graph. Middle: $K_3^{\square 2}$ on the torus K_3^2. Right: $K_{3,1}^{\square 2}$.

2.1. (a) The 3×3 grid graph, see Figure 4, left.

(b) See Figure 4, middle (where boundary cycles are drawn in grey). Alternatively, $K_3^{\square 2}$ is obtained from the graph in (a) by adding edges between corresponding vertices:
- of the 1st and the 3rd rows;
- of the 1st and the 3rd column.

(Compare to obtaining K_3 from the path 123 by adding an edge between 1 and 3.)

(c) See Figure 4, right.

(d) Vertices are nodes of a 4×4 grid. Two vertices are joined by an edge if and only if they are in the same row or in the same column.

2.2. (b) The triodic cycle in $K_{3,1}^{\square 2}$ equals $\sum\limits_{i,j\in[3],i\neq j} i1'j1'$.

(e,f) *Answers:* no.

(e) *Hint.* The left projection of any boundary (and hence of any sum of boundaries) is empty.

2.3. (a) We have $\operatorname{diag}(123) = 1\times K_3 + K_3\times 1 + 12\square 23 + 12\square 31 + 23\square 31$.

(b) The off-diagonal cycle in $K_3^{\square 2}$ equals $1\times K_3 + K_3\times 1 + 12\square 31 + 31\square 12$.

(c) The antidiagonal cycle in $K_3^{\square 2}$ equals $1\times K_3 + K_3\times 1 + 23\square 31 + 31\square 23 + 31\square 31$.

(d) We have $1\times C + C\times 1 = \operatorname{diag} C + \sum\limits_{i,j\in[n],i<j} i(i+1)\square j(j+1)$, where $n+1 := 1$.

(e) *Answer:* no.

2.4. *Answers:* (a) 2^2; (b) 2^2; (c) 2^4; (d) 2^6.

2.5. (a) Prove this by induction on the number of vertices of T, using deletion of a leaf vertex.

(b) This can be proved by induction on the number of pairs of edges of Z left-projected to the same edge of K. The inductive base when the number is zero can be proved by induction on the number of vertices b of K such that $Z\cap(b\times K)\neq\varnothing$. For the inductive step, take such a pair $\{(\sigma,v_1),(\sigma,v_k)\}$, take a path $v_1\ldots v_k$ in K, and replace Z by $Z+\sigma\square v_1v_2+\ldots+\sigma\square v_{k-1}v_k$.

(c) By (b), if $Z_x = Z_y = 0$, then $Z\sim 0$. Applying this to $Z = C + C_x\times a + a\times C_y$, we obtain the representation from (c). The uniqueness follows because the left and the right projections of sum of boundaries are equal to 0.

2.6. *Answers.* (a) The disjoint union of two copies of $K_{2,1}$.

(b) The cycle on 6 vertices.

(c) The cycle on 12 vertices.

(d) The union of edges of a cuboctahedron, see Figure 5.

2.7. *Answers.*

(a) 2^1; (b) 2^5; (c) 2^{17}; (d) 2^{13}; (e) 2^{43}; (f) 2^{41}.

(a') 2^1; (b') 2^1; (c') 2^5; (d') 2^7; (e') 2^8; (f') 2^{12}.

Hint. Apply 1.4.b to obtain (a)-(f).

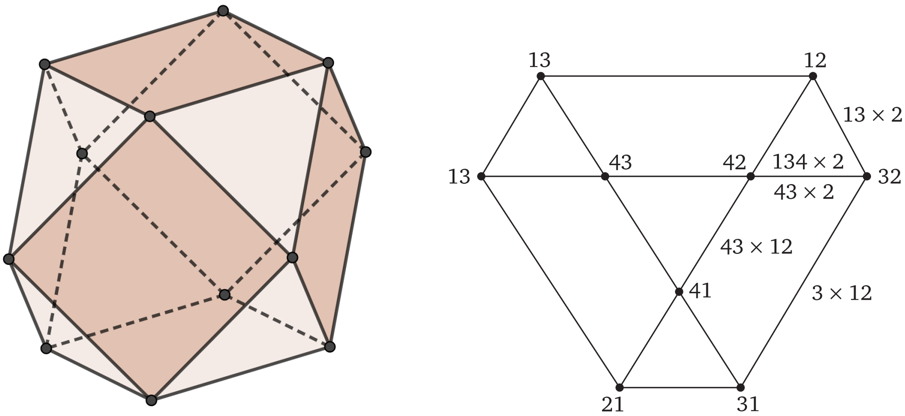


FIGURE 5. Left: cuboctahedron; the union of edges is $K_4^{\square 2}$ (three of the six boundaries are highlighted); the complement to triangular faces is $K_4^{\underline{2}}$.
Right: the same with some explanations; the figure does not show the invisible part whose projection is obtained from the pictured projection by rotation through $\pi/3$

Remark. Cf. examples before Problem 5.4.

2.8. (a) It suffices to prove the result for K connected. It suffices to prove that if a sum of pairwise distinct boundaries is a symmetric 1-cycle, then either the sum is zero, or there are two summands symmetric to each other. The analogous result for $K^{\square 2}$ replaced by $K \square T \bigcup\limits_{T \square T} T \square K$, where T is a tree, is proved by induction on the number of vertices in T, using deletion of a leaf vertex. For reduction of (a) to this analogous result, use the equality $\sum\limits_{i,j} \sigma_i \square \tau_j = 0$ for two simple cycles in K having consecutive edges $\sigma_1 \ldots \sigma_k$ and $\tau_1 \ldots \tau_\ell$. Using this equality we replace the given sum of boundaries by an equal sum not containing summands $\sigma \square \tau$ corresponding to edges σ, τ outside a maximal tree of K.

3.1. (c) It suffices to prove that an arbitraty 2-cycle C equals the sum $\widehat{C} := \sum\limits_{\{i,j,k\} \in C,\ i,j,k<n} T_{i,j,k,n}$ of tetrahedra $T_{i,j,k,n}$ over 3-element subsets $\{i,j,k\} \in C$ not containing n. This follows because every face in $C + \widehat{C}$ contains n, so by (b) we have $C + \widehat{C} = 0$, i.e., $C = \widehat{C}$.

(f) A rigorous formulation is as follows (we identify tetrahedra in $[n]$ with 4-element subsets of $[n]$). Suppose that R is a set of 4-element subsets of $[n]$ such that any 3-element subset of $[n]$ is contained in an even number of those 4-element subsets that are elements of R. Then there is a family R' of 5-element subsets of $[n]$ such that a 4-element subset B of $[n]$ is contained in R if and only if B is contained in an odd number of those 5-element subsets that are elements of R'.

This statement is a higher dimensional analogue of Assertion 3.1.c; the proof is analogous.

3.2. (c) For $a \in [n-1]^\ell$ denote by $P(a) := \{n, a_1\} \times \ldots \times \{n, a_\ell\}$ the parallelepiped with opposite vertices a and $(n, \ldots, n)$. It suffices to prove that any rook cycle $C \subset [n]^\ell$ equals the sum $\widehat{C}$ of parallelepipeds $P(a)$ over $a \in C \cap [n-1]^\ell$. The sum $C + \widehat{C}$ is a rook cycle. Since $P(a) \cap [n-1]^\ell = \{a\}$, we have $(C + \widehat{C}) \cap [n-1]^\ell = \varnothing$. By (b), we have $C + \widehat{C} = \varnothing$, i.e., $C = \widehat{C}$.

(f) *Hint.* Any parallelepiped P with some $P_i \subset [n-1]$ is a sum of some given relations and two parallelepipeds obtained from P by replacing with n one of the two elements in P_i. So in each of the two parallelepipeds the number of pairs P_j not containing n is smaller than in P. Hence any relation between parallelepipeds is a sum of some given relations and a relation $P(a_1) + \ldots + P(a_s) = 0$ for some pairwise distinct $a_1, \ldots, a_s \in [n-1]^\ell$. The latter relation is trivial because

$$\varnothing = (P(a_1) + \ldots + P(a_s)) \cap [n-1]^\ell = \{a_1, \ldots, a_s\}.$$

Here the second equality holds because $P(a) \cap [n-1]^\ell = \{a\}$.

4.2. Let $O, V, A_{11}, \ldots A_{1n}$ be points in $\mathbb{R}^3$ of which no 4 lie in the same plane. For every $p \in [n]$ take a point A_{2p} such that $\overrightarrow{OA_{2p}} = \overrightarrow{OV} + \overrightarrow{OA_{1p}}$. If V is close enough to O, then the points A_{jp}, $j \in \{1,2\}$, $p \in [n]$, are as required, i.e., the union of parallelograms $A_{1p}A_{2p}A_{2q}A_{1q}$ forms the drawing of the cylinder over K_n in $\mathbb{R}^3$.

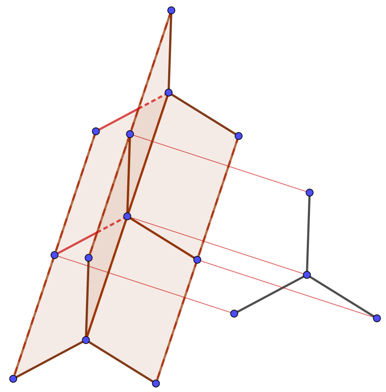


FIGURE 6. To drawing of $K_{3,1}^2$ in 3-space

4.3. (b) See Figure 6.

5.1. (b) In this proof by σ, τ we denote edges of K, and by v we denote a vertex of K:

$$C \text{ is a 2-cycle} \Leftrightarrow \begin{cases} |\{\sigma : \ \sigma \ni v, \ (\sigma,\tau) \in C\}| \text{ is even for any } v \text{ and } \tau \\ |\{\tau : \ \tau \ni v, \ (\sigma,\tau) \in C\}| \text{ is even for any } v \text{ and } \sigma \end{cases} \Leftrightarrow$$

$$\Leftrightarrow \begin{cases} |\{\sigma \in C_{\cdot,\tau} \ : \ \sigma \ni v\}| \text{ is even for any } v \text{ and } \tau \\ |\{\tau \in C_{\sigma,\cdot} \ : \ \sigma \ni v\}| \text{ is even for any } v \text{ and } \sigma \end{cases} \Leftrightarrow \begin{cases} C_{\cdot,\tau} \text{ is a 1-cycle for any } \tau \\ C_{\sigma,\cdot} \text{ is a 1-cycle for any } \sigma. \end{cases}$$

5.2. (a) Let $C := \widetilde{C}_1 \times \widetilde{C}_2 \subset K^2$ be the product of simple cycles $\widetilde{C}_1$ and $\widetilde{C}_2$ in K. For every edge σ of K the set $C_{\sigma,\cdot}$ is either $\widetilde{C}_2$ or the empty set. For every edge τ of K the set $C_{\cdot,\tau}$ is either $\widetilde{C}_1$ or the empty set. Hence by Assertion 5.1.b, C is a cellular 2-cycle.

(c) *Answer:* no.

Solution. Let C be a cellular 2-cycle in T^2. Since T is a tree, by Assertion 5.1.b $C_{\sigma,\cdot} = 0$ for any edge σ of T. Hence $C = 0$.

(d) *Answer:* no.

Solution. Let C be a cellular 2-cycle in $\overline{T}$. Since T is a tree, by Assertion 5.1.b $C_{\sigma,\cdot} = 0$ for any edge σ of $K \setminus T$. Hence $C \subset T \times K$. Since T is a tree, by Assertion 5.1.b $C_{\cdot,\sigma} = 0$ for any edge σ of K. Hence $C = 0$.

5.3. *Answers:* (a) 2; (b) 2; (c) 2^4; (d) 2^9.

Solutions.

(a, b) Let C be a cellular 2-cycle in K^2 such that $C \neq K$, i.e., $(\sigma,\tau) \notin C$ for some edges σ, τ in K. By Assertion 5.1.b, $C_{\sigma,\cdot}$ is a 1-cycle. Since K is a cycle graph, $C_{\sigma,\cdot} = 0$. Then $(\sigma,\sigma) \notin C$. Hence $C \subset \overline{K - \sigma}$. By answer to Problem 5.2.d, $C = 0$.

(c) By answer to Problem 5.5.d, the number of 2-cycles in $K_{2,3}^2$ equals $2^{(E-V+1)^2} = 2^{2^2} = 16$.

(d) By answer to Problem 5.5.d, the number of 2-cycles in K_4^2 equals $2^{(E-V+1)^2} = 2^{3^2} = 2^9 = 512$.

5.4. (a) *Answer:* no.

Solution. Let C be a cellular 2-cycle in $K^{\underline{2}}$. Take an edge σ of K. By Assertion 5.1.b, $C_{\sigma,\cdot}$ is a 1-cycle. Since $C_{\sigma,\cdot}$ is a subset of the path graph $K - \sigma$, then $C_{\sigma,\cdot} = 0$. Hence $C = 0$.

(b) *Answer:* no.

Solution. Let C be a cellular 2-cycle in $K^{\underline{2}}$. By Assertion 5.1.b, $C_{\sigma,\cdot}$, $C_{\cdot,\sigma}$ are 1-cycles for any edge σ of K. Since both $C_{0j,\cdot}$ and $C_{\cdot,0j}$ are subsets of the path graph $K-0-j$ for any $j\in[n]$, then $C_{0j,\cdot}=C_{\cdot,0j}=0$ for any $j\in[n]$. Then $C\subset(K-0)^{\underline{2}}$ for the cycle graph $K-0$. Hence by (a), $C=0$.

(c) Denote $C:=K_{3,3}^{\underline{2}}$. For any edge σ in $K_{3,3}$ both $C_{\sigma,\cdot}$ and $C_{\cdot,\sigma}$ are cycles of length 4. Then the required result follows by Assertion 5.1.b.

(d) Denote $C:=K_5^{\underline{2}}$. For any edge σ in K_5 both $C_{\sigma,\cdot}$ and $C_{\cdot,\sigma}$ are cycles of length 3. Then the required result follows by Assertion 5.1.b.

(e) Take $K:=K_6$ and $C:=123\times456$. Since $(12,34)\notin C$, the product C is a non-empty proper subset of $K^{\underline{2}}$. By Assertion 5.2.a, the product C of cycles is a cellular 2-cycle.

5.5. (a, b) *Hint:* the required representations can be obtained from the proof of (c).

(c) Part (c) easily follows from the particular case of connected K, which we further assume.

Let T be a maximal tree of K. Define a map

$$\varphi\colon H_2(K^2)\to 2^{K^2-\overline{T}}\quad\text{by}\quad \varphi C:=C\cap(K^2-\overline{T}).$$

For any edge $\sigma\in K\setminus T$ the 1-cycle $\widehat{\varphi}\sigma$ is defined in the proof of Assertion 1.4.b. Define a map

$$\widehat{\varphi}\colon 2^{K^2-\overline{T}}\to H_2(K^2)\quad\text{by}\quad \widehat{\varphi}D:=\sum_{(\sigma,\tau)\in D}\widehat{\varphi}\sigma\times\widehat{\varphi}\tau.$$

By Assertion 5.2.d, $\widehat{\varphi}\varphi C=C$ for any $C\in H_2(K^2)$, i.e., an arbitraty cellular 2-cycle C in K^2 is the sum of tori $\widehat{\varphi}\sigma\times\widehat{\varphi}\tau$ over $(\sigma,\tau)\in\varphi C$.

(d) *Answer:* $2^{(E-V+1)^2}$.

Solution. In (c), we defined maps $\varphi: H_2(K^2)\to 2^{K^2-\overline{T}}$ and $\widehat{\varphi}: 2^{K^2-\overline{T}}\to H_2(K^2)$ for a maximal tree T of connected graph K and proved that $\widehat{\varphi}\varphi C=C$ for any $C\in H_2(K^2)$. In addition, $\varphi\widehat{\varphi}D=D$ for any $D\in 2^{K^2-\overline{T}}$. Thus, φ is a 1–1 correspondence. Hence

$$|H_2(K^2)|=|2^{K^2-\overline{T}}|=|2^{(K\setminus T)^2}|=2^{(E-V+1)^2}.$$

5.6. (b) Denote $B:=\{C_i\times C_j\ :\ i,j\in[q]\}$. In the following two paragraphs we prove that every 2-cycle in K^2 is a sum of some 2-cycles from B, and that such a representation is unique, respectively.

Apply Assertion 5.5.c. Every torus $\widetilde{C}_1\times\widetilde{C}_2\subset K^2$ is in turn a sum of some 2-cycles from B, because both $\widetilde{C}_1$ and $\widetilde{C}_2$ are sums of some 1-cycles from $C_1,\dots,C_q$.

Denote by N the number of connected components of K. Analogously to Assertion 1.4.b, $|H_1(K)|=2^{E-V+N}$. Since $C_1,\dots,C_q$ is a base in $H_1(K)$, it follows that $2^q=|H_1(K)|$, so $q=E-V+N$. Therefore $|B|=q^2=(E-V+N)^2$. By generalization of the answer to Problem 5.5.d to an arbitrary graph K, we have $|H_2(K^2)|=2^{(E-V+N)^2}$, which is the number of linear combinations of 2-cycles from B. This implies the uniqueness.

5.7. (a) *Hint:* this follows by Assertion 5.1.b.

(b) *Answer:* no.

Solution. Take $K:=K_5$ (or $K:=K_{3,3}$) and $C:=K^{\underline{2}}$. By Assertion 5.4.c (or 5.4.d), C is a cellular 2-cycle. Since there are no two non-empty vertex-disjoint cycles in K, the 2-cycle C is not a sum of some products of vertex-disjoint cycles.

5.8. (a) *Answer:* $2^{(n^2-3n+1)^2}$.

(c) *Hint.* The 1–1 correspondence is defined by the formula $f(\sigma_1\sigma_2',\tau_1\tau_2'):=(\sigma_1\tau_1',\sigma_2\tau_2')$ for disjoint edges $\sigma,\tau\in[n]^2$. (Recall that for $a,b\in[n]$ we denote by ab' the edge joining a and b'.) Cells $\alpha,\beta\in[n]\times[n]'\times[n]\times[n]'$ in $K_{n,n}^{\underline{2}}$ are adjacent if and only if they differ only at one of their four coordinates. Since $K_{n,n}^{\underline{2}},\widetilde{K_n}^2\subset K_{n,n}^{\underline{2}}$, it follows that α and β in $K_{n,n}^{\underline{2}}$ are adjacent if and only if $f\alpha$ and $f\beta$ in $\widetilde{K_n}^2$ are adjacent, i.e., f respects the adjacence.

Remark. Define a 1–1 correspondence $\widehat{f}$ between edges of $K_{n,n}^{\square 2}$ and edges of $\widetilde{K_n}^{\square 2}$ by skipping one of $\sigma_1,\sigma_2',\tau_1,\tau_2'$ in the formula for f (e.g. $\widehat{f}(\sigma_1,\tau_1\tau_2')=(\sigma_1\tau_1',\tau_2'))$. One can check that the correspondences $f, \widehat{f}$ respect incidence. (Recall that an edge η and a 2-cell $\alpha = (\xi, \zeta)$ are *incident* if $\eta = \xi$ or $\eta = \zeta$.) Note that there is no 1–1 correspondence between vertices that saves incidence. Indeed, there is no 1–1 correspondence between 1-cycles in $K_{n,n}^{\square \underline{2}}$ and in $\widetilde{K_n}^{\square 2}$. E.g. for $n = 3$ we have $|H_1(\widetilde{K_3}^{\square 2})| = 2^{37}$, as opposed to the answer to Problem 2.7.e; besides, in $\widetilde{K_3}^{\square 2}$ there are four 1-cycles up to boundaries, as opposed to the answer to Problem 2.7.e'.

5.9. (c) *Answer:* no.

Solution. Take $K = K_3$ and $C = K^2$. Then C is a non-empty symmetric cellular 2-cycle in K^2. Since $K \times K + K \times K = 0$, there are no non-empty symmetrized tori in K^2. Hence C is not a sum of some symmetrized tori.

5.10. (a) For any symmetric cellular 2-cycle C in $K^{\underline{2}}$ we have

$$C \overset{(1)}{=} \sum_{(\sigma,\tau) \in C - \overline{T}} \widehat{\varphi}\sigma \times \widehat{\varphi}\tau \overset{(2)}{=} \sum_{\{\sigma,\tau\}:\ (\sigma,\tau) \in C - \overline{T}} (\widehat{\varphi}\sigma \times \widehat{\varphi}\tau + \widehat{\varphi}\tau \times \widehat{\varphi}\sigma).$$

Here

- (1) holds by the formula in the hint to Assertion 5.5.c, and
- (2) holds because $C - \overline{T}$ is symmetric, and $C - \overline{T} \subset C \subset K^{\underline{2}}$, so $\sigma \neq \tau$ for any pair $(\sigma, \tau) \in C - \overline{T}$.

(c,d,e) See the details in [SS23].

References

[CPG] * https://en.wikipedia.org/wiki/Cartesian_product_of_graphs

[FH10] *M. Farber, E. Hanbury.* Topology of Configuration Space of Two Particles on a Graph, II. Algebr. Geom. Topol. 10 (2010) 2203–2227. arXiv:1005.2300.

[MS17] *T. Maciazek, A. Sawicki.* Homology groups for particles on one-connected graphs J. Math. Phys. 58, 062103 (2017). arXiv:1606.03414.

[Sa91] *K. S. Sarkaria.* A one-dimensional Whitney trick and Kuratowski's graph planarity criterion, Israel J. Math. 73 (1991), 79–89. http://kssarkaria.org/docs/One-dimensional.pdf.

[Sk06] * *A. Skopenkov,* Embedding and knotting of manifolds in Euclidean spaces, London Math. Soc. Lect. Notes, 347 (2008) 248–342. arXiv:math/0604045.

[Sk14] * *A. Skopenkov,* Realizability of hypergraphs and intrinsic linking theory, Mat. Prosveschenie, to appear, arXiv:1402.0658.

[Sk18] * *A. Skopenkov.* Invariants of graph drawings in the plane. Arnold Math. J., 6 (2020) 21–55; full version: arXiv:1805.10237.

[Sk20] * *A. Skopenkov,* Algebraic Topology From Geometric Standpoint (in Russian), MCCME, Moscow, 2020 (2nd edition). Part of the book: http://www.mccme.ru/circles/oim/obstruct.pdf . Part of the English translation: https://www.mccme.ru/circles/oim/obstructeng.pdf.

[Sk21m] * *A. Skopenkov.* Mathematics via Problems. Part 1: Algebra. Amer. Math. Soc., Providence, 2021. Preliminary version: https://www.mccme.ru/circles/oim/algebra_eng.pdf

[Sk] * *A. Skopenkov.* Algebraic Topology From Algorithmic Standpoint, draft of a book, mostly in Russian, http://www.mccme.ru/circles/oim/algor.pdf.

[SS23] A. Skopenkov and O. Styrt, Embeddability of join powers and minimal rank of partial matrices, arXiv:2305.06339.

Books, surveys and expository papers in this list are marked by the stars.

arXiv is an open-access archive of papers on mathematics, computer science, and other topics. To access a paper enter the identifier (e.g. arXiv:1005.2300) in the search bar of arxiv.org. Googling the identifier usually works as well.

Декомпозиции многочленов, или Первая теорема Ритта

Авторы: Я. Абрамов, А. Петухов, А. Тертерян

1 Вступление

Этот проект мотивирован задачей о классификации коммутирующих многочленов, т.е. таких пар многочленов $f(x)$ и $g(x)$ одной переменной, что $f(g(x)) = g(f(x))$. Предлагаем читателю самому поискать несколько таких пар. В дальнейшем мы будем обозначать композицию многочленов одной переменной так:

$$f \circ g = f(g(x)).$$

Данный проект посвящен изучению вспомогательной задачи разложения многочлена в функциональную композицию других: $F(x) = A \circ B = A(B(x))$. Эта задача возникает естественно и является частью задачи классификации коммутирующих многочленов. Естественно изучать разложение в композицию многочленов, далее неразложимых. Мы придём к следующему результату о разложении произвольного многочлена в неразложимые далее многочлены, сильно напоминающему теорему о разложении числа на простые множители.

Первая теорема Ритта. Для двух разложений многочлена в композицию неразложимых многочленов

$$F(x) = G_1 \circ \ldots \circ G_r = H_1 \circ \ldots \circ H_s$$

(где $\deg G_i > 1$, $\deg H_j > 1$) выполняется следующее:
1) $r = s$, т.е. длина разложения одинакова,
2) наборы степеней многочленов разложения $(\deg G_1, \ldots, \deg G_r)$ и $(\deg H_1, \ldots, \deg H_r)$ получаются друг из друга перестановкой членов,
3) существует последовательность промежуточных разложений $F = F_1^{[i]} \circ \ldots \circ F_r^{[i]}$, такая что

$$F_i^{[1]} = G_i \ (1 \leq i \leq r),$$

два соседних члена в последовательности отличаются только заменой двух соседних многочленов (степени переставляются при замене и взаимно просты) и

$$F_i^{[n]} = l \circ H_i \circ l^{-1} \ (1 \leq i \leq r),$$

где $l(x)$ — какая-то линейная функция, а $l^{-1}(x)$ — обратная к ней, т.е. такая что $l(l^{-1}(x)) = x$.

Пример. Для разложений $x^{12} = x^3 \circ x^2 \circ x^2 = x^2 \circ x^2 \circ x^3$ промежуточная последовательность состоит из ещё одного разложения $x^{12} = x^2 \circ x^3 \circ x^2$.

Обозначения:

В дальнейшем будем считать, что:
i, j, k, l, m, n — какие-то натуральные числа;
$A, B, C, D, F, G, H, P, Q, R, S, T$ — какие-то многочлены (одной переменной, если не указано иное), x, y, z — переменные многочленов;
a, b, c, d — какие-то действительные числа;
M, N — какие-то множества.

2 Задачи без подсказок

В дальнейшем при решении любой задачи можно ссылаться на результаты любой предыдущей.

1. Докажите, что существует такой многочлен
а) $T_2(x)$, б) $T_3(x)$, в) $T_4(x)$, г) $T_n(x)$,
что $T_n(\cos t) = \cos nt$ при любом натуральном n. Выразите $T_{n+2}(x)$ через $T_{n+1}(x)$ и $T_n(x)$.

Определение 1. Многочлен $T_n(x)$ называется <u>n-м многочленом Чебышёва</u>.

2. Докажите, что существует такой многочлен
а) $D_2(x)$,
б) $D_3(x)$,
в) $D_4(x)$,
г) $D_n(x)$,
что $D_n(t+\frac{1}{t}) = t^n + \frac{1}{t^n}$ при любом натуральном n.
Выразите $D_{n+2}(x)$ через $D_{n+1}(x)$ и $D_n(x)$.

Определение 2. Многочлен $D_n(x)$ называется n-м многочленом Диксона.

Определение 3. Декомпозицией многочлена f называется такая последовательность многочленов $f_1, \ldots, f_r$, что $f = f_1 \circ \ldots \circ f_r$. Назовём многочлены, получающиеся друг из друга преобразованием вида $f \to l^{-1} \circ f \circ l$ (где $l(x)$ — линейная функция), сопряжёнными. Назовём две декомпозиции $f_1, \ldots, f_r$ и $g_1, \ldots, g_r$ многочлена f сопряжёнными, если $f_i = l_i^{-1} \circ g_i \circ l_{i+1}$, где $l_i(x)$ — линейная функция, $l_1 = x$, $l_{r+1} = x$.

3. Разложите многочлен а) $T_m(x)$, б) $D_m(x)$ в композицию неразложимых.

4. а) Пусть $F = G \circ H$. Докажите, что $F(x)-F(y)$ как многочлен от x, y делится на $H(x)-H(y)$.
б) Пусть даны многочлены $A(x)$ и $B(x)$. Докажите, что существует не более одного многочлена $C(x)$, такого что $A = C \circ B$.
в) Пусть $F = G \circ H$. Докажите, что $F'(x)$ делится как многочлен на $H'(x)$.

Определение 4. Многочлен называют *приведённым*, если его старший коэффициент равен 1.

5. Докажите, что количество декомпозиций приведённого многочлена без свободного члена в композицию приведённых многочленов без свободных членов конечно.

6. Докажите, что
а) для любого приведённого многочлена $A(x)$, такого что $\deg A = nr$, существует и единственен такой приведённый $C(x)$, что $\deg(A - C^r) < n(r-1)$,
б) а если ещё есть декомпозиция $A = P \circ Q$, $\deg Q = n$, то $A = B \circ C$.

7. а) Пусть остаток от деления многочлена $G(x)$ на $H(x)$ равен $R(x)$. Докажите, что остаток от деления $G(F(x))$ на $H(F(x))$ равен $R(F(x))$.
б) Пусть $F = P \circ A = Q \circ B$. Докажите, что $F = R \circ C$, где $\deg C = HOK(\deg A, \deg B)$, $C = A_1 \circ A = B_1 \circ B$.

8. а) Пусть $P \circ A = P \circ B$, где A и B — приведённые многочлены. Докажите, что $A = B$.
б) Пусть $C \circ F = D \circ F$, где F — приведённый многочлен. Докажите, что $C = D$.

9. * Пусть $F = P \circ A = Q \circ B$. Докажите, что $F = R \circ C$, где $\deg C = (\deg A, \deg B)$.

10. Пусть $f_1, \ldots, f_r$ и $g_1, \ldots, g_r$ — две декомпозиции многочлена $F(x)$ (причём все f_i и g_i неразложимы) и $\deg f_i = \deg g_i$. Докажите, что эти две декомпозиции сопряжены.

11. * **(Первая теорема Ритта, сформулированная в новых терминах)**[1] Докажите, что для двух декомпозиций многочлена в неразложимые $F = G_1 \circ \ldots \circ G_r = H_1 \circ \ldots \circ H_s$ ($\deg G_i > 1$, $\deg H_j > 1$) верно следующее:
1) $r = s$,
2) последовательности ($\deg G_1, \ldots, \deg G_r$) и ($\deg H_1, \ldots, \deg H_r$) являются перестановками друг друга,
3) существует последовательность декомпозиций $F = F_1^{[i]} \circ \ldots \circ F_r^{[i]}$, такая что две соседних декомпозиции в ней отличаются только заменой двух соседних полиномов (степени переставляются при замене и взаимно просты),

$F_i^{[1]} = G_i$ $(1 \le i \le r)$,

$(F_1^{[n]}, \ldots, F_r^{[n]})$ сопряжена $(H_1, \ldots, H_r)$.

[1] **Вспомогательные задачи с подсказками по задачам со звездочками будут выданы 4.08 и 7.08.**

3 Теорема Ритта: первая порция вспомогательных задач

12. Пусть $F(x) = G(H(x))$, $\deg G = m$, $\deg H = n$. Определим многочлены n переменных e_i так: $\sum_{i=0}^{n} t^i e_i(y_1, y_2, \dots, y_n) = (t - y_1)(t - y_2)\dots(t - y_n)$ (они называются элементарными симметрическими многочленами). Пусть у многочлена $F(x)$ ровно mn корней. Докажите, что корни многочлена $F(x)$ можно разбить на m групп по n штук $c_{11}, \dots, c_{1n}, c_{21}, \dots, c_{mn}$ так, чтобы при $i > 0$ было $e_i(c_{11}, c_{12}, \dots, c_{1n}) = e_i(c_{21}, c_{22}, \dots, c_{2n}) = \dots = e_i(c_{m1}, c_{m2}, \dots, c_{mn})$.

13. Может ли быть $(x-1)(x-2)\dots(x-999)$ композицией многочленов степеней 27 и 37?

Ещё при решении предыдущего раздела нам пригождалась идея множества всевозможных выражений от данного многочлена, либо выражений от нескольких данных многочленов. Эта идея обобщается до понятий из высшей математики: колец и полей. Кольца — это всё, что можно получить из данного множества путём сложения, вычитания и умножения, а также добавления констант. А поля — то же самое, но ещё и с операцией деления! Нам пригодится теорема Люрота (задача в конце листка).

3.1 Кольца

Определение 5. *Кольцом*[2] называют множество R с тремя операциями на нём, называемыми сложением $(a+b)$, умножением $(a \cdot b)$ и взятием противоположного $(-a)$, причём эти операции удовлетворяют следующим условиям:

переместительные законы: 1) $a \cdot b = b \cdot a$, 2) $a + b = b + a$,
сочетательные законы: 3) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, 4) $a + (b + c) = (a + b) + c$,
распределительный закон: 5) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
свойства нуля: 6) есть такой элемент $0 \in R$, что $a + 0 = a$ для любого $a \in R$, 7) $a + (-a) = 0$,
8) существует такой элемент $1 \in R$, что $a \cdot 1 = a$ для любого $a \in R$.

Примеры. Как известно из школьной программы, множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ с естественнными операциями удовлетворяют этим условиям.

14 (Упражнение)**.** Для произвольного кольца M опишите (введите) операции сложения, умножения и взятия противоположного на множестве всех многочленов с коэффициентами в M (аналогичные операциям на многочленах с действительными коэффициентами).

Определение 6. Описанное выше кольцо мы обозначим через $M[x]$ (где x — переменная, M — множество коэффициентов).

Пример. Для кольца многочленов от n переменных $\mathbb{R}[x_1, \dots, x_n]$ соответствующее $\mathbb{R}[x_1, \dots, x_n][y]$ — кольцо многочленов от $(n+1)$ переменных $\mathbb{R}[x_1, \dots, x_n, y]$.

Определение 7. Подмножество A в кольце R называется *подкольцом*, если операции сложения, умножения и взятия противоположного не выводят из множества A (то есть если $a, b \in A$, то $a + b, a \cdot b, (-a) \in A$).

Продемонстрируем, что даёт понятие кольца, каким мощным инструментом оно является.

15. Эта задача посвящена доказательству следующей теоремы: если дана последовательность многочленов $f_1(x), \dots, f_n(x), \dots$, то существует такое k, что для любого n выполняется

$$f_n(x) = F_n(f_1(x), \dots, f_k(x)),$$

где $F_n(y_1, \dots, y_k)$ — многочлены.
а) Пусть M — множество всех выражений, получающихся из элементов этой последовательности многочленов многократным применением операций сложения, умножения, вычитания и умножения на константу. Докажите, что M образует подкольцо в кольце многочленов от x.
б) Пусть N — множество всех степеней элементов из M (т.е. всех целых чисел $\deg f$ для f

[2] А точнее, коммутативным кольцом с единицей.

из M). Докажите, что оно замкнуто относительно умножения его элементов на произвольные натуральные числа и сложения его элементов.
в) Докажите, что в множество N порождено относительно сложения и умножения на натуральные числа всего лишь конечным числом его элементов: любой его элемент получается в результате нескольких таких операций из фиксированного конечного набора в N.
г) Докажите, что подкольцо M порождено всего лишь конечным числом его элементов.
д) Докажите теорему.

3.2 Поля

Определение 8. *Полем* называют множество $\mathbb{F}$ с четырьмя операциями на нём, называемыми сложением $(a+b)$, умножением $(a \cdot b)$, взятием противоположного $(-a)$ и взятием обратного для ненулевого элемента (a^{-1}), причём эти операции удовлетворяют следующим условиям:

1-8) те же свойства, что и в определении 5 кольца,

9) $a \cdot a^{-1} = 1$ для любого $a \neq 0$ из $\mathbb{F}$.

Примеры. Множества $\mathbb{Q}$, $\mathbb{R}$ с естественными операциями удовлетворяют этим условиям.

Замечание. Не все привычные операции определены в полях. Например операция извлечения квадратного корня обычно невыполнима в поле $\mathbb{Q}$ (как известно, $\sqrt{2} \notin \mathbb{Q}$).

16 (Упражнение)**.** Для поля $\mathbb{F}$ введите (опишите) операции сложения, умножения, взятия противоложного и взятия обратного на множестве всех рациональных функций (выражений вида $\frac{P(x)}{Q(x)}$, где P, Q — многочлены, причём считается, что $\frac{A(x)B(x)}{A(x)C(x)} = \frac{B(x)}{C(x)}$) с коэффициентами в $\mathbb{F}$ (аналогичные операциям на рациональных функциях с действительными коэффициентами).

Определение 9. Описанное выше поле обозначим через $\mathbb{F}(x)$.

17 (Деление многочленов с остатком)**.** Докажите, что для многочленов $A(x), B(x) \in \mathbb{F}[x]$ $(B(x) \neq 0)$ найдутся такие многочлены $Q(x), R(x) \in \mathbb{F}[x]$, что $A = B \cdot Q + R$ и $\deg B > \deg R$.

18 (Упражнение на понимание)**.** Разделите с остатком многочлены от x с коэффициентами в поле $\mathbb{R}(y, z)$ (т.е. найдите многочлены $Q(x)$ и $R(x)$ из предыдущей задачи, причём коэффициенты этих многочленов можно брать в виде рациональных функций от y и z):
а) $(x+y+z)^3 - x^3 - y^3 - z^3$ на $x+y$, б) $(x+y+z)^5 - x^5 - y^5 - z^5$ на $(x+y)(x+z)$.

19 (Наибольший общий делитель многочленов)**.** Докажите, что для многочленов $A(x), B(x) \in \mathbb{F}[x]$ а) существует $HOD(A(x), B(x))$ б) и $HOD(A(x), B(x)) = A(x)P(x) + B(x)Q(x)$ для некоторых $P(x)$, $Q(x) \in \mathbb{F}[x]$.

20 (Вариант леммы Гаусса)**.** Пусть $C(x), D(x)$ — два многочлена из $S[x]$, где S — кольцо многочленов $\mathbb{R}[t]$ (т.е. C и D — многочлены от x, а их коэффициенты — многочлены от t). Докажите, что у их произведения $C(x)D(x)$ все коэффициенты взаимно просты в $\mathbb{S}[t]$ (т.е. взаимно просты как многочлены от t), если у каждого из них коэффициенты взаимно просты (как многочлены от t).

Определение 10. Подмножество A в поле $\mathbb{F}$ называется *подполем*, если операции сложения, умножения, взятия противоположного и взятия обратного не выводят из множества A (то есть если $a, b \in A$, то $a+b, a \cdot b, (-a) \in A$ и если $a \neq 0$, то $a^{-1} \in A$).

21. Докажите, что множество всех $E(g(x))$, где $g(x)$ — фиксированная, а $E(x)$ — произвольная рациональные функции, является подполем в $\mathbb{R}(x)$.

22 (Теорема Люрота[3])**.** * Докажите, что любое промежуточное подполе $\mathbb{R} \subset K \subset \mathbb{R}(x)$ является полем рациональных функций от какой-нибудь рациональной функции $g(x)$: $K = \mathbb{R}(g(x))$.

23. Докажите, что если в промежуточном подполе $\mathbb{R} \subset K \subset \mathbb{R}(x)$ лежит многочлен, то образующую $g(x)$ в теореме Люрота можно выбрать тоже многочленом.

24. Докажите, что многочлен F *неразложим* тогда и только тогда, когда любое промежуточное подполе $\mathbb{R}(F) \subset L \subset \mathbb{R}(x)$ — это либо $\mathbb{R}(F)$, либо $\mathbb{R}(x)$.

[3]**Вторая порция вспомогательных задач с подсказками по теоремам Ритта и Люрота будет 7.08.**

4 Теорема Ритта: вторая порция вспомогательных задач

4.1 Теорема Люрота и «её применения в народном хозяйстве»

Определение 11. *Степенью* рациональной функции, представимой в виде несократимой дроби $\frac{p(x)}{q(x)} \neq 0$, называют $\max\{\deg p(x), \deg q(x)\}$.

25. Докажите, что для $a, b, c, d \in \mathbb{F}$, $h(x) \in \mathbb{F}(x)$, $ad - bc \neq 0$ степень $\frac{ah(x)+b}{ch(x)+d}$ равна степени $h(x)$.

Определение 12. Назовём подмножество M в поле $\mathbb{F} \subset \mathbb{R}(x)$ *порождающим*, если из его элементов можно получить все элементы поля $\mathbb{F}$, многократно применяя операции сложения, умножения, взятия противоположного, взятия обратного и умножения на константу.

26. (теорема Люрота)
Эта задача посвящена доказательству следующей теоремы: для любого поля K, такого что $\mathbb{R} \subset K \subset \mathbb{R}(x)$, найдётся такая $z(x) \in \mathbb{R}(x)$, что $K = \mathbb{R}(z(x))$. Мы приведём алгоритм построения такой функции $z(x)$.
Для рациональной функции $g(x)$ обозначим через $P_g(x)$ и $Q_g(x)$ многочлены, являющиеся её числителем и знаменателем:

$$g(x) = \frac{P_g(x)}{Q_g(x)},$$

где $(P_g, Q_g) = 1$ и $Q_g(x)$ — приведённый.
Изучим для рациональной функции $g(x)$ вспомогательное выражение $P_g(y) - g(x)Q_g(y)$ от переменных x, y. Заметим, что оно принадлежит кольцу $\mathbb{R}(g(x))[y]$ (т.е. является многочленом от y с коэффициентами в поле $\mathbb{R}(g(x))$).
а) Допустим, что M — множество (не обязательно конечное), порождающее промежуточное подполе K. Для всех $g(x) \in M$ рассмотрим наибольший общий делитель наших выражений

$$HOD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big) = \frac{D(x,y)}{d(x)},$$

где $D(x, y)$ и $d(x)$ — многочлены. Докажите, что $D(x, y)$ делится на $y - x$.
б) Докажите, что $HOD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big)$, если разделить его на старший коэффициент, будет иметь коэффициенты в поле K.
в) Докажите, что

$$P_g(x)Q_g(y) - P_g(y)Q_g(x) = D(x, y)C_g(x, y),$$

где $C_g(x, y)$ — многочлен от x, y.
г) Пусть m — наименьшая степень рациональной функции из M и $f(x) \in M$ — такая рациональная функция, что $\deg f = m$. Докажите, что если $\deg_y D(x, y) < m$, то $\deg_x C_f(x, y) > 0$ и $\deg_x D(x, y) < m$.
д) Пусть $\deg_y D(x, y) < m$. Докажите, что все коэффициенты $\frac{D(x,y)}{d(x)}$ как многочлена от y лежат в поле K и имеют степень меньше, чем m.
е) Определим следующую процедуру над множеством M: добавим к нему все непостоянные коэффициенты многочлена $\frac{D(x,y)}{d(x)}$ и назовём полученное множество $M_{(1)}$. Затем построим по множеству $M_{(1)}$ многочлен $\frac{D_1(x,y)}{d_1(x)} = HOD_{g\in M_{(1)}}\Big(P_g(y) - g(x)Q_g(y)\Big)$ и добавим его непостоянные коэффициенты, получив множество $M_{(2)}$, и т.д. Докажите, что повторяя эту процедуру мы придём к ситуации, когда

$$HOD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big) = c(x)(P_h(y) - h(x)Q_h(y))$$

для некоторого $h(x) \in M$.
ж) Докажите, что $P_h(y) - h(x)Q_h(y)$ (где h — из предыдущего пункта) неразложим на множители в кольце $\mathbb{R}[h(x), y]$.

з) Докажите, что $P_g(y)$ не делится на $P_h(y) - h(x)Q_h(y)$ над полем $\mathbb{R}(h(x))$.
(**Замечание:** напомним, что коэффициенты $P_g(y)$ — вещественные числа, а значит, принадлежат полю $\mathbb{R}(h(x))$).
и) Пусть для некоторого $u(x) \in M$ остатки от деления $P_u(y)$ и $Q_u(y)$ на $P_h(y) - h(x)Q_h(y)$ над полем $\mathbb{R}(h(x))$ равны $\frac{Q(h(x),y)}{q(h(x))}$ и $\frac{S(h(x),y)}{s(h(x))}$ соответственно. Докажите, что $\frac{Q(h(x),y)}{q(h(x))} = u(x)\frac{S(h(x),y)}{s(h(x))}$
к) Докажите, что $u(x)$ из предыдущего пункта принадлежит $\mathbb{R}(h(x))$.
л) Докажите, что $K = \mathbb{R}(h(x))$.

27. Докажите, что если $K = \mathbb{R}(h_1(x))$, то $h_1(x) = \frac{ah(x)+b}{ch(x)+d}$.

4.2 Остаток доказательства первой теоремы Ритта

Определение 13. Для двух полей K, L, таких что $\mathbb{R} \subset K \subset L \subset \mathbb{R}(x)$, назовём степенью расширения полей $[L\colon K]$ следующее число. Если $L = \mathbb{R}(f(x))$, то $K = \mathbb{R}(g(f(x)))$ (по теореме Люрота). Степенью $[L\colon K]$ назовём степень рациональной функции $g(x)$.

28. Докажите, что определение степени корректно (не зависит от выбора образующих в подполях).

29. Пусть $H = r(F)$, где H, F — многочлены, а r — рациональная функция. Докажите, что r — многочлен.

30. Докажите, что степени $[\mathbb{R}(F)\colon (\mathbb{R}(F) \cap \mathbb{R}(G))]$ и $[\mathbb{R}(G)\colon (\mathbb{R}(F) \cap \mathbb{R}(G))]$ взаимно просты.

31. а) Пусть $R(y,z)$ — ненулевой многочлен, $f(x)$ — рациональная функция и $R(f(x),x) = 0$ — тождество. Докажите, что $\deg_z R(y,z) \geqslant \deg f(x)$.
б) Пусть $h(x)$ — рациональная функция. Найдите ненулевой многочлен $T(y,z)$ наименьшей возможной степени по z, такой что $T(f(x),x) = 0$ — тождество.
в) Пусть $S(y,z)$ — ненулевой многочлен, $g(x) \in L \subset \mathbb{R}(x)$ и $R(g(x),x) = 0$ — тождество. Докажите, что $\deg_z S(y,z) \geqslant [L\colon \mathbb{R}(x)]$.

32. Пусть $H(x)$ — многочлен, такой что $\mathbb{R}(H)$ — поле, порождённое многочленами $F(x)$ и $G(x)$. Докажите, что $\deg H = HOD(\deg F, \deg G)$.

33. (Вспоминаем задачу 9*.) Докажите, что если $F(x) = P(A(x)) = Q(B(x))$, то существует такой многочлен $C(x)$, что $\deg C = HOD(\deg A, \deg B)$ и $A(x) = A_1(C(x))$, $B = B_1(C(x))$.

34. Докажите, что многочлены A_1 и A_2 порождают одно и то же подполе тогда и только тогда, когда $A_1 = aA_2 + b$.

35. (Конец доказательства первой теоремы Ритта.)
а) Пусть $\mathbb{R}(G_r) \neq \mathbb{R}(H_s)$. Докажите, что $\mathbb{R}(P) = \mathbb{R}(G_r) \cap \mathbb{R}(H_s)$, где P — многочлен степени $\deg G_r \cdot \deg H_s$.
б) Пусть многочлен P из предыдущего пункта таков, что $P = A \circ G_r$ и $A = A_1 \circ A_2$. Докажите, что тогда либо $\mathbb{R}(P) = \mathbb{R}(A_2 \circ G_r)$ (и тогда $\deg A_1 = 1$), либо $\mathbb{R}(H_s, A_2 \circ G_r) = \mathbb{R}(x)$ (и тогда $\deg A_1 = \deg A$).
в) Докажите первую теорему Ритта.

36. *** Попробуйте придумать аналоги сформулированных лемм и теорем для рациональных функций. Что-то, конечно, тривиально. Можно учитывать, например, то, что обобщением понятия степени для рациональных функций является кратность корня a для функции $f(x) - f(a)$ (понимаемую как кратность корня в уравнении $P(x)Q(a) - Q(x)P(a) = 0$): степень многочлена $p(x)$ зачастую понимается как кратность того, сколько раз он переводит бесконечность в себя, что становится понятнее, если заменить координату на $\frac{1}{x}$, т.е. рассмотреть корни выражения $\frac{1}{p(\frac{1}{x})} - 0$.

Ритт: решения кое-каких задач

Решение задачи 1. Понятно, что для каждого $n \in \mathbb{N}$ такой многочлен не более чем единственный: два различных многочлена не могут совпадать на отрезке $[-1, 1]$ — области значений косинуса. Также понятно, что подходят многочлены $T_1(x) = x$, $T_2(x) = 2x^2 - 1$, тогда далее рекуррентно определим последовательность $T_1, T_2, T_3, \ldots$ условием $T_{n+2}(x) = 2xT_{n+1}(x) - T_n(x)$, и по индукции докажем, что это в точности последовательность нужных многочленов.

База верна по построению, а переход следует из формулы

$$\cos\alpha\cos\beta = \frac{1}{2}(\cos(\alpha+\beta) + \cos(\alpha-\beta)),$$

имеем:

$$T_{n+2}(\cos t) = 2\cos t\cos((n+1)t) - \cos(nt) = \cos((n+2)t) + \cos(nt) - \cos(nt) = \cos((n+2)t).$$

Замечание. Согласно формуле Муавра, этот многочлен может быть найден по формуле

$$T_n(x) = \frac{(\frac{x+\sqrt{x^2-1}}{2})^n + (\frac{x-\sqrt{x^2-1}}{2})^n}{2}.$$

□

Решение задачи 2. Действуем аналогично предыдущей задаче: такой многочлен не более чем единственный: два различных многочлена не могут совпадать на множестве $(-\infty, -2] \cup [2, +\infty)$ — области значений функции $f(t) = t + \frac{1}{t}$. Затем определяем $D_1(x) = x, D_2(x) = x^2 - 2$, и далее рекуррентно: $D_{n+2}(x) = xD_{n+1}(x) - D_n(x)$. По индукции доказываем что $D_n(t + \frac{1}{t}) = t^n + \frac{1}{t^n}$: при $n \in \{1, 2\}$ это ясно, а шаг индукции следует из выкладки:

$$D_{n+2}(t+\frac{1}{t}) = (t+\frac{1}{t})(t^{n+1} + \frac{1}{t^{n+1}}) - (t^n + \frac{1}{t^n}) = t^{n+2} + \frac{1}{t^n} + t^n + \frac{1}{t^{n+2}} - t^n - \frac{1}{t^n} = t^{n+2} + \frac{1}{t^{n+2}}.$$

Замечание. По формуле Муавра, этот многочлен связан с многочленом Чебышёва соотношением $D_n(x) = 2T_n(x/2)$. □

Решение задачи 3. Наблюдение. Многочлен простой степени неразложим.

Доказательство наблюдения. Степень разложимого многочлена равна произведению степеней компонент нетривиального разложения, эти степени больше единицы. □

Пусть $m = p_1 \cdot \ldots \cdot p_d$ — разложение числа m на простые множители (среди множителей могут быть равные).

Пусть n, k — произвольные натуральные числа. Для всякого ненулевого $t \in \mathbb{R}$ имеем: $D_n(D_k(t + \frac{1}{t})) = D_n(t^k + \frac{1}{t^k}) = (t^k)^n + \frac{1}{(t^k)^n} = t^{nk} + \frac{1}{t^{nk}} = D_{nk}(t + \frac{1}{t})$, значит многочлены D_{nk} и $D_n \circ D_k$ совпадают на $(-\infty, -2] \cup [2, +\infty)$ (области значений функции $f(t) = t + \frac{1}{t}$), значит они совпадают. Тогда имеем декомпозицию $D_m = D_{p_1} \circ \ldots \circ D_{p_d}$. В силу наблюдения, далее достаточно понять что степень каждой компоненты — простое число. Для этого достаточно понять, что для любого натурального n степень многочлена D_n равна n. А это тривиально по индукции: при $n \in \{1, 2\}$ это верно, а переход тривиален из соотношения $D_{n+2}(x) = xD_{n+1}(x) - D_n(x)$. Полностью аналогично доказывается что $T_m = T_{p_1} \circ \ldots \circ T_{p_d}$ — искомпая декомпозиция T_m. □

Решение Задачи 4. 4а) Хорошо известно, что $\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2}b + \ldots + b^{n-1}$. Отсюда немедленно следует, что многочлен $F(a) - F(b)$ делится на многочлен $a - b$. Подставляя вместо a и b многочлены $H(x), H(y)$, получаем искомое утверждение.

4в) По формуле производной сложной функции имеем $F'(x) = H'(x)G'(H(x))$. □

Решение Задачи 5. Пусть многочлен $F(x)$ представим в виде композиции $G \circ H$ в соответствии с условием задачи. Достаточно доказать конечность числа таких разложений для фиксированного набора степеней $d_g = \deg G, d_h = \deg H (\deg G \cdot \deg H = \deg F)$. Многочлен H приведён, что откуда следует, что старший коэффициент многочлена H' равен d_H. У многочлена F' есть только конечное число множителей со старшим коэффициентом d_H. Откуда искомое утверждение и следует. □

Решение Задачи 6. Понятно, что степень такого многочлена $C(x)$ должна быть равна n.

Сначала докажем единственность: пусть таких многочленов $C_1(x), C_2(x)$ хотя бы два (оба приведённые степени n). Тогда $\deg(C_1^r - C_2^r) < n(r-1)$. С другой стороны,

$$(C_1^r - C_2^r) = (C_1 - C_2)(C_1^{r-1} + \ldots + C_2^{r-1}).$$

Ведущий коэффициент у каждого из слагаемых второго сомножителя равен $x^{n(r-1)}$, откуда ведущий коэффициент второго сомножителя равен $rx^{n(r-1)}$. Если первый сомножитель не 0, то степень всего выражения $C_1^r - C_2^r$ будет хотя бы $n(r-1)$. Противоречие.

Теперь докажем существование такого многочлена $C(x)$. Рассмотрим приведённый многочлен $C(x)$, для которого выражение $\deg(A - C^r)$ минимально (если таких несколько — возьмём любой). Положим $d := nr - \deg(A - C^r)$. Если $d \geq r$, то многочлен $C(x)$ и есть искомый. Таким образом мы можем считать, что $d \leq r - 1$. $\deg(A - (x^n)^r) < nr$, и, следовательно, $d \geq 1$. Пусть ведущий коэффициент $A - C^r$ равен kx^{nr-d}. Рассмотрим выражение $(A - (C + \frac{k}{n}x^{n-d}))$. Легко видеть, что

$$\deg(A - (C + \frac{k}{r}x^{n-d})) < nr - d.$$

Что противоречит нашему предположению о минимальности для многочлена $C(x)$. □

Решение Задачи 7. 7а) Тождество для остатка и неполного частного остается верным, а условие $\deg R(F(x)) < \deg H(F(x))$ очевидно.

7б) Поделив A и B на их старшие коэффициенты, считаем их далее приведенными. Возьмём многочлен $D = S(A) = T(B)$ наименьшей степени, являющийся одновременно многочленом от A и многочленом от B (S и T выбираем приведенными). Пусть

$$\deg A = ag, \deg B = bg, g = HOD(\deg A, \deg B), \deg D = dabg.$$

Тогда $\deg S = bd$, $\deg T = ad$. По задаче 6(а), существует приведеный многочлен U степени b, такой что $\deg(S(A) - U^d(A)) < b(d-1)a$, а также существует приведенный многочлен V степени a, такой что $\deg(T(B) - V^d(B)) < a(d-1)b$. Тогда

$$\deg(U^d(A) - V^d(B)) = \deg(U^d(A) - T(B) + T(B) - V^d(B)) = \deg(U^d(A) - S(A) + T(B) - V^d(B)) \leqslant$$

$$\leqslant \max(\deg(U^d(A) - S(A)), \deg(T(B) - V^d(B))) < a(d-1)b.$$

При этом

$$U^d(A) - V^d(B) = (U(A) - V(B))(U^{d-1}(A) + \ldots + V^{d-1}(B)).$$

Степени каждого слагаемого в сумме $U^{d-1}(A) + \ldots + V^{d-1}(B)$ одинаковы и равны $(d-1)ab$, а старший член везде равен 1. Значит, степень второго множителя в $(U(A) - V(B))(U^{d-1}(A) + \ldots + V^{d-1}(B))$ равна $ab(d-1)$. При этом само произведение имеет степень, меньшую $ab(d-1)$, согласно написанному ранее. Значит, $U(A) - V(B) = 0$. Тогда, если $d > 1$, то $U(A) = V(B)$ — многочлен меньшей степени, чем D, являющийся одновременно многочленом от A и многочленом от B. Противоречие. Из того, что $\deg F$ делится на $\deg D$ и задачи 6(б) тогда следует, что F является многочленом от этого D. □

Решение задачи 8. 8а) Прямое следствие из задачи 6(б).

8б) Многочлен $C - D$ равен нулю на области значений многочлена F, значит, по теореме Безу, он равен нулю. □

Решение задачи 10. Заметим, что, согласно задаче 7б, многочлены $F_i = f_i \circ f_{i+1} \circ \ldots \circ f_n$ и $G_i = g_i \circ g_{i+1} \circ \ldots \circ g_n$ являются многочленами друг от друга, а значит связаны друг с другом линейным соотношением $F_i = a_i G_i + b_i$. Это линейное соотношение и будет $l_i(y) = a_i y + b_i$ из определения сопряжения. $\square$

Решение задачи 10 без использования задачи 7б.

Лемма 1. Пусть P — многочлен степени $n \geq 1$, и a, b —вещественные числа, $a \neq 0$. Тогда:

(1) Если n — нечётное, то существует многочлен l первой степени такой, что $P \circ l$ имеет старший коэффициент a и следующий за ним коэффициент b.

(2) Если n — чётное, и число a имеет тот же знак что и старший коэффициент многочлена P то существуют многочлены l_+, l_- первой степени такие, что $P \circ l_+$ и $P \circ l_-$ имеют старший коэффициент a и следующий за ним коэффициент b, и у l_+ старший коэффициент положителен а у l_- отрицателен.

Proof. Пусть A — старший коэффициент P, B — коэффициент следующий за ним.

(1) Достаточно взять $l(x) = \sqrt[n]{\frac{a}{A}}x + (n(\sqrt[n]{\frac{a}{A}})^{n-1}A)^{-1} \cdot (b - B(\sqrt[n]{\frac{a}{A}})^{n-1})$.

(2) Достаточно взять $l_+(x) = \sqrt[n]{\frac{a}{A}}x + (n(\sqrt[n]{\frac{a}{A}})^{n-1}A)^{-1} \cdot (b - B(\sqrt[n]{\frac{a}{A}})^{n-1})$,
$l_-(x) = -\sqrt[n]{\frac{a}{A}}x - (n(\sqrt[n]{\frac{a}{A}})^{n-1}A)^{-1} \cdot (b + B(\sqrt[n]{\frac{a}{A}})^{n-1})$. $\square$

Лемма 2. Пусть A, B, P, Q — непостоянные многочлены, $A(P) = B(Q)$, $deg\, A = deg\, B$ и у A и B совпадают первые два коэффициента. Тогда если выполнено хотя-бы одно из двух условий

(1) $deg\, A$ — нечётна.

(2) у P и Q совпадают знаки старших коэффициентов.

То $A = B, P = Q$.

Proof. Пусть $m = deg\, A$. Понятно, что P и Q имеют одинаковую степень (ибо $A(P) = B(Q)$, и у A и B одинаковые ненулевые степени), обозначим её n. Пусть $P(x) = \sum\limits_{k=0}^{n} p_k x^k$, $Q(x) = \sum\limits_{k=0}^{n} q_k x^k$, $A(x) = \sum\limits_{k=0}^{m} a_k x^k$, $B(x) = \sum\limits_{k=0}^{m} b_k x^k$, и a, b — первые два коэффициента A (они же первые два коэффициента B.) Докажем индукцией по $d \in \{1, \ldots, n+1\}$ что первые d коэффициентов многочленов P и Q совпадают.

у $A(P)$ старший коэффициент равен $a(p_n)^m$, а у $B(Q)$ он равен $a(q_n)^m$, т.е. $(p_n)^m = (q_n)^m$, легко видеть что каждое из условий (1) и (2) вместе с этим равенством влечёт $p_n = q_n$, т.е.база $r = 1$ верна. Далее осуществим переход от $d = r \in \{1, \ldots, n\}$ к $d = r + 1$.

Возможны ровно 2 случая, сперва рассмотрим их отдельно:

1) $r = n$. Если в сумме $A(P) = \sum\limits_{k=0}^{m} a_k P^k$ более двух слагаемых, то каждое кроме последних двух — многочлен степени не выше $n(m-2) < nm - n$, поэтому коэффициент при $mn - n-$ой степени у $A(P)$ такой же, как у $a_m P^m + a_{m-1} P^{m-1}$. В случае, когда слагаемых всего два это, разумеется, также верно. Аналогично получаем что у $B(Q)$ коэффициент при $mn - n-$ой степени такой же, как у $b_m Q^m + b_{m-1} Q^{m-1}$, т.е. учитывая $a = a_m = b_m$, $b = a_{m-1} = b_{m-1}$ получаем что у многочленов $aP^m + bP^{m-1}$ и $aQ^m + b^Q m - 1$ одинаковые коэффициенты при $mn - n-$ой степени. Тривиально, что коэффциенты при этой степени у bP^{m-1} и bQ^{m-1} равны $b \cdot (p_n)^{m-1}$ и $b \cdot (q_n)^{m-1}$ соответственно, т.е. совпадают в силу базы индукции. Значит совпадают коэффициенты при этой степени у многочленов aP^m и aQ^m. Эта степень есть $mn - r$.

2) $r < n$: Понятно, что $\sum\limits_{k=0}^{m-1} a_k P^k$ и $\sum\limits_{k=0}^{m-1} b_k P^k$ — многочлены степени не выше $(m-1)n$, а $r + 1-$ый коэффициент многочлена $A(P) = B(Q)$ это коэффициент при степени $mn - r >$ $> mn - n = (m-1)n$, значит он совпадает с коэффициентом при степени $mn - r$ у многочленов

$A(P)-\sum\limits_{k=0}^{m-1}a_kP^k$ и $B(P)-\sum\limits_{k=0}^{m-1}b_kP^k$, т.е. с этим коэффициентом у многочленов aP^m и aQ^m. Значит и в этом случае получаем что у aP^m и aQ^m совпадают коэффициенты при $mn-r-$ой степени.

Итак, в любом случае у aP^m и aQ^m совпадают коэффициенты при $mn-r-$ой степени. Из этого равенства коэффициентов имеем равенство

$$a\cdot\sum\prod_{j=1}^{m}p_{s_j}=a\cdot\sum\prod_{j=1}^{m}q_{s_j},\ (*)$$

где суммирование ведётся по всем упорядоченным наборам $(s_1,\ldots,s_m)$ целых неотрицательных чисел не превосходящих n, таким, что $s_1+\ldots+s_m=mn-r$. Заметим, что в силу предположения индукции слагаемые в левой и правой частях $(*)$ отвечающие одному и тому же набору состоящему из чисел не меньших $n+1-r$ равны друг другу, тогда равны суммы слагаемых в $(*)$ отвечающих всем *остальным* наборам. Если одно из чисел набора не больше чем $n-r$ то сумма остальных равна $mn-n=n(m-1)$, и каждое из этих $m-1$ остальных не больше чем n, значит каждое из этих $m-1$ остальных равно n а последнее равно $n-r$. Значит все *остальные* наборы — в точности наборы в которых одно из чисел равно $n-r$ а остальные равны n, и таких ровно m штук. Значит равенство соответствующих сумм переписывается в виде $mp_m^{n-1}p_{n-r}=mq_m^{n-1}q_{n-r}$, что в силу базы индукции влечёт $p_{n-r}=q_{n-r}$, и переход доказан.

Таким образом все коэффициенты у P и Q совпадают, значит $P=Q$, и имеем
$A(Q)=A(P)=B(Q)$, и Q не константа, значит в силу задачи **4б** имеем $A=B$.

□

Доказываем утверждение индукцией по $r\in\mathbb{N}$. База при $r=1$ тривиальна, осуществим переход от $r=k$ к $r=k+1$, возможны ровно два случая которые рассмотрим отдельно.

1) Если $deg\,g_1$ — нечётна, то пусть l_2 — многочлен первой степени такой, что у $g_1\circ l_2$ первые два коэффициента соответственно совпадают с первыми двумя коэффициентами f_1, согласно **Лемме 1** такой l_2 существует. Тогда имеем $(g_1\circ l_2)\circ(l_2^{-1}\circ g_2\circ\ldots\circ g_{k+1})=f_1\circ(f_2\circ\ldots\circ f_{k+1})$. Тогда согласно **Лемме 2** $g_1\circ l_2=f_1$, и $(l_2^{-1}\circ g_2)\circ\ldots\circ g_{k+1}=f_2\circ\ldots\circ f_{k+1}$, и применяя к последнему равенству предположение индукции получаем требумое.

2) Если $deg\,g_1$ — чётна, то знак старшего коэффициента у композиции $g_1\circ(g_2\circ\ldots\circ g_{k+1})$ совпадает со знаком старшего коэффициента у g_1, аналогично знак старшего коэффициента у f_1 совпадает со знаком старшего коэффициента у $f_1\circ(f_2\circ\ldots\circ f_{k+1})$, т.е. знаки старших коэффициентов у f_1 и g_1 совпадают. Пусть тогда l_+ и l_- — многочлены первой степени с положительным и отрицательным старшим коэффициентом соответственно такие, что у многочленов $g_1(l_+)$ и $g_1(l_-)$ первые два коэффициента совпадают с первыми двумя коэффициентами у многочлена f_1, — такие l_+ и l_- существуют в силу **Леммы 1.** Рассмотрим композиции $K_+=l_+^{-1}\circ g_2\ldots\circ g_{k+1}$ и $K_-=l_-^{-1}\circ g_2\ldots\circ g_{k+1}$ — у них знаки старших коэффициентов противоположны, поэтому у одной из них знак старшего коэффициента такой же, как у старшего коэффициента композиции $f_2\circ\ldots\circ f_{k+1}$, тогда если знак такой же у K_+ то возьмём $l_2=l_+$, иначе $l_2=l_-$. Вновь имеем $(g_1\circ l_2)\circ(l_2^{-1}\circ g_2\circ\ldots\circ g_{k+1})=f_1\circ(f_2\circ\ldots\circ f_{k+1})$, и у этих композиций выполняются условия **Леммы 2.**, поэтому вновь имеем $g_1\circ l_2=f_1$, и $(l_2^{-1}\circ g_2)\circ\ldots\circ g_{k+1}=f_2\circ\ldots\circ f_{k+1}$, и применяя к последнему равенству предположение индукции получаем требумое. □

Ритт: решения ещё кое-каких задач

Решение задачи 12. Пусть $(x-a_1)(x-a_2)\dots(x-a_{mn}) = F(x) = G(H(x))$, $\deg G = m$, $\deg H = n$. Тогда у $G(x)$ должно быть ровно m корней. Пусть эти корни — $b_1, b_2, \dots, b_m$. Тогда

$$F(x) = (H(x)-b_1)(H(x)-b_2)\dots(H(x)-b_m).$$

Тогда часть корней $F(x)$ — корни многочлена $H(x)-b_1$, другая часть — корни $H(x)-b_2, \dots$, — и так мы переберем все корни $F(x)$. Упорядочим корни $F(x)$ так, чтобы первые n были корнями $H(x)-b_1$, вторые n штук - корнями $H(x)-b_2, \dots$ Докажем, что это даёт искомое разбиение. В самом деле, $\sum_{i=0}^n h_i x^i - b_j = H(x) - b_j = (x-c_{j1})\dots(x-c_{jn}) = \sum_{i=0}^n e_i(c_j)x^i$. □

Первое решение задачи 13. Пусть это получилось. Разобьём корни на m групп по n элементов в каждой по принципу из условия предыдущей задачи.

Выделим все корни, кратные простому числу p. Покажем, что все такие корни распределены поровну между некоторыми группами разбиения корней (в остальные группы при этом они не попадут вообще). Пусть в каких-то двух группах A_1 и A_2 содержится $0 < k_1 < k_2$ корней, кратных p, соответственно. Тогда многочлен $e_{n-k_1}(x_1, \dots, x_n)$ является суммой всевозможных произведений $n-k_1$ переменных среди $x_1, \dots, x_n$ без повторений множителей. Тогда для группы A_1 значение e_{n-k_1} не будет кратно p (т.к. ровно одно слагаемое не делится на p). Однако для группы A_2 значение $en-k_1$ делится на p. Это противоречит выводу предыдущей задачи о том, что для $i \neq 0$ значения e_i от корней из различных групп равны.

Положим теперь p = 23. Корней, делящихся на 23, ровно $[\frac{999}{23}] = 43$. Согласно рассуждению выше, все корни должны разбиваться на несколько равных групп, а значит либо все эти корни должны содержаться в одной группе, либо в каждой группе должен быть ровно один такой корень. Оба случая невозможны, поскольку в каждой группе содержится либо 27, либо 37 элементов и всего групп либо 37, либо 27. □

Второе решение задачи 13. Пусть это получилось и $(x-1)(x-2)\dots(x-999) = F(G(x))$. Стандартной техникой делаем $F(x)$ и $G(x)$ приведенными.

Обозначим корни производной $G(x)$ за $a_1, a_2, \dots, a_n$. Их на одну меньше, чем $\deg G$, т.к. у производной $F(G(x))$ по теореме Ролля 998 корней, степень $(F(G(x)))' = G'(x)F'(G(x))$ равна $\deg G - 1 + (\deg F - 1)\deg G$ и, таким образом, у G' и $F'(G)$ максимально возможное число корней. Таким образом, $n+1 = \deg G$ — нечетное число. Также обозначим $a_0 = -\infty$, $a_{n+1} = +\infty$. Обозначим корни $F'(x)$ как $b_1 < \dots < b_m$. Заметим, что в силу того, что у декомпозируемого многочлена ровно 999 корней, то $(m+1)(n+1) = 999$. Тогда корни $F'(G(x))$ разбиваются на m групп по $n+1$ штук (по тому признаку, чему равно $G(x)$ в этом корне). Обозначим эти группы

$$c_{1,1} < \dots < c_{1,n+1};$$

$$c_{2,1} < \dots < c_{2,n+1};$$

$$\dots$$

$$c_{m,1} < \dots < c_{m,n+1},$$

причем $G(c_{i,j}) = b_i$.

Тогда по теореме Ролля между $c_{i,j}$ и $c_{i,j+1}$ есть корень $G'(x)$ и он должен быть равен a_j. Значит, некоторые названные числа упорядочены так: $c_{i,1} < a_1 < c_{i,2} < a_2 < \dots < a_n < c_{i,n+1}$. На промежутке $(a_j; a_{j+1})$ функция $G(x)$ монотонна, причем на промежутках $(a_0; a_1)$ и $(a_n; a_{n+1})$ она возрастает, а на промежутках между ними она чередуется в свойстве возрастания/убывания.

Обозначим теперь корни $F(x)$ за $d_1 < d_2 < \ldots < d_{m+1}$. Тогда $d_1 < b_1 < d_2 < b_2 < \ldots < b_m < d_{m+1}$ и множество $\{1, 2, \ldots, 999\}$ разбивается на $m+1$ множество корней уравнений $G(x) = d_i$ по $n+1$ штуке в каждом. Обозначим эти множества как

$$h_{1,1} < h_{1,2} < \ldots < h_{1,n+1};$$

$$h_{2,1} < h_{2,2} < \ldots < h_{2,n+1};$$

$$\ldots$$

$$h_{m+1,1} < h_{m+1,2} < \ldots < h_{m+1,n+1},$$

причём $G(h_{i,j}) = d_i$. Тогда по теореме Ролля $h_{i,1} < a_1 < h_{i,2} < a_2 < \ldots < a_n < h_{i,n+1}$.

Получается, что до $m+1 < a_1 < m+2$, $2m+2 < a_2 < 2m+3$, $\ldots$, $n(m+1) < a_n < n(m+1)+1$, а кроме того

$$G(1) = d_1 < G(2) = d_2 < \ldots < G(m) = d_m < G(m+1) = d_{m+1} =$$

$$= d_{m+1} = G(m+2) > G(m+3) = d_m > \ldots > G(2m+1) = d_2 > G(2m+2) = d_1 =$$

$$= d_1 = G(2m+3) < d_2 = G(2m+4) < \ldots < G(3m+2) = d_m < G(3m+3) = d_{m+1} =$$

$$= d_{m+1} = G(3m+4) > \ldots$$

$$\ldots > G(n(m+1)) = d_1 =$$

$$= d_1 = G(n(m+1)+1) < d_2 = G(n(m+1)+2) < \ldots < d_m = G(998) < d_{m+1} = G(999).$$

Тогда по предыдущей задаче $e_1(1, 2m+2, 2m+3, 4m+4, \ldots, n(m+1), n(m+1)+1) = e_1(2, 2m+1, 2m+4, 4m+3, \ldots, n(m+1)-1, n(m+1)+2)$, что невозможно, поскольку они разной четности. $\square$

Третье решение задачи 13. Предположим, это так. Т.е. $(x-1)(x-2)\ldots(x-999) = F(G(x))$, где F, G — многочлены, $deg\, F = m$, $deg\, G = n$, и $\{m, n\} = \{27, 37\}$. Согласно предыдущей задаче числа $1, 2, \ldots, 999$ разбиваются на m групп по n штук так, что каждый элементарный симметрический многочлен (от n переменных) степени меньше n принимает одно и то же значение во всех точках вида $(t_1, \ldots, t_n)$ где $t_1, \ldots, t_n$ — в точности все числа из одной группы. Многочлен $S_{22}(x_1, \ldots, x_n) = x_1^{22} + x_2^{22} + \ldots + x_n^{22}$ выражается через элементарные симметрические многочлены (от n переменных) степени не больше $22 < n$. Значит он также принимает одно и тоже значение во всех точках вида $(t_1, \ldots, t_n)$ где $t_1, \ldots, t_n$ — числа из одной группы. $22-$ая степень всякого натурального числа не кратного 23 сравнима с 1 по модулю 23, а числа кратного 23 — с 0 по модулю 23. Пусть $(a_1, \ldots, a_n)$ — произвольная группа, тогда в силу выше написанного $a_1^{23} + a_2^{23} + \ldots + a_n^{23}$ сравнимо по модулю 23 с количеством чисел не кратных 23 в этой группе, т.е. сравнимо с числом равным "n минус "количество чисел в этой группе кратных 23." " Таким образом в каждой группе одинаковое по модулю 23 количество чисел кратных 23. Всего среди натуральных чисел от 1 до 999 ровно 43 кратных 23. Если бы в какой-то группе было 0 чисел кратных 23, то по доказанному выше в каждой группе кол-во чисел кратных 23 было бы кратно 23, но тогда бы и в объединении всех групп было бы кратное 23 кол-во чисел кратных 23, но там их 43, а 43 не кратно 23. По принципу Дирихле в какой-то группе не более чем одно число кратное 23 т.к. $2m > 43$, значит, в силу показанного выше — в какой-то группе ровно одно число кратное 23. Тогда в каждой группе кол-во чисел кратных 23 сравнимо с 1 по модулю 23, тогда кол-во чисел кратных 23 в объединении всех групп сравнимо с m по модулю 23, т.е. имеем $m \equiv 43\, (mod\, 23)$. Но это не так ибо $m \in \{27, 37\}$ — противоречие завершающее решение задачи.

$\square$

Решение задачи 14. Сложение: $\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i + b_i) x^i$.

Умножение: $(\sum_i a_i x^i) \cdot (\sum_j b_j x^j) = \sum_l x^l \sum_{i+j=l} a_i b_j$.

Противоположный: $-\sum_i a_i x^i = \sum_i (-a_i x^i)$.

Перестановочные законы:

$$A(x)+B(x) = \sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i+b_i)x^i = \sum_i (b_i+a_i)x^i = \sum_i b_i x^i + \sum_i a_i x^i = B(x)+A(x),$$

$$A(x)\cdot B(x) = (\sum_i a_i x^i)\cdot(\sum_j b_j x^j) = \sum_l x^l \sum_{i+j=l} a_i b_j = \sum_l x^l \sum_{j+i=l} b_j a_i = (\sum_j b_j x^j)\cdot(\sum_i a_i x^i) = B(x)\cdot A(x).$$

Проверка определения: Сочетательные законы:

$$(A(x)+B(x))+C(x) = \sum_i ((a_i+b_i)+c_i)x^i = \sum_i (a_i+(b_i+c_i))x^i = A(x)+(B(x)+C(x)),$$

$$(A(x)\cdot B(x))\cdot C(x) = \sum_l x^l \sum_{i+j+k=l} a_i b_j c_k = A(x)\cdot(B(x)\cdot C(x)).$$

Распределительный закон:

$$A(x)\cdot(B(x)+C(x)) = \sum_l x^l \sum_{i+j=l} a_i(b_j+c_j) = \sum_l x^l (\sum_{i+j=l} a_i b_j + \sum_{i+j=l} a_i c_j) = A(x)\cdot B(x) + A(x)\cdot C(x).$$

Свойства нуля:

$$A(x)+(-A(x)) = \sum_i (a_i - a_i)x^i = 0,$$

$$0\cdot A(x) = \sum_l x^l \sum_{i+j=l} 0 a_i = 0.$$

Свойство единицы:

$$1\cdot A(x) = \sum_l x^l (1 a_l + \sum_{i+j=l, i>0} 0 a_j) = \sum_l a_l x^l = A(x).$$

Таким образом, все равенства (1-8) выполняются для любых многочленов. □

Решение задачи 15. 15а) В самом деле, операции сложения, умножения и вычитания не выводят из множества M: их результаты дают просто сумму, прозведение и разность соответствующих выражений, которые тоже являются выражениями от указанных многочленов, а следовательно, по определению, лежат в M.

15б) Заметим, что $\deg(F\cdot G) = \deg F + \deg G$, а $\deg F^n = n \deg F$. Это доказывает требуемое.

15в) Пусть m — наименьший элемент в N. Тогда все кратные ему тоже принадлежат N. Пусть $r_1, r_2, \ldots, r_s$ — все возможные остатки от деления элементов N на m. Обозначим за k_i наименьший элемент в N, дающий остаток r_i при делении на m. Тогда все числа вида $k_i + lm$, где l — целое неотрицательное, тоже принадлежат N, согласно задаче 15(б). Числа таких видов исчерпывают всё N. Таким образом, N порождено элементами $m, k_1, k_2, \ldots k_s$, коих конечное число.

15г) Пусть $d_1, \ldots, d_r$ — набор порождающих для N. Пусть $g_1(x), \ldots, g_r(x)$ — приведенные многочлены этих степеней. Докажем, что M порождено ими. В самом деле, пусть $f(x)$ — многочлен наименьшей степени в M, не выразимый через $g_1, \ldots, g_r$. Поделив его на старший коэффициент, сделаем его приведенным. Тогда $\deg f = n_1 d_1 + \ldots + n_r d_r$. Тогда $\deg(f - g_1^{n_1} g_2^{n_2} \ldots g_r^{n_r}) < \deg f$ и $f - g_1^{n_1} g_2^{n_2} \ldots g_r^{n_r}$ принадлежит M, невыразим через g_i и имеет меньшую степень, чем f. Противоречие.

15д) Достаточно взять конечные наборы f_i, через которые выражается g_j. Объединение этих наборов дает требуемый список f_s. □

Решение задачи 16. Определим операции так : $\frac{P_1}{Q_1}+\frac{P_2}{Q_2}:=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}$, $\frac{P_1}{Q_1}\cdot\frac{P_2}{Q_2}:=\frac{P_1P_2}{Q_1Q_2}$, $-\frac{P_1}{Q_1}:=\frac{-P_1}{Q_1}$, и $(\frac{P_1}{Q_1})^{-1}:=\frac{Q_1}{P_1}$, при $P_1\neq 0$.

Проверим корректность задания операций (независимость от выбора конкретной реализации рациональной функции в виде отношения многочленов). Пусть $P_1,Q_1,P_2,Q_2,\widetilde{P_1},\widetilde{Q_1},\widetilde{P_2},\widetilde{Q_2}$ такие многочлены, что $\frac{P_1}{Q_1}=\frac{\widetilde{P_1}}{\widetilde{Q_1}}$ и $\frac{P_2}{Q_2}=\frac{\widetilde{P_2}}{\widetilde{Q_2}}$, т.е. $P_1\widetilde{Q_1}=\widetilde{P_1}Q_1$ и $P_2\widetilde{Q_2}=\widetilde{P_2}Q_2$. Имеем:
для суммы: $\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}=\frac{P_1Q_2\widetilde{Q_1}\widetilde{Q_2}+P_2Q_1\widetilde{Q_1}\widetilde{Q_2}}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}Q_1Q_2\widetilde{Q_2}+\widetilde{P_2}Q_1\widetilde{Q_1}Q_2}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{Q_2}+\widetilde{P_2}\widetilde{Q_1}}{\widetilde{Q_1}\widetilde{Q_2}}$.
Для произведения: $\frac{P_1P_2}{Q_1Q_2}=\frac{P_1P_2\widetilde{Q_1}\widetilde{Q_2}}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{P_2}Q_1Q_2}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{P_2}}{\widetilde{Q_1}\widetilde{Q_2}}$.
Для взятия противоположного: $\frac{-P_1}{Q_1}=\frac{-P_1\widetilde{Q_1}}{Q_1\widetilde{Q_1}}=\frac{-\widetilde{P_1}Q_1}{Q_1\widetilde{Q_1}}=\frac{-\widetilde{P_1}}{\widetilde{Q_1}}$.
Для взятия обратного: $\frac{Q_1}{P_1}=\frac{Q_1\widetilde{P_1}}{P_1\widetilde{P_1}}=\frac{\widetilde{Q_1}P_1}{P_1\widetilde{P_1}}=\frac{\widetilde{Q_1}}{\widetilde{P_1}}$.

Итак, операции заданы корректно, теперь проверим аксиомы поля: Пусть P_1,Q_1,P_2,Q_2,P_3,Q_3 — произвольные многочлены, такие, что Q_1,Q_2,Q_3 — ненулевые. Коммутативность сложения, то, что $\frac{0}{1}$ –нейтральный элемент по сложению, и то что у всякого элемента есть противоположный по сложению — тривиально. Проверим ассоциативность сложения:
$(\frac{P_1}{Q_1}+\frac{P_2}{Q_2})+\frac{P_3}{Q_3}=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}+\frac{P_3}{Q_3}=\frac{P_1Q_2Q_3+P_2Q_1Q_3+Q_1Q_2P_3}{Q_1Q_2Q_3}=\frac{P_1}{Q_1}+\frac{P_2Q_3+P_3Q_2}{Q_2Q_3}=\frac{P_1}{Q_1}+(\frac{P_2}{Q_2}+\frac{P_3}{Q_3})$. Далее, тривиальны также коммутативность умножения, ассоциативность умножения, то, что $\frac{1}{1}$ — нейтральный элемент по умножению, и то, что у каждого ненулевого элемента есть обратный по умножению. Тривиально и то что $\frac{1}{1}\neq\frac{0}{1}$. Проверяем дистрибутивность:
$(\frac{P_1}{Q_1}+\frac{P_2}{Q_2})\frac{P_3}{Q_3}=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}\cdot\frac{P_3}{Q_3}=\frac{P_1Q_2P_3+P_2Q_1P_3}{Q_1Q_2Q_3}=\frac{P_1Q_2P_3Q_1Q_2Q_3+P_2Q_1P_3Q_1Q_2Q_3}{Q_1Q_2Q_3Q_1Q_2Q_3}=\frac{P_1Q_2P_3}{Q_1Q_2Q_3}+\frac{P_2Q_1P_3}{Q_1Q_2Q_3}=$
$=\frac{P_1P_3}{Q_1Q_3}+\frac{P_2P_3}{Q_2Q_3}=\frac{P_1}{Q_1}\cdot\frac{P_3}{Q_3}+\frac{P_2}{Q_2}\cdot\frac{P_3}{Q_3}$. □

Решение задачи 17. В случае, когда $B=b$ — ненулевая константа — утверждение тривиально: $A=b\cdot(b^{-1}A)+0$. Поэтому далее можем и будем считать, что $B(x)=\sum\limits_{j=0}^{n}b_jx^j$, где $n\in\mathbb{N}$ — степень B. Доказываем нужное утверждение индукцией по степени A : для A со степенью меньшей n утверждение тривиально: подойдут $Q=0,R=A$. Остаётся доказать, что если утверждение верно для всех многочленов A со степенью не выше k, где $k\geq n-1$ то оно верно и для многочленов со степенью $k+1$. Сделаем это. Пусть $A=\sum\limits_{j=1}^{k+1}a_jx^j$ — произвольный многочлен степени $k+1$, тогда $A-a_{k+1}(b_n)^{-1}Bx^{k+1-n}$ — многочлен степени не выше k, и по предположению индукции для некоторых многочленов Q,R с $deg\,R<deg\,B$ выполнено
$A-a_{k+1}(b_n)^{-1}Bx^{k+1-n}=B(x)\cdot Q(x)+R(x)$, значит
$A(x)=B(x)\cdot(Q(x)+a_{k+1}(b_n)^{-1}x^{k+1-n})+R(x)$ — это то что нужно. □

Решение задачи 18. а) $(x+y+z)^3-x^3-y^3-z^3=3(x+y)(y+z)(x+z)+0$ проверить это можно раскрытием скобок. Но можно и иначе: тривиально, что в обеих частях равенства стоят многочлены 2−ой степени от x, поэтому достаточно (согласно аналогу теоремы Безу для полей) проверить совпадение их значений в трёх различных точках из $\mathbb{R}(y,z)$. Легко видеть что значения совпадают при $x\in\{-y,-z,0\}$.

б) $(x+y+z)^5-x^5-y^5-z^5=5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0$, проверить это можно раскрытием скобок. Но можно и иначе: тривиально, что в обеих частях равенства стоят многочлены 4−ой степени от x, поэтому (согласно аналогу теоремы Безу для полей) достаточно проверить совпадение их значений в пяти различных точках из $\mathbb{R}(y,z)$. При $x=-y$, и $x=-z$ совпадение тривиально. При $x=-y-z$ имеем: $(x+y+z)^5-x^5-y^5-z^5=(y+z)^5-y^5-z^5=5y^4z+10y^3z^2+10y^2z^3+5yz^4$, и
$5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0=5(-z)(-y)(y+z)((x+y+z)^2-xy-xz-zy)=$
$=5yz(y+z)(-zy+(z+y)^2)=5yz(y+z)(z^2+yz+y^2)=5yz(z^3+yz^2+y^2z+y^3+yz^2+y^2z)=$
$=5yz(z^3+2z^2y+2zy^2+y^3)=5z^4y+10z^3y^2+10z^2y^3+5zy^4$. При $x=-y-1$ имеем

$(x+y+z)^5-x^5-y^5-z^5=(z-1)^5-z^5+(y+1)^5-y^5=-5z^4+10z^3-10z^2+5z-1+5y^4+$
$+10y^3+10y^2+5y+1=5(y^4-z^4+2y^3+2z^3+2y^2-2z^2+y+z)$, и
$5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0=-5(z-y-1)(y+z)((x+y+z)^2-z(x+y)-xy)=$
$=5(y+1-z)(y+z)((z-1)^2+z+y^2+y)=5(y+z)(y+1-z)(z^2-z+1+y^2+y)=$
$=5(y^2+y-zy+zy+z-z^2)(z^2-z+1+y^2+y)=5(y^2-z^2+z+y)(z^2-z+1+y^2+y)=$
$5((y^2+y)-(z^2-z))((y^2+y)+(z^2-z)+1)=5((y^2+y)^2-(z^2-z)^2+(y^2+y)-(z^2-z))=$
$=5(y^4+2y^3+y^2-z^4+2z^3-z^2+y^2+y-z^2+z)=5(y^4-z^4+2y^3+2z^3+2y^2-2z^2+y+z)$. Аналогично значения совпадают при $x=-z-1$. □

Решение задачи 19. Считаем, что хотя бы один из многочленов ненулевой. Если один из многочленов нулевой — тривиально, что другой является $HOD-$ом и представляется в нужном виде, поэтому далее считаем, что среди A, B — нет нулевых многочленов. Далее доказываем оба утверждения (для ненулевых многочленов) вместе индукцией по $n=\min(\deg A, \deg B)$. При $n=0$ тривиально, что 1 является $HOD-$ом и представляется в нужном виде.

Шаг индукции: Пусть для $n=k\geq 0$ утверждения верны, докажем что они верны для $n=k+1$. Не умаляя общности $\deg A\geq \deg B$. Разделим A на B с остатком: $A=BD+R$. Если $R=0$ то тривиально, что B является $HOD-$ом A и B и представляется в нужном виде. Если же $R\neq 0$, то пара многочленов (B,R) удовлетворяет предположению индукции, пусть тогда $X=BV+RW=$ $=HOD(B,R)$, где V,W — многочлены. Т.к. $A=BD+R$ то нетрудно понять, что множество общих делителей многочленов A и B совпадает с множеством общих делителей многочленов B и R. Значит X является также и $HOD-$ом A и B. Наконец $X=BV+(A-BD)W=AW+B(V-DW)$, и шаг индукции доказан. □

Решение задачи 20. Пусть коэффициенты $R(x)=C(x)D(x)$ не взаимнопросты. Тогда есть $\lambda\in\mathbb{C}$ при подстановке которого вместо t в $R(x)$ получается 0; мы обозначим такую подстановку $R(x)\mid_{t=\lambda}$. Тогда $C(x)\mid_{t=\lambda}\cdot D(x)\mid_{t=\lambda}=0$. То есть или $C(x)\mid_{t=\lambda}=0$ или $D(x)\mid_{t=\lambda}=0$. Что и требовалось. □

Решение задачи 21. Это практически очевидное утверждение, но давайте проверим что оно-таки выполнено (то есть, что операции "$+$" и "$\cdot$" сохраняют заявленное подмножество многочленов вида $E(g(x))$).

$$+:\quad \frac{A(g(x))}{B(g(x))}+\frac{C(g(x))}{D(g(x))}=\frac{(A\cdot D+B\cdot C)(g(x))}{(B\cdot D)(g(x))},$$
$$\cdot:\quad \frac{A(g(x))}{B(g(x))}\cdot\frac{C(g(x))}{D(g(x))}=\frac{(A\cdot C)(g(x))}{(B\cdot D)(g(x))}.$$

□

Решение задачи 23. Пусть есть цепочка полей $\mathbb{R}\subset K\subset\mathbb{R}(x)$ и K содержит многочлен $g(x)\in\mathbb{R}[x]\backslash\mathbb{R}$. Проверим, что $K=\mathbb{R}(f(x))$ для некоторого многочлена $f(x)$. По теореме Люрота, $K=\mathbb{R}(\widetilde{f})$ для некоторой функции $\widetilde{f}\in\mathbb{R}(x)$; $f=\frac{f_+}{f_-}$, где $f_+,f_-\in\mathbb{R}[x]$ и $(f_+,f_-)=1$.

Заметим, что $\mathbb{R}(g(x))\subset K=\mathbb{R}(\widetilde{f})$, и, следовательно, существует

$$s\in\mathbb{R}(x)\colon s(\tilde{f})=g(x);$$

$s=\frac{s_+}{s_-}$, где $s_+,s_-\in\mathbb{R}[x]$ и $(s_+,s_-)=1$. Тогда $\frac{s_+(\frac{f_+}{f_-})}{s_-(\frac{f_+}{f_-})}=g(x)$. Обозначим через $\alpha_1,\ldots,\alpha_{n_+}$ корни многочлена s_+, а через $\beta_1,\ldots,\beta_{n_-}$ корни многочлена s_-, обозначим через C_+,C_- ведущие коэффициенты многочленов s_+ и s_- соответственно.

Без ограничения общности считаем, что $f_-\notin\mathbb{R}$. Используя все эти обозначения сразу имеем:

$$g(x)=\frac{C_+}{C_-}\frac{f_-^{n_--n_+}(f_+-\alpha_1f_-)(f_+-\alpha_2f_-)\ldots(f_+-\alpha_{n_+}f_-)}{(f_+-\beta_1f_-)(f_+-\beta_2f_-)\ldots(f_+-\beta_{n_-}f_-)}.$$

Заметим, что для $\alpha \neq \beta$ имеем $(f_1 - \alpha f_2, f_1 - \beta f_2) = 1$. Так же имеем, что $(f_2, f_1 - \gamma f_2)$ для всех $\gamma \in \mathbb{C}$. То есть все множители из формулы выше взаимнопросты, и, следовательно, никак не могут друг друга сокращать. Из того, что $g(x)$ всё же многочлен, следует, что (1) или (2):

(1) $n_- = 0$;

(2) $n_- > 0$ и $\deg(f_+ - \beta_i f_-) = 0$ для всех $i, 1 \leqslant i \leqslant n_-$.

В случае (1), если $n_+ = 0$, то $g(x) \in \mathbb{R}$ (что невозможно); а если $n_+ > 0$, то множитель $f_-^{n_- - n_+}$ создаёт нетривиальный знаменатель для $g(x)$ (то есть в этом случае $g(x)$ не многочлен, противоречие).

В случае (2) имеем $f_+ - \beta_1 f_- = C_0$ для некоторой ненулевой константы C_0. А из этого следует, что $K = \mathbb{R}(\tilde{f}) = \mathbb{R}(f_+)$ — что и требовалось. □

Решение задачи 24. Пусть $F \in \mathbb{R}[x]$ разложим, то есть

$$F(x) = G(H(x)) \text{ для } G, H \in \mathbb{R}[x] \text{ и } \deg G > 1, \deg H > 1.$$

Тогда для $L = \mathbb{R}(H(x))$ имеем: $\mathbb{R}(F) \subsetneq \mathbb{R}(H) \subsetneq \mathbb{R}(x)$. Это доказывает искомое утверждение в одну сторону.

Осталось проверить, что, если есть какое-то промежуточное поле $L, \mathbb{R}(F) \subsetneq L \subsetneq \mathbb{R}(x)$, то $F(x)$ разложим. Заметим, что поле L содержит многочлен F, и, следовательно $L = \mathbb{R}(H(x)), H \in \mathbb{R}[x]$, по задаче 23. Из теоремы Люрота следует, что существует $G \in \mathbb{R}(x)$, для которого $F(x) = G(H(x))$. По аналогии с предыдущей задачей представим $G(x)$ в виде отношения двух многочленов, рассмотрим корни каждого из этих многочленов и их старшие коэффициенты. Получим формулу:

$$F(x) = \frac{C_+}{C_-} \frac{(H(x) - \alpha_1)(H(x) - \alpha_2) \ldots (H(x) - \alpha_{n_+})}{(H(x) - \beta_1)(H(x) - \beta_2) \ldots (H(x) - \beta_{n_-})}.$$

Как и в предыдущей задаче, все соответствующие множители взаимнопросты, и, следовательно, $F(x)$ может быть многочленом только если все множители, находящиеся в знаменателе являются константами. А это возможно или если $H(x) \in \mathbb{R}$, или если $n_+ = 0$. Первый случай невозможен в силу выбора $H(x)$. Второй случай гарантирует, что $G(x) \in \mathbb{R}[x]$, то есть что $F(x)$ — разложим. □

Ритт: ещё кое-какие решения ещё кое-каких задач

Решение задачи 26. Мы сразу будем считать что K не совпадает с $\mathbb{R}$.

а) По построению x — корень всех наших выражений, поэтому они кратны $y-x$, в кольце $\mathbb{R}(x)[y]$ дальнейшее ясно в силу следствий Леммы Гаусса (или "деления в столбик")

б) Рассмотрим каноническое разложение HOD-а по степеням неприводимых многочленов, для каждого множителя выберем наше выражение в которое этот множитель входит в точности в такой степени как в HOD. Мы выбрали конечное кол-во выражений, и по построению их HOD совпадает с HOD-ом всех наших выражений. Для конечного кол-ва выражений HOD можно найти алгоритмом евклида, его итерации не выводят коэффициенты из поля K, поэтому отношение любых двух коэффициентов (если оно определено) лежит в поле K.

в) Следует из возможности разложения левой части на множители и несократимости $\frac{D(x,y)}{d(x)}$.

Далее мы будем выбирать постороенный HOD приведённым многочленом, тогда в реализации $\frac{D(x,y)}{d(x)}$ у $D(x,y) \in \mathbb{R}[x][y]$ старший коэффициент равен $d(x)$, и все коэффициенты $D(x,y)$ взаимно просты в совокупности как элементы $\mathbb{R}[x]$.

г) Прямо из определения степени рациональной фунции следует, что $P_f(y)Q_f(x) - P_f(x)Q_f(y)$ — многочлен степени m по каждой из переменных, и понятно что он кососимметрический. Тогда условия $\deg_x D(x,y) < m$ и $\deg_x C_f(x,y) > 0$ равносильны друг другу, и достаточно доказать второе. Предположим оно не выполнено. Т.е. $C_f(x,y)$ — многочлен от y. Из кососимметричности получаем что $D(x,y)C_f(x,y)$ делится на $C_f(y,x)$ — многочлен от x, т.е. $D(x,y)$ делится на $C_f(y,x)$, но его коэффициенты взаимнопросты в совокупности как элементы $\mathbb{R}[x]$, значит $C_f(y,x) = c$ — константа. Значит степень $P_f(y)Q_f(x) - P_f(x)Q_f(y)$ по любой переменной такая же как у $D(x,y)$ т.е. m — противоречие.

д) Из предыдущих пунктов уже знаем что коэффициенты лежат в K, посмотрим ещё раз на нашу реализацию дробью, про степень числителя нужное доказано, а для знаменателя это верно т.к. он есть старший коэффициент числителя рассмотренного как многочлено от y.

е) Предположим, что мы не придём к такой ситуации. Рассмотрим тогда любую итерацию, и реализуем выражение для HOD через $\frac{D(x,y)}{d(x)}$ с соглашениями указанными в предыдущих пунктах, и пусть f рациональная функция наименьшей степени m в множестве на этой итерации. По доказанному выше $P_f(y)Q_f(x) - P_f(x)Q_f(y) = C_f(y,x)D(x,y)$, и справа стоят многочлены. Понятно, что степень $D(x,y)$ по x не меньше m.

Первый случай: степень по y равна m, тогда $C_f = C$ — константа. По определению НОДа многочлен $P_f(y) - f(x)Q_f(y) = \frac{CD(x,y)}{Q_f(x)}$ делится на $\frac{D(x,y)}{d(x)}$. Тогда для некоторого (x) верно $\frac{D(x,y)}{Q_f(x)}c(x) = \frac{D(x,y)}{d(x)}$. Значит $f(x) \in M$ является тем самым которого нет по нашему предположению — в этом случае получили противоречие, т.е. он невозможен.

Значит на каждой итерации реализуется случай когда степень $D(x,y)$ по y меньше чем m, согласно пункту д) в этом случае все коэффициенты $\frac{D(x,y)}{d(x)}$ имеют степень меньше m, т.е. после выполнения итерации множество пополняются новой нетривиальной рациональной функцией имеющий меньшую степень чем все имеющиеся в множестве до этого. Но в K есть некая нетривиальная рациональная функция наименьшей степени, поэтому количество таких итераций не может быть бесконечным, а оно таково — противоречие.

ж) Многочлен $P_h(y) - h(x)Q_h(y)$ имеет первую степень по $h(x)$. Поэтому, если он разложим в $\mathbb{R}[h(x), y]$, то один из множителей в нетривиальном разложении — многочлена от y. Тогда P_h и Q_h имеют нетривиальный общий делитель — противоречие.

з) Докажем от противного. Пусть $P_g(y)$ делится на $P_h(y) - h(x)Q_h(y)$ в $\mathbb{R}(h(x))[y] \subset K[y]$, т.к. $g(x)Q_g(y)$ делится на $P_h(y) - h(x)Q_h(y)$ в $K[y]$ то значит $P_g(y)$ и $Q_g(y)$ имеют нетривиальный общий делитель в $K[y]$, однако мы знаем, что их HOD находится применением алгоритма Евклида, но в подкольце $\mathbb{R}(h(x))[y]$ алгоритм Евклида приводит к тривиальному $HOD-$у противоречие.

и) Пусть

$$P_u(y) = (P_h(y) - h(x)Q_h(y))v(h(x)) + \frac{T(h(x), y)}{t(h(y))}$$

и

$$Q_u(y) = (P_h(y) - h(x)Q_h(y))w(h(x)) + \frac{S(h(x), y)}{s(h(y))}.$$

Тогда

$$P_u(y) - u(x)Q_u(y) = (P_h(y) - h(x)Q_h(y))(v(h(x)) - u(x)w(h(x))) + \frac{T(h(x), y)}{t(h(y))} - u(x)\frac{S(h(x), y)}{s(h(y))}.$$

Разность $P_u(y) - u(x)Q_u(y)$ и разность $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))}$ при делении на $P_h(y) - h(x)Q_h(y)$ дают одинаковые остатки над K. При этом первый многочлен делится на $P_h(y) - h(x)Q_h(y)$, поэтому второй многочлен тоже делится на $P_h(y) - h(x)Q_h(y)$ над K. Степень $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))}$ по y меньше, чем степень $\deg_y(P_h(y) - h(x)Q_h(y))$, по построению. Поэтому $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))} = 0$.

к) Многочлены от y с обеих сторон равенства $\frac{T(h(x),y)}{t(h(y))} = u(x)\frac{S(h(x),y)}{s(h(y))}$ не равны тождественно 0 (по пункту з). Поэтому $u(x)$ лежит в $\mathbb{R}(h(x))$ как отношение.

л) h лежит в K, поэтому $\mathbb{R}(h(x)) \subset K$, обратное включение доказано в предыдущем пункте. □

Решение задачи 27. Пусть $\mathbb{R}(h) = \mathbb{R}(h_1)$ для некоторых $h, h_1 \in \mathbb{R}(x)$. Тогда существуют $f, g \in \mathbb{R}(x)$, для которых $f(h) = h_1, g(h_1) = h$. Достаточно доказать, что $\deg f \leq 1$. Представим f в виде несократимой дроби $f = \frac{f_+}{f_-}, (f_+, f_-) = 1$. Если f_- константа, то f — многочлен, а тогда по второй части решения задачи 24 получается, что g — тоже многочлен. Тогда

$$\deg h = \deg f(g(h)) = \deg f \deg g \deg h.$$

Откуда $\deg f = 1$. Аналогично рассматривается случай $g_- \in \mathbb{R}$.

Далее считаем, что $f_-, g_- \notin \mathbb{R}$. По аналогии с рассуждением из решения задачи 23, представим $f(x)$ в виде отношения двух многочленов, рассмотрим корни каждого из этих многочленов и их старшие коэффициенты. Получим формулу:

$$h_1 = f(g(h_1)) = \frac{C_+}{C_-}\frac{g_-^{n_- - n_+}(g_+ - \alpha_1 g_-)(g_+ - \alpha_2 g_-)\dots(g_+ - \alpha_{n_+} g_-)}{(g_+ - \beta_1 g_-)(g_+ - \beta_2 g_-)\dots(g_+ - \beta_{n_-} g_-)}.$$

Все множители числителя и знаменателя правой части этой формулы взаимнопросты.

Пусть $n_- = n_+$. Заметим, что постоянный множитель не может возникнуть и в числителе, и в знаменателе одновременно. Откуда $n_- = n_+ = 1$, и, следовательно, $\deg f = 1$.

Пусть $n_- \neq n_+$. Тогда $h \sim g_-^{n_- - n_+}$, и, в частности, $n_- - n_+ = 1$ и $n_- \geq 1$. Если $n_+ \neq 0$, то в формуле будет по крайней мере два непостоянных и взаимнопростых множителя. Противоречие. Следовательно, $n_- = 1, n_+ = 0, \deg f = 1$. □

Решение задачи 28. Пусть есть два поля $K = \mathbb{R}(f) \subset L = \mathbb{R}(g)$. Из условия $K \subset L$ следует, что есть $H \in \mathbb{R}(x)\colon f = H(g)$.

По задаче 27, все образующие поля K имеют вид $\frac{a_1 f + b_1}{c_1 f + d_1}, a_1 d_1 - b_1 c_1 \neq 0$, а все образующие поля L имеют вид $\frac{a_2 g + b_2}{c_2 g + d_2}, a_2 d_2 - b_2 c_2 \neq 0$. Отсюда следует, что функции перехода $\widetilde{H}$ (для других образующих) имеют вид

$$\frac{a_1 H(\frac{a_2 x + b_2}{c_2 x + d_2}) + b_1}{c_1 H(\frac{a_2 x + b_2}{c_2 x + d_2}) + d_1}.$$

Достаточно проверить, что
$$\deg H = \deg(\frac{aH+b}{cH+d}) = \deg(H(\frac{ax+b}{cx+d})), ad-bc \neq 0.$$
Равенство $\deg H = \deg(\frac{aH+b}{cH+d}), ad-bc\neq 0$, проверяется в задаче 25. То есть осталось проверить, что $\deg H = \deg(H(\frac{ax+b}{cx+d})), ad-bc\neq 0$.

Фиксируем $a,b,c,d\in\mathbb{R}$, для которых $ad-bc\neq 0$. По аналогии с рассуждением из решения задачи 23, представим $H(x)$ в виде отношения двух многочленов, рассмотрим корни каждого из этих многочленов и их старшие коэффициенты. Получим формулу:
$$H(\frac{ax+b}{cx+d}) = \frac{C_+}{C_-}\frac{(cx+d)^{n_- - n_+}((ax+b)-\alpha_1(cx+d))((ax+b)-\alpha_2(cx+d))\dots((ax+b)-\alpha_{n_+}(cx+d))}{((ax+b)-\beta_1(cx+d))((ax+b)-\beta_2(cx+d))\dots((ax+b)-\beta_{n_-}(cx+d))}.$$
Из этой формулы очевидно, что $\deg H(\frac{ax+b}{cx+d})\le \deg H$. Так как $H(x)=H(\frac{ay+b}{cy+d})$, где
$$y = \frac{\frac{d}{ad-bc}x + \frac{-c}{ad-bc}}{\frac{-b}{ad-bc}x+\frac{a}{ad-bc}},$$
то из неё же следует, что $\deg H \le \deg H(\frac{ax+b}{cx+d})$. Откуда имеем, что
$$\deg H(\frac{ax+b}{cx+d}) = \deg H.$$
□

Решение задачи 29. Решение этой задачи написано во второй части решения задачи 24. □

Решение задачи 30. Из условия и НОК-леммы следует, что есть многочлен H, для которого $\deg H = \text{НОК}(\deg F, \deg G)$ и $\mathbb{R}(H)\subset\mathbb{R}(F)\cap\mathbb{R}(G)$. Откуда имеем
$$([\mathbb{R}(F):\mathbb{R}(H)],[\mathbb{R}(G):\mathbb{R}(H)])=1.$$
Осталось заметить, что $[\mathbb{R}(F):\mathbb{R}(F)\cap\mathbb{R}(G)]$ делит $[\mathbb{R}(F):\mathbb{R}(H)]$, а $[\mathbb{R}(G):\mathbb{R}(F)\cap\mathbb{R}(G)]$ делит $[\mathbb{R}(G):\mathbb{R}(H)]$ так как $\mathbb{R}(H)\subset\mathbb{R}(F)\cap\mathbb{R}(G)$. □

Решение задачи 31. а) Предположим противное — пусть $\deg_z R(y,z)<\deg f(x)$. Заметим, что $n := \deg_y R(y,z)\ge 1$ (в ином случае $R(y,z)$ не зависит от y, откуда $R(-,z)=0$). Тогда $R(y,z)=R_0(z)+R_1(z)y+\ldots+R_n(z)z^n$, где $R_i\in\mathbb{R}[x], \deg R_i<\deg f$ для любого i. Но тогда $\deg R_n(x)f^n > \deg R_i(x)f^i$ для любого i, откуда бы следовало что $R(f(x),x)\neq 0$. Противоречие.

б) Представим h в виде несократимой дроби $\frac{h_+}{h_-}$. Тогда, очевидно, $T(y,z)=h_-(z)y-h_+(z)$ удовлетворяет условию $T(h(z),z)=0$. Проверим, что $T(y,z)$ является наименьшим по степени по z таким многочленом (его степень равна $\deg H$). Пусть есть многочлен $\widetilde{T}(y,z)$ меньшей степени. Положим $d:=\deg\widetilde{T}(y,z)$. Тогда $h_-^d\widetilde{T}(y,z)=Q(y,z)T(y,z)+R(z)$ для некоторых $Q(y,z)\in\mathbb{R}[y,z], R(z)\in\mathbb{R}[z]$. Из определения $\widetilde{T}$ следует, что $R(x)=0$, то есть $R=0$. Тогда
$$h_-^d(z)\widetilde{T}(y,z)=Q(y,z)T(y,z).$$
Из задачи 20 следует, что $Q(y,z)=h_-^a(z)\widetilde{Q}(y,z), T(y,z)=h_-^b(z)\widehat{T}(y,z)$ для некоторых $Q(y,z)\widehat{T}(y,z)\in\mathbb{R}[x,y], a,b\in\mathbb{Z}_{\ge 0}, a+b=d$. Но тогда $h_+(x)$ делится на $h_-(x)^b$, что возможно только если $b=0$. Откуда $a=d$ и
$$\widetilde{T}(y,z)=\widetilde{Q}(y,z)T(y,z).$$
Что противоречит предположению $\deg_z T(y,z)>\deg_z\widetilde{T}(y,z)$.

в) Заметим, что $[L:\mathbb{R}(x)]=[L:\mathbb{R}(g(x))][\mathbb{R}(g(x)):\mathbb{R}(x)]$. Что позволяет заменить L на $\mathbb{R}(g(x))$. А для $L=\mathbb{R}(g(x))$ утверждение пункта в) совпадает с утверждением пункта б). □

Решение задачи 32, Доказательство НОД-леммы. Пусть оказалось, что $\mathbb{R}(F, G) = \mathbb{R}(H)$ и $\deg H < HOD(\deg F, \deg G)$. Тогда $F = A(H)$, $G = B(H)$. Тогда $\mathbb{R}(A, B) = \mathbb{R}(x)$. При этом, согласно НОК-лемме (задача 7б) существуют такие P и Q, что $P(A) = Q(B)$ и $\deg P(A) = HOK(\deg A, \deg B)$.

Докажем, что многочлен $R(y, z) = P(y) - Q(z)$ — минимальный по степени для расширения поля $\mathbb{R}(A, B)$ над $\mathbb{R}(A)$ из предыдущей задачи. В самом деле, если бы был многочлен меньшей степени, при подставновке в которой A и B получался бы 0, то необходимо было бы сократить старший член по x в неком $A^s B^t$ со старшим членом какого-то другого $A^k B^l$. Тогда $(k-s)\deg A + (l-t)\deg B = 0$ и $k - s \neq 0$ делится на $\frac{\deg B}{HOD(\deg A, \deg B)}$, т.е. степень этого многочлена была бы хотя бы $\frac{\deg B}{HOD(\deg A, \deg B)} = \frac{HOK(\deg A, \deg B)}{\deg A} = \deg P$.

Но тогда

$$\deg A = [\mathbb{R}(x) : \mathbb{R}(A)] = [\mathbb{R}(A, B) : \mathbb{R}(A)] = \frac{HOK(\deg A, \deg B)}{\deg B} = \frac{\deg A}{HOD(\deg A, \deg B)} < \deg A.$$

Противоречие. □

Решение задачи 33. Следует из задачи 32 и задачи 29. □

Решение задачи 34. Следует из задачи 27 и задачи 29. □

Решение задачи 35, Доказательство Первой Теоремы Ритта. Будем доказывать утверждение теоремы по индукции по $\deg F$. Для $\deg F = 1$ утверждение очевидно.

Если G_r и H_s имеют одинаковую степень, то $G_r = aH_s + b$ и достаточно доказать утверждение для $G_1 \circ \ldots G_{r-1} \circ (ax + b) = H_1 \circ \ldots \circ H_{s-1}$, что следует из индуктивной гипотезы.

Если G_r и H_s имеют разную степень, то эти степени взаимно просты, иначе, согласно НОД-лемме (задача 9) имеем, что они разложимы. Тогда, согласно НОК-лемме (задача 7б), существуют многочлены C, D_1 и D_2, такие что $G_1 \circ \ldots G_{r-1} = C \circ D_1$, $H_1 \circ \ldots \circ H_{s-1} = C \circ D_2$, $D_1 \circ G_r = D_2 \circ H_s$, $\deg D_1 = HOK(\deg G_r, \deg H_s)/\deg G_r = \deg H_s$, $\deg D_2 = HOK(\deg G_r, \deg H_s)/\deg H_s = \deg G_r$. Тогда, согласно индуктивной гипотезе, все утверждения верны для многочленов $H_1 \circ \ldots \circ H_{s-1} = C \circ D_2$ и $G_1 \circ \ldots G_{r-1} = C \circ D_1$.

Если $C = C_1 \circ \ldots \circ C_l$ — декомпозиция C в неразложимые, то декомпозиции $C_1 \circ \ldots \circ C_l \circ D_1$ и $G_1 \circ \ldots G_{r-1}$ удовлетворяют теореме Ритта, а значит строится последовательность промежуточных демпозиций. Она трансформируется путем добавления в конец каждой декомпозиции многочлена G_r. А затем она может быть продолжена путем добавления аналогичных промежуточных декомпозиций между $C_1 \circ \ldots \circ C_l \circ D_2$ и $H_1 \circ \ldots \circ H_{s-1}$. □

Decompositions of polynomials, or the First Ritt Theorem

Authors[1]: Ya. Abramov, A.Petukhov, A.Terteryan

1 Introduction

This project has been motivated by the problem of classification of commuting polynomials, that is, of polynomial pairs $f(x)$ and $g(x)$ in a single variable, such that $f(g(x)) = g(f(x))$. We recommend to find out several such pairs on your own. In the sequel we denote the composition of polynomials in a single variable as follows:

$$f \circ g = f(g(x)).$$

The project is devoted to the auxiliary problem of *decomposition* of a polynomial into a **functional composition** of other polynomials: $F(x) = A \circ B = A(B(x))$. This problem arises naturally and is a part of the famous problem of classification of commuting polynomials. It is natural to study decomposition into indecomposable polynomials. We shall arrive to the following result regarding decomposition of an arbitrary polynomial into indecomposable ones, which resembles the theorem about decomposition of a positive integer into primes.

The first Ritt Theorem. Given two decompositions of a polynomial into a composition of indecomposable polynomials:

$$F(x) = G_1 \circ \ldots \circ G_r = H_1 \circ \ldots \circ H_s$$

(where $\deg G_i > 1$, $\deg H_j > 1$), we have the following:
1) $r = s$, thus the length of the decompositions is the same,
2) the sequences $(\deg G_1, \ldots, \deg G_r)$ and $(\deg H_1, \ldots, \deg H_r)$ of the degrees of the polynomials in the decompositions are permutations of each other,
3) there exists a sequence of intermediate decompositions $F(x) = F_1^{[i]} \circ \ldots \circ F_r^{[i]}$, such that

$$F_i^{[1]} = G_i \ (1 \le i \le r),$$

two its successive terms are connected by interchange of two neighboring polynomials (the corresponding degrees interchange and are coprime),

$$F_i^{[n]} = l \circ H_i \circ l^{-1} \ (1 \le i \le r),$$

where $l(x)$ is a linear function, $l^{-1}(x)$ is its inverse, that is, $l(l^{-1}(x)) = x$.

Example. For decompositions $x^{12} = x^3 \circ x^2 \circ x^2 = x^2 \circ x^2 \circ x^3$ the intermediate sequence consists of a single decomposition $x^{12} = x^2 \circ x^3 \circ x^2$.

Notation

In the sequel we assume the following:

i, j, k, l, m, n are arbitrary positive integers;

$A, B, C, D, F, G, H, P, Q, R$ are arbitrary polynomials (of a single variable if the contrary is not indicated);

x, y, z are variables of polynomials;

a, b, c, d are arbitrary numbers;

M, N are arbitrary sets.

[1]translated into English by B. Frenkin

2 Problems without hints

1. Prove existence of a polynomial
a) $T_2(x)$, b) $T_3(x)$, c) $T_4(x)$, d) $T_n(x)$
such that $T_n(\cos t) = \cos nt$ for any integer n. Express $T_{n+2}(x)$ in $T_{n+1}(x)$ и $T_n(x)$.

Definition 1. The polynomial $T_n(x)$ is called nth Chebyshev polynomial.

2. Prove existence of the polynomial
a) $D_2(x)$, b) $D_3(x)$, c) $D_4(x)$, d) $D_n(x)$
such that $D_n(t + \frac{1}{t}) = t^n + \frac{1}{t^n}$ for any integer n. Express $D_{n+2}(x)$ in $D_{n+1}(x)$ and $D_n(x)$.

Definition 2. The polynomial $D_n(x)$ is called nth Dickson polynomial.

Definition 3. A decomposition of a polynomial f is a sequence of polynomials $f_1, \dots, f_r$, such that $f = f_1 \circ \dots \circ f_r$. We will call two polynomials conjugate if they are connected by a transformation of the form $f(x) \to l^{-1} \circ f \circ l$ (where $l(x)$ is a linear function). Two decompositions $f_1, \dots, f_r$ и $g_1, \dots, g_r$ of a polynomial f will be called conjugate if $f_i = l_i^{-1} \circ g_i \circ l_{i+1}$, where $l_i(x)$ is a linear function, $l_1 = x$, $l_{r+1} = x$.

3. Decompose the polynomial a) $T_m(x)$, b) $D_m(x)$ into a composition of indecomposable polynomials.

4. a) Prove that if $F = G \circ H$ then $F(x) - F(y)$ as a polynomial in x, y is a multiple of $H(x) - H(y)$.
b) Prove that for given polynomials $A(x)$ and $B(x)$ there exists at most one polynomial $C(x)$ such that $A = C \circ B$.
c) Prove that if $F = G \circ H$ then $F'(x)$ as a polynomial is a multiple of $H'(x)$.

5. Prove that for a polynomial $f(x)$ with leading coefficient 1 and intercept 0 the number of decompositions into polynomials with the same properties is finite.

6. Prove that
a) for any polynomial $A(x)$ such that $\deg A = nr$ there exists the single $C(x)$ with leading coefficient 1, such that $\deg(A - C^r) < n(r-1)$,
b) if moreover there is a decomposition $A = P \circ Q$, $\deg Q = n$, then $A = B \circ C$ for some polynomial B.

7. a) Suppose that the residue of a polynomial $G(x)$ modulo $H(x)$ equals $R(x)$. Prove that the residue of $G(F(x))$ modulo $H(F(x))$ equals $R(F(x))$.
b) Prove that if $F = P \circ A = Q \circ B$ then $F = R \circ C$, where $\deg C = LCM(\deg A, \deg B)$, $C = A_1 \circ A = B_1 \circ B$.

8. a) Suppose $P \circ A = P \circ B$ for A and B with leading coefficient 1. Prove that $A = B$.
b) Suppose $C \circ F = D \circ F$ for F with leading coefficient 1. Prove that $C = D$.

9. * Prove that if $F = P \circ A = Q \circ B$ then $F = R \circ C$, where $\deg C = GCD(\deg A, \deg B)$.

10. Suppose $f_1, \dots, f_r$ and $g_1, \dots, g_r$ are two decompositions of a polynomial F, where all f_i and g_i are indecomposable and $\deg f_i = \deg g_i$. Prove that these decompositions are conjugate.

11. * (The first Ritt theorem formulated in alternative terminology.) [2] Prove that for any two decompositions of a polynomial into indecomposable ones $F = G_1 \circ \dots \circ G_r = H_1 \circ \dots \circ H_s$ (where $\deg G_i > 1$, $\deg H_j > 1$), the following holds:
1) $r = s$,
2) the sequences $(\deg G_1, \dots, \deg G_r)$ and $(\deg H_1, \dots, \deg H_r)$ are permutations of each other,
3) there exists a sequence of decompositions $F = F_1^{[i]} \circ \dots \circ F_r^{[i]}$, such that any two successive terms in it are connected by interchange of two neighboring polynomials (the corresponding degrees interchange and are coprime), $F_i^{[1]} = G_i$ $(1 \le i \le r)$, and $(F_1^{[n]}, \dots, F_r^{[n]})$ is conjugate to $(H_1, \dots, H_r)$.

[2]For starred problems, some auxiliary problems with hints will be given on August 4 and August 7.

3 Ritt theorem: first portion of auxiliary problems

12. Let $F(x) = G(H(x))$, $\deg G = m$, $\deg H = n$. Define polynomials in n variables e_i's as: $\sum_{i=0}^{n} t^i e_i(y_1, y_2, \ldots, y_n) = (t - y_1)(t - y_2)\ldots(t - y_n)$ (they are called elemenatry symmetric polynomials). Let polynomial $F(x)$ has exactly mn roots. Prove that roots of polynomial $F(x)$ can be organized in m groups of n elements $c_{11}, \ldots, c_{1n}, c_{21}, \ldots, c_{mn}$ such that for $i > 0$ holds $e_i(c_{11}, c_{12}, \ldots, c_{1n}) = = e_i(c_{21}, c_{22}, \ldots, c_{2n}) = \ldots = e_i(c_{m1}, c_{m2}, \ldots, c_{mn})$.

13. Is it true that $(x-1)(x-2)\ldots(x-999)$ is a composition of polynomials of degrees 27 and 37?

In the solutions for the preceding sections we have already made use of the idea of the set of various expressions in terms of a given polynomial or of several given polynomials. This idea can be generalized to some notions of higher mathematics, namely rings and fields. A ring is what we can obtain from some elements using addition, subtraction, multiplication and including constants. The case of fields is similar but the operation of division is also adjoined! We will make use of Lueroth theorem (the problem at the end of the section).

3.1 Rings

Definition 5. A *ring*[3] is a set R with three operations on it, called addition $(a+b)$, multiplication $(a \cdot b)$ and taking the opposite element $(-a)$, such that the following holds:
commutativity: 1) $a \cdot b = b \cdot a$, 2) $a + b = b + a$,
associativity: 3) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, 4) $a + (b + c) = (a + b) + c$,
distributivity: 5) $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$,
properties of zero: 6) there exists an element $0 \in R$ such that $a + 0 = a$ for any $a \in R$,
7) $a + (-a) = 0$,
8) there exists an element $1 \in R$ such that $a \cdot 1 = a$ for any $a \in R$.

Examples: as you know from the school curriculum, the sets $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ with natural operations have the above properties.

14 (Exercise)**.** For an arbitrary ring M introduce (describe) the operations of addition, multiplication and taking the inverse on the set of all polynomials in a single variable with coefficients from M (similar to the natural operations with polynomials).

Definition 6. The above ring will be denoted by $M[x]$ (where x is the variable, M is the set of possible coefficients).

Example. For the ring $\mathbb{R}[x_1, \ldots, x_n]$ of polynomials in n variables, the corresponding $\mathbb{R}[x_1, \ldots, x_n][y]$ is the ring $\mathbb{R}[x_1, \ldots, x_n, y]$ of polynomials in $n+1$ variables.

Definition 7. A subset A in a ring R is called a subring if it is closed under the operations of multiplication, addition and taking the opposite element (that is, if $a, b \in A$ then $a+b, a \cdot b, (-a) \in A$).

Now let us see how useful and powerful is the definition of the ring.

15. This problem is devoted to the proof of the following theorem: given a sequence of polynomials $f_1(x), \ldots, f_n(x), \ldots$, there exists k such that for any n we have

$$f_n(x) = F_n(f_1(x), \ldots, f_k(x)),$$

where $F_n(y_1, \ldots, y_k)$ are polynomials.
a) Consider the set M of all expressions obtained from the elements of this sequence using addition, multiplication, subtraction and multiplication by a constant. Prove that M is a subring in the ring of polynomials.
b) Consider the set N of all powers of elements of M. Prove that it is closed under addition and

[3]More precisely, a commutative ring with unit.

under multiplication by positive integers.
c) Prove that the set N is generated by a finite subset under multiplication by positive integers and addittion: every its element is obtained by these operations from a finite subset of N.
d) Prove that the ring R is generated by a finite number of its elements.
e) Prove the above theorem.

3.2 Fields

Definition 8. *A field* is a set $\mathbb{F}$ with four operations called addition $(a+b)$, multiplication $(a \cdot b)$, taking the opposite element $(-a)$ and taking the inverse element for a nonzero element (a^{-1}), such that the following holds:

1)-8) the same properties as in Definition 5 of a ring,

9) $a \cdot a^{-1} = 1$ for any $a \neq 0$ in $\mathbb{F}$.

Examples. The sets $\mathbb{Q}$, $\mathbb{R}$ with natural operations fulfil these conditions.

Remark. Not all customary operations are defined in the fields. For instance, the operation of root extraction is usually not executable in the field $\mathbb{Q}$ (as is well-known, $\sqrt{2} \notin \mathbb{Q}$).

16 (Exercise)**.** For a field $\mathbb{F}$ introduce (describe) the operations of multiplication, addition, taking the opposite and the inverse element on the set of all rational functions (expressions of the form $\frac{P(x)}{Q(x)}$, where P, Q are polynomials with convention that $\frac{A(x)B(x)}{A(x)C(x)} = \frac{B(x)}{C(x)}$) with coefficients from $\mathbb{F}$ (similar to the operations for rational functions with real coefficients).

Definition 9. This field will be denoted by $\mathbb{F}(x)$.

17 (Division with remainder)**.** Prove that for polynomials $A(x), B(x) \in \mathbb{F}[x]$ $(B(x) \neq 0)$ there exist polynomials $Q(x), R(x) \in \mathbb{F}[x]$ such that $A = B \cdot Q + R$ and $\deg B > \deg R$.

18 (Exercise for understanding)**.** Divide with remainder the polynomials in x with coefficients from $\mathbb{R}(y, z)$ (in the notation of the preceding problem, determine $Q(x)$ and $R(x)$ taking their coefficients from the set of rational functions in y and z):
a) $(x+y+z)^3 - x^3 - y^3 - z^3$ by $x + y$, b) $(x+y+z)^5 - x^5 - y^5 - z^5$ by $(x+y)(x+z)$.

19 (Greaterst common divisor of polynomials)**.** Prove that for polynomials $A(x), B(x) \in \mathbb{F}[x]$ a) there exists $GCD(A(x), B(x))$ b) and $GCD(A(x), B(x)) = A(x)P(x) + B(x)Q(x)$ for some $P(x)$, $Q(x) \in$ $\in \mathbb{F}[x]$.

20 (A version of Gauss lemma)**.** Suppose $C(x), D(x)$ are two polynomials from $S[x]$, where S is the ring of polynomials $\mathbb{R}[t]$ (that is, C and D are polynomials in x, and their coefficients are polynomials in t). Prove that all coefficients of their product $C(x)D(x)$ are coprime in $\mathbb{S}[t]$ in general (that is, coprime as polynomials in t) if each of them has coefficients coprime as polynomials in t).

Definition 10. A set A in a field $\mathbb{F}$ is called *a subfield* if it is closed under operations of addition, multiplication, taking the opposite and the inverse element A (that is, if $a, b \in A$, then $a + b, a \cdot b, (-a) \in A$ and if moreover $a \neq 0$, then $a^{-1} \in A$).

21. Prove that the set of all $E(g(x))$, where $g(x)$ is a fixed, and $E(x)$ is an arbitrary rational function, is a subfield in $\mathbb{R}(x)$.

22 (Lueroth theorem[4])**.** * Prove that any intermediate subfield $\mathbb{R} \subset K \subset \mathbb{R}(x)$ is the field of rational functions in some rational function $g(x)$: $K = \mathbb{R}(g(x))$.

23. Prove that if some intermediate field $\mathbb{R} \subset K \subset \mathbb{R}(x)$ contains a polynomial then the generator $g(x)$ in Lueroth theorem can be chosen among polynomials.

24. Prove that a polynomial F is *indecomposable* if and only if then any intermediate subfield $\mathbb{R}(F) \subset L \subset \mathbb{R}(x)$ is either $\mathbb{R}(F)$ or $\mathbb{R}(x)$.

[4]The second portion of auxiliary problems with hints regarding Ritt and Lueroth theorem will be delivered on August 7.

4 Ritt theorem: the second portion of auxiliary problems

4.1 Lueroth theorem and «its application in national economy»

Definition 11. <u>*The degree*</u> of a rational function, which can be expressed as irreducible fraction $\frac{p(x)}{q(x)} \neq 0$, is $\max\{\deg p(x), \deg q(x)\}$.

25. Prove that for $a, b, c, d \in \mathbb{F}$, $h(x) \in \mathbb{F}(x)$, $ad - bc \neq 0$ the degree of $\frac{ah(x)+b}{ch(x)+d}$ equals the degree of $h(x)$.

Definition 12. A subset M of a field $\mathbb{F} \subset \mathbb{R}(x)$ is called <u>*generating*</u> if all elements of $\mathbb{F}$ can be obtained from the elements of M by repeated use of addition, multiplication, taking the opposite and the inverse element and multiplication by constants.

26. (Lueroth theorem)
This problem is devoted to the proof of the following theorem: for any field K such that $\mathbb{R} \subset K \subset$ $\subset \mathbb{R}(x)$ there exists $z(x) \in \mathbb{R}(x)$ such that $K = \mathbb{R}(z(x))$. We give the algorithm for constructing such $z(x)$.
If $g(x)$ is a rational function then let the polynomials $P_g(x)$ and $Q_g(x)$ be its numerator and denominator:

$$g(x) = \frac{P_g(x)}{Q_g(x)},$$

where $GCD(P_g, Q_g) = 1$ and the leading coefficient of $Q_g(x)$ is 1.
For the rational function $g(x)$ let us consider an auxiliary expression $P_g(y) - g(x)Q_g(y)$ in variables x, y. Observe that it belongs to $\mathbb{R}(g(x))[y]$ (is a polynomial in y with coefficients from $\mathbb{R}(g(x))$).
a) Suppose that M is a generating set (not necessarily finite) for an intermediate subfield K. For all $g(x) \in M$ consider

$$GCD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big) = \frac{D(x,y)}{d(x)},$$

where $D(x, y)$ and $d(x)$ are polynomials. Prove that $D(x, y)$ is a multiple of $y - x$.
b) Prove that $GCD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big)$, after division by the leading coefficient, has the coefficients from K.
c) Prove that

$$P_g(x)Q_g(y) - P_g(y)Q_g(x) = D(x, y)C_g(x, y),$$

where $C_g(x, y)$ is a polynomial in x, y.
d) Let m be the least degree of rational functions in M, and $f(x) \in M$ be a rational function such that $\deg f = m$. Prove that if $\deg_y D(x, y) < m$ then $\deg_x C_f(x, y) > 0$ and $\deg_x D(x, y) < m$.
e) Suppose $\deg_y D(x, y) < m$. Prove that all coefficients of $\frac{D(x,y)}{d(x)}$ as a polynomial in y lie in K and have degree less than m.
f) Define the following procedure on M: append all nonconstant coefficients of $\frac{D(x,y)}{d(x)}$ to M and denote the resulting set by $M_{(1)}$. Now starting from $M_{(1)}$ construct the polynomial $\frac{D_1(x,y)}{d_1(x)} =$ $= GCD_{g\in M_{(1)}}\Big(P_g(y) - g(x)Q_g(y)\Big)$ and append its nonconstant coefficients to get the set $M_{(2)}$, and so on. Prove that repeating this procedure we arrive to the situation when

$$GCD_{g\in M}\Big(P_g(y) - g(x)Q_g(y)\Big) = c(x)(P_h(y) - h(x)Q_h(y))$$

for some $h(x) \in M$.
g) Prove that $P_h(y) - h(x)Q_h(y)$ (where h if from the preceding item) cannot be factorized in $\mathbb{R}[h(x), y]$.
h) Prove that $P_g(y)$ is not a multiple of $P_h(y) - h(x)Q_h(y)$ over $\mathbb{R}(h(x))$. (**Remark:** remind that

the coefficients of $P_g(y)$ are real and hence belong to $\mathbb{R}(h(x))$).
i) Suppose that for some $u(x) \in M$ the remainders of $P_u(y)$ and $Q_u(y)$ when divided by $P_h(y) - - h(x)Q_h(y)$ over $\mathbb{R}(h(x))$, are equal to $\frac{Q(h(x),y)}{q(h(x))}$ and $\frac{S(h(x),y)}{s(h(x))}$ respectively. Prove that $\frac{Q(h(x),y)}{q(h(x))} = = u(x)\frac{S(h(x),y)}{s(h(x))}$
j) Prove that $u(x)$ from the preceding item belongs to $\mathbb{R}(h(x))$.
k) Prove that $K = \mathbb{R}(h(x))$.

27. Prove that if $K = \mathbb{R}(h_1(x))$ then $h_1(x) = \frac{ah(x)+b}{ch(x)+d}$.

4.2 The rest of the proof of the first Ritt theorem

Definition 13. Let K, L be two fields such that $\mathbb{R} \subset K \subset L \subset \mathbb{R}(x)$. The degree of the field extension $[L\colon K]$ is the following integer. If $L = \mathbb{R}(f(x))$ then $K = \mathbb{R}(g(f(x)))$ (by Lueroth theorem). Then the degree $[L\colon K]$ is the degree of the rational function $g(x)$.

28. Prove that the definition of the degree is correct (that is, independent of the choice of generators in the subfields).

29. Suppose $H = r(F)$, where H, F are polynomials, and r is a rational function. Prove that r is a polynomial.

30. Prove that the degrees $[\mathbb{R}(F)\colon (\mathbb{R}(F) \cap \mathbb{R}(G))]$ and $[\mathbb{R}(G)\colon (\mathbb{R}(F) \cap \mathbb{R}(G))]$ are coprime.

31. a) Suppose $R(y, z)$ is a nonzero polynomial, $f(x)$ is a rational funcxtion and $R(f(x), x) = 0$ is an identity. Prove that $\deg_z R(y, z) \geqslant \deg f(x)$.
b) Let $h(x)$ be a rational function. Find a nonzero polynomial $T(y, z)$ of minimal possible degree in z, such that $T(f(x), x) = 0$ is an identity.
c) Let $S(y, z)$ be a nonzero polynomial $g(x) \in L \subset \mathbb{R}(x)$ and $R(g(x), x) = 0$ be an identity. Prove that $\deg_z S(y, z) \geqslant [L\colon \mathbb{R}(x)]$.

32. Let $H(x)$ be a polynomial such that $\mathbb{R}(H)$ is a field generated by polynomials $F(x)$ and $G(x)$. Prove that $\deg H = GCD(\deg F, \deg G)$.

33. (Remind Problem 9*.) Prove that if $F = P \circ A = Q \circ B$ then there exists a polynomial $C(x)$ such that $\deg C = GCD(\deg A, \deg B)$ and $A = A_1 \circ C$, $B = B_1 \circ C$.

34. Prove that A_1 and A_2 generate the same subfield if and only if then $A_1 = aA_2 + b$.

35. (The end of the proof for the first Ritt theorem.)
a) Suppose $\mathbb{R}(G_r) \neq \mathbb{R}(H_s)$. Prove that $\mathbb{R}(P) = \mathbb{R}(G_r) \cap \mathbb{R}(H_s)$, where P is a polynomial of degree $\deg G_r \cdot \deg H_s$.
b) Let the polynomial P from the preceding item be such that $P = A \circ G_r$ and $A = A_1 \circ A_2$. Prove that either $\mathbb{R}(P) = \mathbb{R}(A_2 \circ G_r)$ (and then $\deg A_1 = 1$) or $\mathbb{R}(H_s, A_2 \circ G_r) = \mathbb{R}(x)$ (and then $\deg A_1 = \deg A$).
c) Prove the first Ritt theorem.

Ritt: solutions for some problems

Translated by Ya. Abramov, A. Petukhov and A. Terteryan and edited by B. Frenkin

Solutiom for Problem 1. It is clear that for all $n \in \mathbb{N}$ such polynomial is unique if it exists: two different polynomials can't take the same values in every point from $[-1, 1]$, range of cosine. It is also clear that we can pick $T_1(x) = x$, $T_2(x) = 2x^2 - 1$, and then we define sequence $T_1, T_2, T_3, \ldots$ by recurrence relation $T_{n+2}(x) = 2xT_{n+1}(x) - T(x)$, and by induction proof it is exactly what we need.

The base is true by construction, and the step follows from the formula $\cos\alpha\cos\beta = \frac{1}{2}(\cos(\alpha+\beta) + \cos(\alpha-\beta))$. We have:

$$T_{n+2}(\cos t) = 2\cos t \cos((n+1)t) - \cos(nt) = \cos((n+2)t) + \cos(nt) - \cos(nt) = \cos((n+2)t).$$

□

Solution for Problem 2. We act similarly to the previous problem: such polynomial is unique if it exists: two different polynomials can't take the same values in every point from $(-\infty, -2] \cup [2, +\infty)$, the range of function $f(t) = t + \frac{1}{t}$. We define $D_1(x) = x, D_2(x) = x^2 - 2$, and recurrently $D_{n+2}(x) = xD_{n+1}(x) - D_n(x)$. By induction we prove that $D_n(t + \frac{1}{t}) = t^n + \frac{1}{t^n}$: if $n \in \{1, 2\}$ then this is clear, and the induction step follows from

$$D_{n+2}(t + \frac{1}{t}) = (t + \frac{1}{t})(t^{n+1} + \frac{1}{t^{n+1}}) - (t^n + \frac{1}{t^n}) = t^{n+2} + \frac{1}{t^n} + t^n + \frac{1}{t^{n+2}} - t^n - \frac{1}{t^n} = t^{n+2} + \frac{1}{t^{n+2}}.$$

□

Solution for Problem 3. **Observation.** A polynomial of prime degree can't be decomposed into the composition of two polynomials of degrees greater than 1.

Proof. Suppose $A = B \circ C$ is such decomposition. Then $deg\,A = (\deg B) \cdot (\deg C)$ is not prime, a contradiction. □

Let $m = p_1 \cdot \ldots \cdot p_d$ be a decomposition of m into prime factors (perhaps some factors are equal).

Let n, k be arbitrary positive integers. For every non-zero $t \in \mathbb{R}$ we have: $D_n(D_k(t+\frac{1}{t})) = D_n(t^k + \frac{1}{t^k}) = (t^k)^n + \frac{1}{(t^k)^n} = t^{nk} + \frac{1}{t^{nk}} = D_{nk}(t+\frac{1}{t})$, therefore polynomials D_{nk} and $D_n \circ D_k$ coincide on $(-\infty, -2] \cup [2, +\infty)$ (the range of the function $f(t) = t + \frac{1}{t}$), so they are equal to each other. This implies that we have a decomposition $D_m = D_{p_1} \circ \ldots \circ D_{p_d}$. By the above observation, now it will be enough to prove that the degree of every component is a prime number. For this, it will be enough to prove that for every positive integer n the degree of D_n is equal to n. And this is trivial by induction: for $n \in \{1, 2\}$ it is true, and the inductive step is trivial by relation $D_{n+2}(x) = xD_{n+1}(x) - D_n(x)$. Exactly the same argument shows that $T_m = T_{p_1} \circ \ldots \circ T_{p_d}$ is a suitable decomposition of T_m. □

Solution for Problem 4. 4a) We have $\frac{a^n - b^n}{a-b} = a^{n-1} + a^{n-2}b + \ldots + b^{n-1}$. This implies that the polynomial $(a-b)$ divides the polynomial $F(a) - F(b)$. Replacing a and b by $H(x)$ and $H(y)$ we obtain the desired statement.

4c) We have $F' = H'(x)G'(H(x))$. □

Solution of Problem 5. Assume that $F(x) = G \circ H$ with F, G, H as in Problem 5. It is enough to show that the list of such decompositions with fixed $d_g = \deg G, d_h = \deg H$ is finite $(\deg G \cdot \deg H = \deg F)$. Polynomial H is monic and thus the leading term of H' is $d_H x^{d_H - 1}$. Polynomial F' has only finitely many multiples with the leading term $d_H x^{d_H - 1}$. This implies the desired result. □

Solution for Problem 6. It is clear that $\deg C(x) = n$.

Firstly we will show that such a polynomial $C(x)$ is unique under the assumption that $C(x)$ exists. Assume to the contrary that there are two such polynomials $C_1(x), C_2(x)$. Then $\deg(C_1^r - C_2^r) < n(r-1)$. We have

$$(C_1^r - C_2^r) = (C_1 - C_2)(C_1^{r-1} + \ldots + C_2^{r-1}).$$

The leading term of each summand of the second multiple is $x^{n(r-1)}$. Therefore the resulting leading term of the second multiple is $rx^{n(r-1)}$. If the first multiple is nonzero then $\deg(C_1^r - C_2^r) \geq n(r-1)$. This is a contradiction.

Now we show that at least one such $C(x)$ exists. Consider polynomial $C(x)$ with the minimal possible $\deg(A - C^r)$ (if there is more then one such polynomial, we take any one). Set $d := nr - \deg(A - C^r)$. If $d \geq r$ then $C(x)$ satisfies the desired condition. This allows us to assume that $d \leq r - 1$. We have $\deg(A - (x^n)^r) < nr$ and therefore $d \geq 1$. Then the leading term of $A - C^r$ is kx^{nr-d} for some coefficient k. Consider $(A - (C + \frac{k}{n}x^{n-d}))$. It is easy to see that

$$\deg(A - (C + \frac{k}{r}x^{n-d})) < nr - d.$$

This contradicts our minimality assumption on $C(x)$. □

Solution for Problem 7. 7a) The identity for the remainder and the incomplete quotient is the same and the condition $\deg R(F(x)) < \deg H(F(x))$ is obvious.

7b) We can assume that the leading coefficients of A and B are 1. Consider the polynomial $D = S(A) = T(B)$ of least possible degree which is a polynomial both of A and B at the same time (we choose the leading coefficients of S and T to be 1). Let

$$\deg A = ag, \deg B = bg, g = GCD(\deg A, \deg B), \deg D = dabg.$$

Then $\deg S = bd$, $\deg T = ad$. From Problem 6a we have that there exists a polynomial U of degree b with leading coefficient 1, such that $\deg(S(A) - U^d(A)) < b(d-1)a$, and also there exists polynomial V of degree a with leading coefficient 1, such that $\deg(T(B) - V^d(B)) < a(d-1)b$. Then

$$\deg(U^d(A) - V^d(B)) = \deg(U^d(A) - T(B) + T(B) - V^d(B)) = \deg(U^d(A) - S(A) + T(B) - V^d(B)) \leqslant$$

$$\leqslant \max(\deg(U^d(A) - S(A)), \deg(T(B) - V^d(B))) < a(d-1)b.$$

Also we have

$$U^d(A) - V^d(B) = (U(A) - V(B))(U^{d-1}(A) + \ldots + V^{d-1}(B)).$$

The degrees of each summand in $U^{d-1}(A) + \ldots + V^{d-1}(B)$ are the same and equal to $(d-1)ab$, and the leading coefficient is everywhere 1. So the degree of the second factor in $(U(A) - V(B))(U^{d-1}(A) + \ldots + V^{d-1}(B))$ equals $ab(d-1)$. At the same time the product itself has degree lesser than $ab(d-1)$, according to the previous argument. So $U(A) - V(B) = 0$. If $d > 1$ then we have $U(A) = V(B)$, a polynomial of lesser degree than D, which is a polynomial of both A and B, a contradiction. Since by Problem 6b $\deg F$ is a multiple of $\deg D$, we have that F is a polynomial of D. □

Solution for Problem 8. 8a) A direct corollary of Problem 6b.

8b) The polynomial $C - D$ equals zero on the image set of the polynomial F, so by Bezout Theorem C and D are equal. □

Solution for Problem 10. Note that, according to problem 7b, the polynomials $F_i = f_i \circ f_{i+1} \circ \ldots \circ f_n$ and $G_i = g_i \circ g_{i+1} \circ \ldots \circ g_n$ are polynomials of each other, hence they are connected by a linear relation $F_i = a_i G_i + b_i$. This linear relation will be the desired $l_i(y) = a_i y + b_i$ from the definition of conjugation. □

Ritt: solutions for yet more problems

Translated by Ya. Abramov, A. Petukhov and A. Terteryan and edited by B. Frenkin

Solution for Problem 12. Let $(x-a_1)(x-a_2)\dots(x-a_{mn}) = F(x) = G(H(x))$, $\deg G = m$, $\deg H = n$. Then $G(x)$ has exactly m roots. Let these roots be $b_1, b_2, \dots, b_m$. Then

$$F(x) = (H(x)-b_1)(H(x)-b_2)\dots(H(x)-b_m).$$

Then a part of the roots are roots of $H(x)-b_1$, another part are roots of $H(x)-b_2,\dots$, and so we exhaust all the roots of $F(x)$. Rearrange roots of $F(x)$ so that the first n of them would be roots of $H(x)-b_1$, the second n ones would be roots of $H(x)-b_2,\dots$. Let us prove that we obtain the desired partition. Indeed, $\sum_{i=0}^n h_i x^i - b_j = H(x) - b_j = (x-c_{j1})\dots(x-c_{jn}) = \sum_{i=0}^n e_i(c_j)x^i$. □

Solution for Problem 13. Assume it happened to be as required in the Problem. Let us divide roots into m groups of n elements in each similarly to the previous Problem.

Select the roots divisible by some prime number p. Let us prove that these roots are distributed equally between some of the groups of the above distribution (the other groups include no such roots). Let there be groups A_1 and A_2 with $0 < k_1 < k_2$ roots respectively, divisible by p. The polynomial $e_{n-k_1}(x_1,\dots,x_n)$ is the sum of all possible non-repeating products of $n-k_1$ variables in the list $x_1,\dots,x_n$. Then for group A_1 the value e_{n-k_1} won't be divisible by p (i.e. exactly one summand won't be divisible by p). But for the group A_2 the value e_{n-k_1} is divisible by p. This contradicts with the result of the previous problem that for $i \neq 0$ the values e_i for roots from different groups would be equal.

Set now $p = 23$. There are exactly $[\frac{999}{23}] = 43$ roots divisible by 23. According to the above statements all the roots (which are divisible by p) should be distributed in several equal groups, and so either all these roots are in one group or each group includes just one element. Both cases are impossible, because all the groups are either of 27 or of 37 elements and there are either 27 or 37 groups in total. □

Solution for Problem 14. Addition: $\sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i+b_i)x^i$.

Multiplication: $(\sum_i a_i x^i)\cdot(\sum_j b_j x^j) = \sum_l x^l \sum_{i+j=l} a_i b_j$.

Negation: $-\sum_i a_i x^i = \sum_i (-a_i x^i)$.

Checking of agreement with definition:

Commutativity laws:

$$A(x)+B(x) = \sum_i a_i x^i + \sum_i b_i x^i = \sum_i (a_i+b_i)x^i = \sum_i (b_i+a_i)x^i = \sum_i b_i x^i + \sum_i a_i x^i = B(x)+A(x),$$

$$A(x)\cdot B(x) = (\sum_i a_i x^i)\cdot(\sum_j b_j x^j) = \sum_l x^l \sum_{i+j=l} a_i b_j = \sum_l x^l \sum_{j+i=l} b_j a_i = (\sum_j b_j x^j)\cdot(\sum_i a_i x^i) = B(x)\cdot A(x).$$

Associativity laws:

$$(A(x)+B(x))+C(x) = \sum_i ((a_i+b_i)+c_i)x^i = \sum_i (a_i+(b_i+c_i))x^i = A(x)+(B(x)+C(x)),$$

$$(A(x)\cdot B(x))\cdot C(x) = \sum_l x^l \sum_{i+j+k=l} a_i b_j c_k = A(x)\cdot(B(x)\cdot C(x)).$$

Distributivity law:

$$A(x)\cdot(B(x)+C(x)) = \sum_l x^l \sum_{i+j=l} a_i(b_j+c_j) = \sum_l x^l(\sum_{i+j=l} a_i b_j + \sum_{i+j=l} a_i c_j) = A(x)\cdot B(x) + A(x)\cdot C(x).$$

Properties of zero:

$$A(x)+(-A(x)) = \sum_i (a_i-a_i)x^i = 0,$$

$$0\cdot A(x)=\sum_l x^l\sum_{i+j=l}0a_i=0.$$

Property of unit:

$$1\cdot A(x)=\sum_l x^l(1a_l+\sum_{i+j=l,i>0}0a_j)=\sum_l a_lx^l=A(x).$$

So, all the conditions (1-8) hold for any such polynomials. $\square$

Solution for Problem 15. 15a) Indeed, the operations of addition, multiplication and subtraction don't lead out of the set M: their results just give sums, products and differences of the corresponding expressions, which are also expressions in terms of the given polynomials, so they belong to M by definition.

15b) Note that $\deg(F\cdot G)=\deg F+\deg G$ and $\deg F^n=n\deg F$. This proves what is needed.

15c) Let m be the least element in N. Then every number, divisible by it, also belongs to N. Let $r_1,r_2,\dots,r_s$ be the list of all possible remainders under division of elements of N by m. Denote by k_i the least element in N which equals r_i modulo m. Then all the numbers of the form k_i+lm, where l is nonnegative integer, also belong to N, according to Problem 15b. The list of the numbers of such form exhausts N. So N is generated by elements $m,k_1,k_2,\dots k_s$ and this list is finite.

15d) Let $d_1,\dots,d_r$ be a set of generators for N. Let $g_1(x),\dots,g_r(x)\in M$ be monic polynomials with these degrees. Let us prove that they generate M. Indeed, let $f(x)$ be a polynomial of the least degree in M and not expressible in $g_1,\dots,g_r$. By dividing it by its leading coefficient we make it monic. Then $\deg f=n_1d_1+\ldots+n_rd_r$. Furthermore $\deg(f-g_1^{n_1}g_2^{n_2}\dots g_r^{n_r})<\deg f$ and $f-g_1^{n_1}g_2^{n_2}\dots g_r^{n_r}\in M$ is not expressible in g_i's and has lesser degree than f. Contradiction.

15e) It is sufficient to take finite sets of f_i's, generating all of the g_j's. $\square$

Solution for Exercise 16. Define the operations in the following way : $\frac{P_1}{Q_1}+\frac{P_2}{Q_2}:=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}$, $\frac{P_1}{Q_1}\cdot\frac{P_2}{Q_2}:=\frac{P_1P_2}{Q_1Q_2}$, $-\frac{P_1}{Q_1}:=\frac{-P_1}{Q_1}$, and
$(\frac{P_1}{Q_1})^{-1}:=\frac{Q_1}{P_1}$, for $P_1\neq 0$.

Let's check that the operations are well defined (the result of an operation doesn't depend on choice of polynomials in realization of a rational function). Let $P_1,Q_1,P_2,Q_2,\widetilde{P_1},\widetilde{Q_1},\widetilde{P_2},\widetilde{Q_2}$ be polynomials, such that $\frac{P_1}{Q_1}=\frac{\widetilde{P_1}}{\widetilde{Q_1}}$ and $\frac{P_2}{Q_2}=\frac{\widetilde{P_2}}{\widetilde{Q_2}}$, i.e. $P_1\widetilde{Q_1}=\widetilde{P_1}Q_1$ и $P_2\widetilde{Q_2}=\widetilde{P_2}Q_2$. We have:
for sum: $\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}=\frac{P_1Q_2\widetilde{Q_1}\widetilde{Q_2}+P_2Q_1\widetilde{Q_1}\widetilde{Q_2}}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}Q_1Q_2\widetilde{Q_2}+\widetilde{P_2}Q_1\widetilde{Q_1}Q_2}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{Q_2}+\widetilde{P_2}\widetilde{Q_1}}{\widetilde{Q_1}\widetilde{Q_2}}$.
For product: $\frac{P_1P_2}{Q_1Q_2}=\frac{P_1P_2\widetilde{Q_1}\widetilde{Q_2}}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{P_2}Q_1Q_2}{Q_1Q_2\widetilde{Q_1}\widetilde{Q_2}}=\frac{\widetilde{P_1}\widetilde{P_2}}{\widetilde{Q_1}\widetilde{Q_2}}$.
For the opposite element: $\frac{-P_1}{Q_1}=\frac{-P_1\widetilde{Q_1}}{Q_1\widetilde{Q_1}}=\frac{-\widetilde{P_1}Q_1}{Q_1\widetilde{Q_1}}=\frac{-\widetilde{P_1}}{\widetilde{Q_1}}$.
For the inverse element: $\frac{Q_1}{P_1}=\frac{Q_1\widetilde{P_1}}{P_1\widetilde{P_1}}=\frac{\widetilde{Q_1}P_1}{P_1\widetilde{P_1}}=\frac{\widetilde{Q_1}}{\widetilde{P_1}}$.

The operations are well defined, then let's check that the axioms of field are satisfied. Let P_1,Q_1,P_2,Q_2,P_3,Q_3 be arbitrary polynomials such that Q_1,Q_2,Q_3 are non-zero. It's trivial that addition is commutative, $\frac{0}{1}$ is the neutral element under addition, and for every element there exists the opposite element. Let's check associativity of addition:
$(\frac{P_1}{Q_1}+\frac{P_2}{Q_2})+\frac{P_3}{Q_3}=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}+\frac{P_3}{Q_3}=\frac{P_1Q_2Q_3+P_2Q_1Q_3+Q_1Q_2P_3}{Q_1Q_2Q_3}=\frac{P_1}{Q_1}+\frac{P_2Q_3+P_3Q_2}{Q_2Q_3}=\frac{P_1}{Q_1}+(\frac{P_2}{Q_2}+\frac{P_3}{Q_3})$. Furthermore it's trivial that multiplication is commutative and associative, and $\frac{1}{1}$ is the neutral element under multiplication, and for every non-zero element there exists the multiplicative inverse. It's trivial that $\frac{1}{1}\neq\frac{0}{1}$. Let's check distributivity of multiplication relative to addition:
$(\frac{P_1}{Q_1}+\frac{P_2}{Q_2})\frac{P_3}{Q_3}=\frac{P_1Q_2+P_2Q_1}{Q_1Q_2}\cdot\frac{P_3}{Q_3}=\frac{P_1Q_2P_3+P_2Q_1P_3}{Q_1Q_2Q_3}=\frac{P_1Q_2P_3Q_1Q_2Q_3+P_2Q_1P_3Q_1Q_2Q_3}{Q_1Q_2Q_3Q_1Q_2Q_3}=\frac{P_1Q_2P_3}{Q_1Q_2Q_3}+\frac{P_2Q_1P_3}{Q_1Q_2Q_3}=$
$=\frac{P_1P_3}{Q_1Q_3}+\frac{P_2P_3}{Q_2Q_3}=\frac{P_1}{Q_1}\cdot\frac{P_3}{Q_3}+\frac{P_2}{Q_2}\cdot\frac{P_3}{Q_3}$. $\square$

Solution for problem 17. In the case when $B=b$, a non-zero constant, the statement is trivial: $A=b\cdot(b^{-1}A)+0$. Therefore we can (and we do) assume that $B(x)=\sum_{j=0}^n b_jx^j$, where $n\in\mathbb{N}$ is the degree of B.

We prove our statement by induction by degree of A. For A with degree less than n the statement is trivial: we can pick $Q = 0, R = A$. So, it's enough to prove that, if our statement is true for every polynomial A with degree not greater than k, where $k \geq n-1$, then it is true for polynomials with degree $k+1$. Let $A = \sum_{j=1}^{k+1} a_j x^j$, an arbitrary polynomial with degree $k+1$, then $A - a_{k+1}(b_n)^{-1}Bx^{k+1-n}$ is a polynomial with degree not greater than k. By inductive assumption, for some polynomials Q, R with $deg\, R < deg\, B$ we have
$A - a_{k+1}(b_n)^{-1}Bx^{k+1-n} = B(x) \cdot Q(x) + R(x)$, therefore
$A(x) = B(x) \cdot (Q(x) + a_{k+1}(b_n)^{-1}x^{k+1-n}) + R(x)$, as required. □

Solution for problem 18. a) $(x+y+z)^3 - x^3 - y^3 - z^3 = 3(x+y)(y+z)(x+z) + 0$, this can be checked directly. But we have another way: it's trivial that, in both parts of equation we have polynomials with degree 2 (in x). In view of this, it will be enough to check that the values of parts coincide at 3 different points from $\mathbb{R}(y,z)$. It's easy to see that values coincide when $x \in \{-y, -z, 0\}$.

b) $(x+y+z)^5 - x^5 - y^5 - z^5 = 5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0$, it can be checked directly. But we have another way: it's trivial that, in both parts of equation we have polynomials with degree 4 (in x). In view of this it will be enough to check that the values of parts coincide at 5 different points from $\mathbb{R}(y,z)$. It's trivial that for $x = -y$, and $x = -z$ values of parts coincide. When $x = -y-z$ we have: $(x+y+z)^5 - x^5 - y^5 - z^5 = (y+z)^5 - y^5 - z^5 = 5y^4z + 10y^3z^2 + 10y^2z^3 + 5yz^4$, and
$5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0 = 5(-z)(-y)(y+z)((x+y+z)^2 - xy - xz - zy) =$
$= 5yz(y+z)(-zy + (z+y)^2) = 5yz(y+z)(z^2+yz+y^2) = 5yz(z^3+yz^2+y^2z+y^3+yz^2+y^2z) =$
$= 5yz(z^3+2z^2y+2zy^2+y^3) = 5z^4y + 10z^3y^2 + 10z^2y^3 + 5zy^4$. When $x = -y-1$ we have
$(x+y+z)^5 - x^5 - y^5 - z^5 = (z-1)^5 - z^5 + (y+1)^5 - y^5 = -5z^4 + 10z^3 - 10z^2 + 5z - 1 + 5y^4 +$
$+ 10y^3 + 10y^2 + 5y + 1 = 5(y^4 - z^4 + 2y^3 + 2z^3 + 2y^2 - 2z^2 + y + z)$, and
$5(x+y)(x+z)(y+z)(x^2+y^2+z^2+xy+zx+yz)+0 = -5(z-y-1)(y+z)((x+y+z)^2 - z(x+y) - xy) =$
$= 5(y+1-z)(y+z)((z-1)^2 + z + y^2 + y) = 5(y+z)(y+1-z)(z^2 - z + 1 + y^2 + y) =$
$= 5(y^2 + y - zy + zy + z - z^2)(z^2 - z + 1 + y^2 + y) = 5(y^2 - z^2 + z + y)(z^2 - z + 1 + y^2 + y) =$
$5((y^2+y) - (z^2-z))((y^2+y) + (z^2-z) + 1) = 5((y^2+y)^2 - (z^2-z)^2 + (y^2+y) - (z^2-z)) =$
$= 5(y^4 + 2y^3 + y^2 - z^4 + 2z^3 - z^2 + y^2 + y - z^2 + z) = 5(y^4 - z^4 + 2y^3 + 2z^3 + 2y^2 - 2z^2 + y + z)$. Similarly the values coincide when $x = -z-1$. □

a) $(x+y+z)^3 - x^3 - y^3 - z^3 = (x+y)^3 + 3(x+y)^2z + 3(x+y)z^2 + z^3 - (x+y)(x^2 - xy + y^2) - z^3 =$
$= (x+y)((x+y)^2 + 3(x+y)z + 3z^2 - x^2 + xy - y^2) + 0$.

Solution for Problem 19. We assume that at least one of the polynomials is not zero. If one of the polynomials is zero then it's trivial that another one is the GCD and can be written in the form that we need, therefore further we assume that A, B are non-zero polynomials.We will prove both statements together (for non-zero polynomials) by induction by $n = min(deg\, A,\, deg\, B)$. When $n = 0$ it's trivial that 1 is the GCD and it can be written in the form that we need. Inductive step: Suppose for $n \leq k$ (where $k \geq 0$) the statements are true, let's prove that they are true for $n = k+1$. Without loss of generality we can assume that
$\deg A \geq \deg B$. Divide A by B with remainder: $A = BD + R$. If $R = 0$ then it's trival that B is the GCD of A and B and it can be written in the form that we need. If $R \neq 0$, then pair (B, R) satisfies the conditions of the statement of inductive assumption, then let $X = BV + RW = GCD(B, R)$, where V, W are polynomials. As $A = BD + R$, it is not hard to see that the set of all common divisors of polynomials A and B coincides with the set of all common divisors of polynomials B and R. Therefore X is the GCD of A and B. Finally we have $X = BV + (A - BD)W = AW + B(V - DW)$, and the inductive step is proved. □

Solution for Problem 20. Assume that the coefficients of $R(x) = C(x)D(x)$ are not coprime. Then there exists $\lambda \in \mathbb{C}$ such that $R(x)$ becomes zero if we replace t by λ; we denote this substitution $R(x)\mid_{t=\lambda}$. We have $C(x)\mid_{t=\lambda}\cdot D(x)\mid_{t=\lambda}=0$. Therefore either $C(x)\mid_{t=\lambda}=0$ or $D(x)\mid_{t=\lambda}=0$. This implies the desired result. □

Solution for Problem 21. This statement is straightforward but let's check it (we need to check that "+" and "·" preserve the mentioned set of functions $E(g(x))$).

$$+: \quad \frac{A(g(x))}{B(g(x))}+\frac{C(g(x))}{D(g(x))}=\frac{(A\cdot D+B\cdot C)(g(x))}{(B\cdot D)(g(x))},$$

$$\cdot: \quad \frac{A(g(x))}{B(g(x))}\cdot\frac{C(g(x))}{D(g(x))}=\frac{(A\cdot C)(g(x))}{(B\cdot D)(g(x))}.$$

□

Solution for Problem 23. Assume that there exists a sequence of fields $\mathbb{R}\subset K\subset\mathbb{R}(x)$ and K contains a polynomial $g(x)\in\mathbb{R}[x]\backslash\mathbb{R}$. We will check that $K=\mathbb{R}(f(x))$ for some $f(x)\in\mathbb{R}[x]$. Lüroth theorem implies that $K=\mathbb{R}(\widetilde{f})$ for some $\widetilde{f}\in\mathbb{R}(x)$; $f=\frac{f_+}{f_-}$, with $f_+,f_-\in\mathbb{R}[x]$ и $(f_+,f_-)=1$.

Note that $\mathbb{R}(g(x))\subset K=\mathbb{R}(\widetilde{f})$, and thus there exists

$$s\in\mathbb{R}(x)\colon s(\tilde{f})=g(x);$$

$s=\frac{s_+}{s_-}$, with $s_+,s_-\in\mathbb{R}[x]$ and $(s_+,s_-)=1$. Hence $\frac{s_+(\frac{f_+}{f_-})}{s_-(\frac{f_+}{f_-})}=g(x)$. Denote by $\alpha_1,\dots,\alpha_{n_+}$ the roots of s_+, and denote by $\beta_1,\dots,\beta_{n_-}$ the roots of s_-; set C_+,C_- to be the leading coefficient of s_+ and s_- respectively.

Without loss of generality we can assume that $f_-\notin\mathbb{R}$. Combining the notation we have:

$$g(x)=\frac{C_+}{C_-}\frac{f_-^{n_--n_+}(f_+-\alpha_1f_-)(f_+-\alpha_2f_-)\dots(f_+-\alpha_{n_+}f_-)}{(f_+-\beta_1f_-)(f_+-\beta_2f_-)\dots(f_+-\beta_{n_-}f_-)}.$$

Note that if $\alpha\neq\beta$ then $(f_1-\alpha f_2,f_1-\beta f_2)=1$. Further we have that $(f_2,f_1-\gamma f_2)$ for all $\gamma\in\mathbb{C}$. This means that the factors in the above formula are mutually coprime and hence they can't cancel. The fact that $g(x)$ is a polynomial implies that either (1) or (2):

(1) $n_-=0$;

(2) $n_->0$ and $\deg(f_+-\beta_if_-)=0$ for all $i, 1\leqslant i\leqslant n_-$.

If (1) then $n_+=0$ and therefore $g(x)\in\mathbb{R}$ (this is a contradiction); if $n_+>0$ then the factor $f_-^{n_--n_+}$ will provide a nontrivial contribution into the denominator of $g(x)$ (and this contradicts the fact that $g(x)$ is a polynomial). If (2) then $f_+-\beta_1f_-=C_0$ for a nonzero constant C_0. This implies that $K=\mathbb{R}(\tilde{f})=\mathbb{R}(f_+)$ as desired. □

Solution for Problem 24. Assume $F\in\mathbb{R}[x]$ is a decomposable polynomial, i.e., $F(x)=G(H(x))$ for some $G,H\in\mathbb{R}[x]$ with $\deg G>1,\deg H>1$. Then set $L:=\mathbb{R}(H(x))$; for this L we have: $\mathbb{R}(F)\subsetneq\mathbb{R}(H)\subsetneq\mathbb{R}(x)$. These arguments solve a half of our problem.

To solve the other half we need to check the following statement: let L be a field with $\mathbb{R}(F)\subsetneq L\subsetneq\mathbb{R}(x)$, then $F(x)$ is decomposable. Note that L contains polynomial F and therefore $L=\mathbb{R}(H(x)),H\in\mathbb{R}[x]$ due to problem 23. Lüroth theorem implies that there exists $G\in\mathbb{R}(x)$ such that $F(x)=G(H(x))$. Repeating the arguments of problem 23 we represent $G(x)$ as a ratio of two coprime polynomials, consider the roots of these polynomials and their leading terms. This provides the following formula:

$$F(x)=\frac{C_+}{C_-}\frac{(H(x)-\alpha_1)(H(x)-\alpha_2)\dots(H(x)-\alpha_{n_+})}{(H(x)-\beta_1)(H(x)-\beta_2)\dots(H(x)-\beta_{n_-})}.$$

All the factors will be mutually coprime (this is completely analogous with what we have in problem 23) and hence $F(x)$ is polynomial only if all the multiples of the denominator are constants. This can be the case only if either $H(x)\in\mathbb{R}$ or $n_+=0$. We have $H(x)\notin\mathbb{R}$ and this excludes the first case. The second case guarantees that $G(x)\in\mathbb{R}[x]$ and thus $F(x)$ is decomposable as desired. □

Ritt: yet more solutions for yet more problems

Translated by Ya. Abramov and edited by B. Frenkin

Solution for Problem 26. We will make trivial assumption that K is not $\mathbb{R}$.

26a) By construction x is a root of all our expressions, so they are divisible by $y-x$ in the ring $\mathbb{R}(x)[y]$, and the rest is clear from corollaries to Gauss Lemma.

26b) Let us consider the canonical expression of GCD as a product of powers of irreducible polynomials. For each multiplier we choose the expression such that this multiplier counts there in the same degree as it counts in the GCD expression. We have chosen a finite number of expressions, and by construction their GCD coincides with the GCD of our expressions. For finite number of expressions their GCD can be found by Euclid's algorithm, its iterations doesn't lead coefficients out of field K, so the quotient of each two coefficients (if defined) also belongs to K.

26c) Follows immediately from possibility of factoring left side and irreducibility of fraction $\frac{D(x,y)}{d(x)}$.

From now on we will choose the constructed GCD as a polynomial with leading coefficient 1. So, in its realisation as $\frac{D(x,y)}{d(x)}$ polynomial $D(x,y) \in \mathbb{R}[x][y]$ will have leading coefficient $d(x)$, and all coefficients of $D(x,y)$ will be coprime in total as elements of $\mathbb{R}[x]$.

26d) Directly from the definition of the degree of a rational function we have that $P_f(y)Q_f(x) - P_f(x)Q_f(y)$ is a polynomial of degree m in each of the variables. It is clear that this polynomial is antisymmetric. Then conditions $\deg_x D(x,y) < m$ and $\deg_x C_f(x,y) > 0$ are equivalent, so it is sufficient to prove the second one. Assume it doesn't hold. So $C_f(x,y)$ is a polynomial in y. From antisymmetry property we have that $D(x,y)C_f(x,y)$ is not divisible by $C_f(y,x)$, which is a polynomial in x. So we have that $D(x,y)$ is divisible by $C_f(y,x)$, and its coefficients are coprime in total as elements of $\mathbb{R}[x]$. Hence $C_f(y,x) = const$. Then the degree of $P_f(y)Q_f(x) - P_f(x)Q_f(y)$ in each variable is the same as for $D(x,y)$, i.e. equals m. Contradiction.

26e) From the previous parts we have that the coefficients belong to K. Consider once again our expression as a fraction. For the degree of the numerator the needed was proven, and for the denominator this holds since it is the leading coefficient of the considered expression as a polynomial in y.

26f) Assume that we haven't come to this situation. Then consider an arbitrary iteration and express GCD as $\frac{D(x,y)}{d(x)}$ under agreements from the previous parts of this Problem. Let f be a rational function of the least degree m in the set given by this iteration. By what is proven above, $P_f(y)Q_f(x) - P_f(x)Q_f(y) = C_f(y,x)D(x,y)$, and on the right side there is a product of polynomials. It is clear that the degree $D(x,y)$ in x is not less than m.

First case: the degree in y equals m, so $C_f = C$ is a constant. By definition of GCD polynomial $P_f(y) - f(x)Q_f(y) = \frac{CD(x,y)}{Q_f(x)}$ is divisible by $\frac{D(x,y)}{d(x)}$. Then for some x we have $\frac{D(x,y)}{Q_f(x)}c(x) = \frac{D(x,y)}{d(x)}$. Hence $f(x) \in M$ is a function such that doesn't exist by our assumption. Contradiction.

So on each iteration the degree of $D(x,y)$ in y is lesser than m. From 26e we have that all of the coefficients of $\frac{D(x,y)}{d(x)}$ have degree less than m, i.e. after the iteration the set $M_{(k)}$ contains some new nontrivial rational function with degree less than all functions in $M_{(k-1)}$. But there is a nontrivial rational function in K of the least possible degree, so the number of such iterations is finite, which leads to contradiction.

26g) Polynomial $P_h(y) - h(x)Q_h(y)$ has degree 1 in $h(x)$. Hence, if it is reducible in $\mathbb{R}[h(x), y]$, then one of its multilpiers in a nontrivial reduction is a polynomial in y. Then P_h and Q_h have a common nontrivial divisor. Contradiction.

26h) Assume the contrary. Let $P_g(y)$ be divisible by $P_h(y) - h(x)Q_h(y)$ in $\mathbb{R}(h(x))[y] \subset K[y]$. Since $g(x)Q_g(y)$ is divisible by $P_h(y) - h(x)Q_h(y)$ in $K[y]$, this means that $P_g(y)$ and $Q_g(y)$ have a common nontrivial divisor in $K[y]$. However we know that their GCD can be found by Euclid's algorithm, but in subring $\mathbb{R}(h(x))[y]$ Euclid's algorithm leads to trivial GCD. Contradiction.

26i) Let

$$P_u(y) = (P_h(y) - h(x)Q_h(y))v(h(x)) + \frac{T(h(x), y)}{t(h(y))}$$

and

$$Q_u(y) = (P_h(y) - h(x)Q_h(y))w(h(x)) + \frac{S(h(x), y)}{s(h(y))}.$$

Then

$$P_u(y) - u(x)Q_u(y) = (P_h(y) - h(x)Q_h(y))(v(h(x)) - u(x)w(h(x))) + \frac{T(h(x), y)}{t(h(y))} - u(x)\frac{S(h(x), y)}{s(h(y))}.$$

Difference $P_u(y) - u(x)Q_u(y)$ and difference $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))}$ when divided by $P_h(y) - h(x)Q_h(y)$ give equal remainders over K. Along with this we have that the first polynomial is divisible by $P_h(y) - h(x)Q_h(y)$, so the second polynomial is also divisible by $P_h(y) - h(x)Q_h(y)$ over K. The degree of $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))}$ in y is less than the degree $\deg_y(P_h(y) - h(x)Q_h(y))$ by construction. Hence $\frac{T(h(x),y)}{t(h(y))} - u(x)\frac{S(h(x),y)}{s(h(y))} = 0$.

26j) The polynomials in y from both sides of equality $\frac{T(h(x),y)}{t(h(y))} = u(x)\frac{S(h(x),y)}{s(h(y))}$ don't identically equal 0 (by 26i). Hence $u(x)$ belongs to $\mathbb{R}(h(x))$ as a fraction.

26k) h belongs to K, so $\mathbb{R}(h(x)) \subset K$, and the inverse inclusion was proven in 26j.

$\square$

Solution for Problem 27. Let $\mathbb{R}(h) = \mathbb{R}(h_1)$ for some $h, h_1 \in \mathbb{R}(x)$. Then there exist $f, g \in \mathbb{R}(x)$, for which $f(h) = h_1, g(h_1) = h$. It is sufficient to prove that $\deg f \leq 1$. Express f as an irreducible fraction $f = \frac{f_+}{f_-}, (f_+, f_-) = 1$. If f_- is a constant then f is a polynomial, hence by the second part of the solution for Problem 24 we have that g is also a polynomial. Then

$$\deg h = \deg f(g(h)) = \deg f \deg g \deg h.$$

Hence $\deg f = 1$. The case $g_- \in \mathbb{R}$ is analogous.

From now on we assume $f_-, g_- \notin \mathbb{R}$. By analogy with the solution for Problem 23, express $f(x)$ as a ratio of two polynomials and consider roots of both these polynomials and their leading coefficients. We will have the formula:

$$h_1 = f(g(h_1)) = \frac{C_+}{C_-} \frac{g_-^{n_- - n_+}(g_+ - \alpha_1 g_-)(g_+ - \alpha_2 g_-)\dots(g_+ - \alpha_{n_+} g_-)}{(g_+ - \beta_1 g_-)(g_+ - \beta_2 g_-)\dots(g_+ - \beta_{n_-} g_-)}.$$

All the multipliers in numerator and denominator of the right hand of this formula are coprime.

Assume $n_- = n_+$. Note that constant multiplier can't arise both in numerator and denominator at the same time. Hence $n_- = n_+ = 1$ and then $\deg f = 1$.

Assume $n_- \neq n_+$. Then $h \sim g_-^{n_- - n_+}$ and, in general, $n_- - n_+ = 1$ and $n_- \geq 1$. If $n_+ \neq 0$ then in formula above will be at least two nonconstant and coprime multipliers. Contradiction. Hence $n_- = 1, n_+ = 0, \deg f = 1$. $\square$

Solution for Problem 28. Let there be two fields $K = \mathbb{R}(f) \subset L = \mathbb{R}(g)$. From the task $K \subset L$ we have that there is $H \in \mathbb{R}(x)$: $f = H(g)$.

By Problem 27, all of the generators of field K are expressable as $\frac{a_1 f + b_1}{c_1 f + d_1}, a_1 d_1 - b_1 c_1 \neq 0$ and all of the generators of field L are expressable as $\frac{a_2 g + b_2}{c_2 g + d_2}, a_2 d_2 - b_2 c_2 \neq 0$. Hence we have that transition functions $\widetilde{H}$ (for other generators) are expressable as

$$\frac{a_1 H(\frac{a_2 x + b_2}{c_2 x + d_2}) + b_1}{c_1 H(\frac{a_2 x + b_2}{c_2 x + d_2}) + d_1}.$$

It is sufficient to check that

$$\deg H = \deg(\frac{aH+b}{cH+d}) = \deg(H(\frac{ax+b}{cx+d})), ad-bc \neq 0.$$

Equality $\deg H = \deg(\frac{aH+b}{cH+d}), ad-bc \neq 0$ was checked in Problem 25. So it is sufficient to check that $\deg H = \deg(H(\frac{ax+b}{cx+d})), ad-bc \neq 0$.

Fix $a,b,c,d \in \mathbb{R}$, for which $ad-bc \neq 0$. By analogy with the solution of Problem 23 express $H(x)$ as a ratio of two polynomials and then consider the roots of each of those polynomials and their leading coefficients. We get the formula:

$$H(\frac{ax+b}{cx+d}) = \frac{C_+}{C_-}\frac{(cx+d)^{n_- - n_+}((ax+b)-\alpha_1(cx+d))((ax+b)-\alpha_2(cx+d))\dots((ax+b)-\alpha_{n_+}(cx+d))}{((ax+b)-\beta_1(cx+d))((ax+b)-\beta_2(cx+d))\dots((ax+b)-\beta_{n_-}(cx+d))}.$$

From this formula we have that $\deg H(\frac{ax+b}{cx+d}) \leq \deg H$. Since $H(x) = H(\frac{ay+b}{cy+d})$, where

$$y = \frac{\frac{d}{ad-bc}x + \frac{-c}{ad-bc}}{\frac{-b}{ad-bc}x + \frac{a}{ad-bc}},$$

this formula also leads to $\deg H \leq \deg H(\frac{ax+b}{cx+d})$. Hence we have that

$$\deg H(\frac{ax+b}{cx+d}) = \deg H.$$

$\square$

Solution for Problem 29. The solution is written in the second part of solution for Problem 24. $\square$

Solution for Problem 30. From the condition and LCM-Lemma (Problem 7b) we have that there is a polynomial H, for which $\deg H = \mathrm{LCM}(\deg F, \deg G)$ and $\mathbb{R}(H) \subset \mathbb{R}(F) \cap \mathbb{R}(G)$. Hence we have

$$([\mathbb{R}(F) : \mathbb{R}(H)], [\mathbb{R}(G) : \mathbb{R}(H)]) = 1.$$

It is sufficient to notice that $[\mathbb{R}(F) : \mathbb{R}(F) \cap \mathbb{R}(G)]$ divides $[\mathbb{R}(F) : \mathbb{R}(H)]$ and $[\mathbb{R}(G) : \mathbb{R}(F) \cap \mathbb{R}(G)]$ divides $[\mathbb{R}(G) : \mathbb{R}(H)]$, since $\mathbb{R}(H) \subset \mathbb{R}(F) \cap \mathbb{R}(G)$. $\square$

Solution of Problem 31. a) Assume the contrary: let $\deg_z R(y,z) < \deg f(x)$. Note that $n := \deg_y R(y,z) \geq 1$ (otherwise $R(y,z)$ doesn't depend on y, so $R(-,z) = 0$). Then $R(y,z) = R_0(z) + R_1(z)y + \ldots + R_n(z)z^n$, where $R_i \in \mathbb{R}[x], \deg R_i < \deg f$ for any i. But then $\deg R_n(x)f^n > \deg R_i(x)f^i$ for any i,which leads to $R(f(x),x) \neq 0$. Contradiction.

b) Let us express h as an irreducible fraction $\frac{h_+}{h_-}$. Then, obviously, $T(y,z) = h_-(z)y - h_+(z)$ satisfies $T(h(z),z) = 0$. Let us check that the degree of $T(y,z)$ in z is minimal for such polynomials (this degree equals $\deg H$). Assume that there is a desired polynomial $\widetilde{T}(y,z)$ with lesser degree. Set $d := \deg \widetilde{T}(y,z)$. Then $h_-^d \widetilde{T}(y,z) = Q(y,z)T(y,z) + R(z)$ for some $Q(y,z) \in \mathbb{R}[y,z], R(z) \in \mathbb{R}[z]$. From the definition of $\widetilde{T}$ it follows that $R(x) = 0$, i.e. $R = 0$. Then

$$h_-^d(z)\widetilde{T}(y,z) = Q(y,z)T(y,z).$$

From the Problem 20 it follows that $Q(y,z) = h_-^a(z)\widetilde{Q}(y,z), T(y,z) = h_-^b(z)\widehat{T}(y,z)$ for some $Q(y,z)\widehat{T}(y,z) \in \mathbb{R}[x,y], a,b \in \mathbb{Z}_{\geq 0}, a+b = d$. But then $h_+(x)$ is divisible by $h_-(x)^b$, which is possible only if $b = 0$. Hence $a = d$ and

$$\widetilde{T}(y,z) = \widetilde{Q}(y,z)T(y,z).$$

This contradicts to the assumption that $deg_z T(y,z) > \deg_z \widetilde{T}(y,z)$.

c) Note that $[L : \mathbb{R}(x)] = [L : \mathbb{R}(g(x))] \cdot [\mathbb{R}(g(x)) : \mathbb{R}(x)]$. This allows to consider L as $\mathbb{R}(g(x))$. And for $L = \mathbb{R}(g(x))$ the statement follows from 31b. $\square$

Solution for Problem 32, Proof of GCD-Lemma. Let $\mathbb{R}(F,G)=\mathbb{R}(H)$ and $\deg H < GCD(\deg F, \deg G)$. Then $F=A(H)$, $G=B(H)$ and $\mathbb{R}(A,B)=\mathbb{R}(x)$. Also, according to LCM-Lemma (Problem 7b) there exist polynomials P and Q such that $P(A)=Q(B)$ and $\deg P(A)=LCM(\deg A, \deg B)$.

Let us prove that polynomial $R(y,z)=P(y)-Q(z)$ is minimal by degree for field extension $\mathbb{R}(A,B)$ over field $\mathbb{R}(A)$ in the sense of the previous Problem. Indeed, if there is a polynomial of lesser degree, vanishing under the substitution of A and B, then we should cancel the leading monomial in x of some A^sB^t with the leading monomial of some another A^kB^l. Then $(k-s)\deg A+(l-t)\deg B=0$, and $k-s\neq 0$ is divisible by $\frac{\deg B}{GCD(\deg A, \deg B)}$, i.e. the degree of this polynomial should be at least $\frac{\deg B}{GCD(\deg A, \deg B)} = = \frac{LCM(\deg A, \deg B)}{\deg A} = \deg P$.

But then

$$\deg A = [\mathbb{R}(x):\mathbb{R}(A)] = [\mathbb{R}(A,B):\mathbb{R}(A)] = \frac{GCD(\deg A, \deg B)}{\deg B} = \frac{\deg A}{GCD(\deg A, \deg B)} < \deg A.$$

Contradiction. □

Solution for Problem 33. Follows from Problems 32 and 29. □

Solution for Problem 34. Follows from Problems 27 and 29. □

Solution for Problem 35, Proof of Ritt's First Theorem. We will prove the statement by induction on $\deg F$. For $\deg F=1$ the statement is obvious.

If G_r and H_s have equal degrees, then $G_r=aH_s+b$ and it is sufficient to prove the statement for $G_1\circ\ldots G_{r-1}\circ(ax+b)=H_1\circ\ldots\circ H_{s-1}$, which follows from the inductive hypothesis.

If G_r and H_s have different degrees, then this degrees are coprime, since otherwise (according to Problem 9) they are reducible. Then (by Problem 7b) there exist polynomials C, D_1 and D_2 such that $G_1\circ\ldots G_{r-1} = C\circ D_1$, $H_1\circ\ldots\circ H_{s-1}=C\circ D_2$, $D_1\circ G_r = D_2\circ H_s$, $\deg D_1 = LCM(\deg G_r, \deg H_s)/\deg G_r = \deg H_s$, $\deg D_2 = LCM(\deg G_r, \deg H_s)/\deg H_s = \deg G_r$. Then by inductive hypothesis all the statements of the theorem hold for polynomials $H_1\circ\ldots\circ H_{s-1} = C\circ D_2$ and $G_1\circ\ldots G_{r-1}=C\circ D_1$.

If $C=C_1\circ\ldots\circ C_l$ is a decomposition of C into irreducible polynomials, then for decompositions $C_1\circ\ldots\circ C_l\circ D_1$ and $G_1\circ\ldots G_{r-1}$ Ritt's theorem holds, hence there exists a sequence of intermediate decompositions. It can be modified by adding the polynomial G_r to the end of each decomposition. And then it can be continued by adding analogus intermediate decompositions between $C_1\circ\ldots\circ C_l\circ D_2$ and $H_1\circ\ldots\circ H_{s-1}$. □

Про вписанные окружности

И.Фролов

Проект представляют А.Заславский, П.Кожевников

Часть 1

Задача 1. (*"Леммы о воробьях"*)

(a) На сторонах AB и BC треугольника ABC выбраны точки P и Q соответственно так, что $AP = CQ$. Докажите, что окружность (BPQ) проходит через середину дуги ABC.

(b) На сторонах AB и BC треугольника ABC выбраны точки P и Q соответственно так, что $AP+CQ = AC$. Докажите, что окружность (BPQ) проходит через центр вписанной окружности треугольника ABC.

Задача 2. Вписанная окружность треугольника ABC касается AC в точке D. На стороне AC выбрана точка P.

(a) Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников ABP и CBP проходит через D.

(b) Пусть I_1 и I_2 — центры вписанной окружности треугольников ABP и CBP. Докажите, что точки I_1, I_2, D и P лежат на одной окружности.

Задача 3. Внутри угла ABC взята точка P. Пусть I_1 и I_2 — центры вписанных окружностей треугольников PAB и PBC, а BL_1 и BL_2 — биссектрисы этих треугольников. Докажите, что прямые I_1I_2 и L_1L_2 пересекаются на внешней биссектрисе угла APC или параллельны ей.

Задача 4. Четырехугольник $ABCD$ вписан в окружность. Прямая ℓ — вторая общая касательная к вписанным окружностям треугольников ABC и ABD. Докажите, что $\ell \parallel CD$.

Задача 5. Четырехугольник $ABCD$ вписан в окружность. Точки I_1 и I_2 — центры вписанных окружностей треугольников ABC и ABD. Точки J_1 и J_2 — центры вневписанных окружностей треугольников ACD и BCD, лежащих напротив вершин C и D соответственно. Докажите, что I_1, I_2, J_1, J_2 лежат на одной прямой.

Задача 6. На стороне AD описанного четырехугольника $ABCD$ выбрана точка P. Докажите, что

(a) точка P и центры вписанных окружностей треугольников PAB, PBC, PCD лежат на одной окружности;

(b) вписанные окружности треугольников PAB, PBC, PCD имеют общую касательную.

Часть 2

Задача 7. Внутри описанного четырехугольника $ABCD$ взята точка P. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Докажите, что внешняя биссектриса угла APC проходит через вторую точку пересечения окружностей (PI_1I_2) и (PI_3I_4) или касается их.

Задача 8. Внутри выпуклого четырехугольника $ABCD$ взята точка P, не лежащая на диагоналях. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Оказалось, что прямые I_1I_2 и I_3I_4 пересекаются на внешней биссектрисе угла APC. Докажите, что прямые I_2I_3 и I_1I_4 пересекаются на внешней биссектрисе угла BPD или параллельны ей.

Задача 9. Четырехугольник $ABCD$ описан около окружности ω с центром I. Пусть ω_1 и ω_2 — вписанные окружности треугольников IAB и IBC. Пусть ω_3 — вневписанная окружность треугольника ICD, лежащая напротив вершины C. Докажите, что

(a) окружности ω_1, ω_3 и ω имеют общую касательную;

(b) окружности ω_1, ω_2 и ω_3 имеют общую касательную;

(c) центры ω_1, ω_2, ω_3 и вневписанной окружности треугольника IDA напротив вершины A лежат на одной окружности.

Задача 10. Внутри параллелограмма $ABCD$ взята точка P, такая что $\angle PDA = \angle PBA$. Пусть ω_1 и ω_4 — центры вневписанных окружностей треугольников PAB и PDA, лежащие напротив вершины A. Пусть ω_2 и ω_3 — вписанные окружности треугольников PBC и PCD. Докажите, что

(a) одна из общих касательных к ω_1 и ω_3 параллельна AD;

(b) окружности ω_1, ω_2, ω_3 и ω_4 имеют общую касательную, проходящую через центр параллелограмма;

(c) центры ω_1, ω_2, ω_3 и ω_4 лежат на одной окружности.

Задача 11. У выпуклого четырехугольника $ABCD$ углы A и C равны. Докажите, что одна из общих касательных к вписанным окружностям треугольников ABD и BCD проходит через середину AC.

Задача 12. Пусть I — центр вписанной окружности треугольника ABC. Вписанная окружность треугольника AIC касается стороны AC в точке E. Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников AIB и BIC проходит через E.

Следующая задача дает способ строить окружности Мальфатти в треугольнике.

Задача 13. Точка I — центр вписанной окружности треугольника ABC. В углы A, B, C соответственно вписаны попарно касающиеся окружности ω_a, ω_b, ω_c. Докажите, что общая внутренняя касательная к ω_b и ω_c касается вписанных окружностей треугольников AIB и AIC.

Задача 14. Около треугольника ABC описана окружность Ω. Полувписанная окружность касается Ω в точке P и касается сторон AB и BC. Вписанная окружность треугольника APC касается стороны AC в точке F. Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников APB и BPC проходит через F.

Задача 15. Диагонали описанного четырехугольника $ABCD$ пересекаются в точке P. Докажите, что центры вписанных окружностей треугольников PAB, PBC, PCD и PDA лежат на одной окружности.

Задача 16. Четырехугольник $ABCD$ вписан в окружность с центром O и описан около окружности. Докажите, что центры вписанных окружностей треугольников OAB, OBC, OCD и ODA лежат на одной окружности.

Про вписанные окружности

Часть 3

Задача 17. Четырехугольник $ABCD$ описан около окружности с центром I. Внутри него взята точка P. Пусть PL и PK — биссектрисы треугольников PAC и PBD. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Тогда следующие четыре утверждения эквивалентны:

(1) Точки L, K и I лежат на одной прямой.

(2) Прямые I_1I_2 и I_3I_4 пересекаются на внешней биссектрисе угла APC.

(3) Точки I_1, I_2, I_3, I_4 лежат на одной окружности.

(4) Образы точек A, B, C, D при инверсии с центром P являются вершинами описанного четырехугольника.

Задача 18. Четырехугольник $ABCD$ описан около окружности ω. Точка P такова, что $ABCP$ — выпуклый четырехугольник, содержащий точку D, и $\angle APD = \angle BPC$. Пусть ω_1, ω_2, ω_3, ω_4 — вписанные окружности треугольников PAB, PBC, PCD, PDA, а I_1, I_2, I_3, I_4 — их центры, соответственно. Тогда

(a) Окружности ω_1, ω_3 и ω имеют общую касательную (а также ω_2, ω_4 и ω имеют общую касательную).

(b) Окружности ω_1, ω_2, ω_3, ω_4 имеют общую касательную.

(c) Точки I_1, I_2, I_3, I_4 лежат на одной окружности с центром на прямой PI.

(d) Точка Микеля четырехугольника $I_1I_2I_3I_4$ совпадает с P.

Часть 4

Задача 19. Пусть чевианы AA_1, BB_1, CC_1 треугольника ABC пересекаются в точке P. Докажите, что в следующих случаях центры вписанных окружностей треугольников APB_1, APC_1, BPC_1, BPA_1, CPA_1, CPB_1 лежат на одной конике:

(a) если P — центр вписанной окружности треугольника ABC;

(b) если P — точка Торричелли треугольника ABC.

Про вписанные окружности

И.Фролов

Проект представляют А.Заславский, П.Кожевников

Решения

Часть 1

Задача 1. (*"Леммы о воробьях"*)

(a) На сторонах AB и BC треугольника ABC выбраны точки P и Q соответственно так, что $AP = CQ$. Докажите, что окружность (BPQ) проходит через середину W дуги ABC.

(b) На сторонах AB и BC треугольника ABC выбраны точки P и Q соответственно так, что $AP+CQ = AC$. Докажите, что окружность (BPQ) проходит через центр вписанной окружности треугольника ABC.

Доказательство. (a) Треугольники APW и CQW равны, поскольку $\angle PAW = \angle QCW$ и $AW = CW$. Следовательно, $\angle BPW = \angle BQW$, откуда следует искомое утверждение.

(b) Пусть C_1 и A_1 — точки касания вписанной окружности со сторонами AB, BC соответственно. Так как $AC_1 + CA_1 = AC$, то $C_1P = A_1Q$. Значит, треугольники C_1PI и A_1QI равны, т.е $\angle PIQ = \angle A_1IC_1 = 180° - \angle PBQ$. □

Задача 2. Вписанная окружность треугольника ABC касается AC в точке D. На стороне AC выбрана точка P.

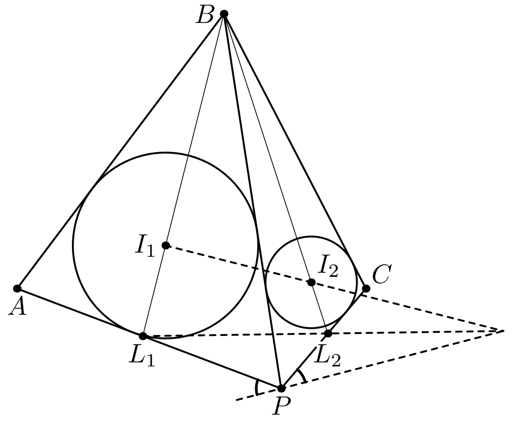
(a) Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников ABP и CBP проходит через D.

(b) Пусть I_1 и I_2 — центры вписанных окружностей треугольников ABP и CBP. Докажите, что точки I_1, I_2, D и P лежат на одной окружности.

Доказательство. (a) Пусть вторая общая внутренняя касательная пересекает AC и BP в точках D' и X соответственно. Тогда $D'A - AB = D'X - XB = D'C - CB$. Легко видеть, что D — единственная точка на AC, удовлетворяющая равенству $DA - AB = DC - CB$, значит, $D = D'$.

(b) Очевидно, что $\angle I_1PI_2 = 90°$, а из п. (a) получаем, что $\angle I_1DI_2 = 90°$. □

Задача 3. Внутри угла ABC взята точка P. Пусть I_1 и I_2 — центры вписанных окружностей треугольников PAB и PBC, а BL_1 и BL_2 — биссектрисы этих треугольников. Докажите, что прямые I_1I_2 и L_1L_2 пересекаются на внешней биссектрисе угла APC или параллельны ей.



Доказательство. Пусть внешняя биссектриса угла APC пересекает L_1L_2 в точке T. По свойству биссектрисы

$$\frac{BI_1}{I_1L_1} = \frac{BP}{PL_1}, \qquad \frac{BI_2}{I_2L_2} = \frac{BP}{PL_2}, \qquad \frac{L_1T}{TL_2} = \frac{PL_1}{PL_2}$$

Применяя к треугольнику BL_1L_2 теорему Менелая, получаем утверждение задачи. □

Задача 4. Четырехугольник $ABCD$ вписан в окружность. Прямая ℓ — вторая общая касательная к вписанным окружностям треугольников ABC и ABD. Докажите, что $\ell \parallel CD$.

Доказательство. Пусть I_1 и I_2 — центры вписанных окружностей треугольников ABC и ABD. Прямые CI_1 и DI_2 пересекаются в середине M дуги AB описанной окружности. Пусть N — середина дуги CD. Так как $MI_1 = MI_2$, то $I_1I_2 \perp MN$. Поэтому $\angle(AB, MN) = \angle(MN, \ell)$. Легко видеть, что $\angle(AB, MN) = \angle(MN, CD)$, значит, $\ell \parallel CD$. □

Задача 5. Четырехугольник $ABCD$ вписан в окружность. Точки I_1 и I_2 — центры вписанных окружностей треугольников ABC и ABD. Точки J_1 и J_2 — центры вневписанных окружностей треугольников ACD и BCD, лежащих напротив вершин C и D соответственно. Докажите, что I_1, I_2, J_1, J_2 лежат на одной прямой.

Доказательство. Как показано в решении предыдущей задачи, $I_1I_2 \perp MN$, где M и N — середины дуг AB и CD описанной окнружности. Пусть K и L середины дуг AD и BC. Известно, что $MN \perp KL$. Поскольку $KJ_1 = KA = KI_2$ и KL — внешняя биссектриса угла J_1KI_2, получаем, что $J_1I_2 \parallel KL$. Следовательно, J_1 лежит на I_1I_2, для J_2 доказательство аналогично. □

Задача 6. На стороне AD описанного четырехугольника $ABCD$ выбрана точка P. Докажите, что

(a) точка P и центры вписанных окружностей треугольников PAB, PBC, PCD лежат на одной окружности;

(b) вписанные окружности треугольников PAB, PBC, PCD имеют общую касательную.

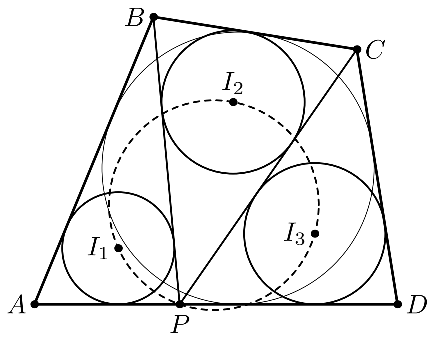


Схема первого доказательства. (a) Пусть I — центр окружности, вписанной в четырехугольник $ABCD$. Так как $\angle BIC + \angle I_1II_3 = 180^\circ$, у точки I есть изогонально сопряженная относительно четырехугоьника BCI_3I_1. Она совпадает с I_2, потому что $\angle CBI = \angle I_1BI_2$ и $\angle BCI = \angle I_3CI_2$. Значит, $\angle BI_2C + \angle I_1I_2I_3 = 180^\circ$ и подсчетом углов получаем искомое утверждение.

(b) Пусть m — прямая, симметричная BP относительно I_1I_2 (т.е. вторая общая внутренняя касательная к ω_1 и ω_2), а прямая n симметрична CP относительно I_2I_3. Используя п. (a), подсчетом углов получаем, что $m \parallel n$, следовательно, m и n совпадают. □

Схема второго доказательства. (b) Пусть ℓ — вторая общая касательная к ω_1 и ω_3. Обозначим точки пересечения ℓ с BP и CP через K и L, точки пересечения ω_1 с AB, BP, AD, ℓ через X_1, X_2, X_3, X_4, а точки пересечения ω_3 с CD, CP, AD, ℓ через Y_1, Y_2, Y_3, Y_4 соответственно. Тогда

$$0 = AB + CD - AD - BC = X_1B + CY_1 - X_3Y_3 - BC = X_2B + CY_2 - X_4Y_4 - BC = KB + CL - KL - BC$$

Следовательно, четырехугольник $BCLK$ — описанный.

(a) Выводится из п. (b) счетом углов. □

Про вписанные окружности

Решения

Часть 2

Задача 7. Внутри описанного четырехугольника $ABCD$ взята точка P. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Докажите, что внешняя биссектриса угла APC проходит через вторую точку пересечения окружностей (PI_1I_2) и (PI_3I_4) или касается их.

Схема доказательства. Применим несколько раз задачу 1. □

Задача 8. Внутри выпуклого четырехугольника $ABCD$ взята точка P, не лежащая на диагоналях. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Оказалось, что прямые I_1I_2 и I_3I_4 пересекаются на внешней биссектрисе угла APC. Докажите, что прямые I_2I_3 и I_1I_4 пересекаются на внешней биссектрисе угла BPD или параллельны ей.

Схема доказательства. Сделав инверсию с центром P, применим утверждение предыдущей задачи и обратное к нему. □

Задача 9. Четырехугольник $ABCD$ описан около окружности ω с центром I. Пусть ω_1 и ω_2 — вписанные окружности треугольников IAB и IBC. Пусть ω_3 — вневписанная окружность треугольника ICD, лежащая напротив вершины C. Докажите, что

(a) окружности ω_1, ω_3 и ω имеют общую касательную;

(b) окружности ω_1, ω_2 и ω_3 имеют общую касательную;

(c) центры ω_1, ω_2, ω_3 и вневписанной окружности треугольника IDA напротив вершины A лежат на одной окружности.

Доказательство. Обозначим центр окружности ω_k через I_k.

(a) Общая касательная ω и ω_1 симметрична прямой AB относительно II_1, а общая касательная ω и ω_3 симметрична прямой CD относительно II_3. Легко видеть, что $\angle I_1II_3 = \angle AID$. Поскольку прямые AB и CD симметричны AD относительно IA, ID соответственно, они также симметричны относительно II_1, II_3 прямой, полученной из AD поворотом вокруг I на удвоенный угол AII_1. Эта прямая и будет общей кастельной трех окружностей.

(b) Обозначим длины касательных к ω из A, B, C, D через a, b, c, d соответственно. Тогда длина общей внешней касательной к ω и ω_1 равна $b-(a+b+BI-AI)/2$, длина общей внешней касательной к ω и ω_3 равна $(c+d+CI+DI)/2-c$, а общей внешней касательной к ω_1 и ω_3 — разности этих отрезков (из пункта (a)). Посчитав аналогично длины общих внутренних касательных к ω_1 и ω_2, ω_2 и ω_3, убедимся, что один из полученных отрезков равен сумме двух других. Известно, что отсюда следует существование искомой общей касательной.

(c) Общая касательная к ω_1, ω_2 и ω_3 симметрична прямым IB, IC относительно I_1I_2 и I_2I_3 соответственно. Отсюда находим угол $I_1I_2I_3$. Аналогично находим угол $I_1I_4I_3$, где I_4 — центр четвертой окружности, и убеждаемся, что четыре центра лежат на одной окружности. □

Задача 10. Внутри параллелограмма $ABCD$ взята точка P, такая что $\angle PDA = \angle PBA$. Пусть ω_1 и ω_4 — центры вневписанных окружностей треугольников PAB и PDA, лежащие напротив вершины A. Пусть ω_2 и ω_3 — вписанные окружности треугольников PBC и PCD. Докажите, что

(a) одна из общих касательных к ω_1 и ω_3 параллельна AD;

(b) окружности ω_1, ω_2, ω_3 и ω_4 имеют общую касательную, проходящую через центр параллелограмма;

(c) центры ω_1, ω_2, ω_3 и ω_4 лежат на одной окружности.

Схема доказательства. Из условия следует, что радиусы окружностей (PAD) и (PAB) равны. Тогда окружности (PBC) и (PCD) имеют такие же радиусы.

(a) После параллельного переноса на вектор $\overrightarrow{PQ} = \overrightarrow{AD}$ задача превращается в такую: Дан произвольный вписанный четырехугольник $CPDQ$. Тогда одна из общих касательных к окружности, вписанной в треугольник PCD и вневписанной для треугольника CDQ напротив вершины D, параллельна PQ.

Последнее аналогично Задаче 4.

Подробнее см. Турнир городов, осень 2021, сложный тур, 10-11.5.

(b) Равносильно следующей задаче.

(c) Выводится из пункта (b) аналогично пункту (c) предыдущей задачи. □

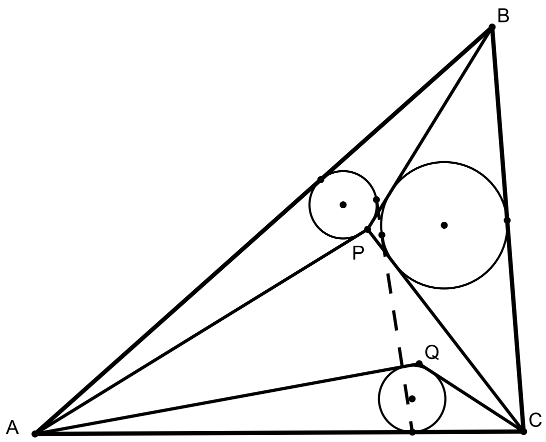
Задача 11. У выпуклого четырехугольника $ABCD$ углы A и C равны. Докажите, что одна из общих касательных к вписанным окружностям треугольников ABD и BCD проходит через середину AC.

Доказательство. См. задачу 10.4 XVIII олимпиады им, Шарыгина, 2022. □

Задача 12. Пусть I — центр вписанной окружности треугольника ABC. Вписанная окружность треугольника AIC касается стороны AC в точке E. Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников AIB и BIC проходит через E.

Схема доказательства. Пусть D — точка касания вписанной окружности треугольника ABC со стороной AC и пусть ℓ — вторая внутренняя касательная к вписанным окружностям треугольников AIB и BIC. Применим Задачу 9(b) к (вырожденному) описанному четырехугольнику $ABCD$. Получим, что ℓ касается вневписанных окружностей треугольников AID и CID, лежащих напротив вершин A и C соответственно. Остается применить аналог Задачи 2(a) для вневписанных окружностей к треугольнику AIC и точке D на стороне AC. □

Примечание. Как показал Г.Галяпин утверждение задачи допускает следующее обобщение. Если точки P и Q изогонально сопряжены относительно треугольника ABC, то общая внутренняя касательная к вписанным окружностям треугольников APB и BPC, отличная от прямой PB, проходит через точку касания стороны AC с вписанной окружностью треугольника AQC.



Следующая задача дает способ строить окружности Мальфатти в треугольнике.

Задача 13. Точка I — центр вписанной окружности треугольника ABC. В углы A, B, C соответственно вписаны попарно касающиеся окружности ω_a, ω_b, ω_c. Докажите, что общая внутренняя касательная к ω_b и ω_c касается вписанных окружностей треугольников AIB и AIC.

Доказательство. Обозначим через a, b, c общие внутренние касательные к вписанным окружностям треугольников IAC и IAB, IAB и IBC, IBC и IAC, отличные от биссектрис ABC, а через A', B', C' — точки касания окружностей, вписанных в треугольники IBC, IAC, IAB с соответствующими сторонами ABC.

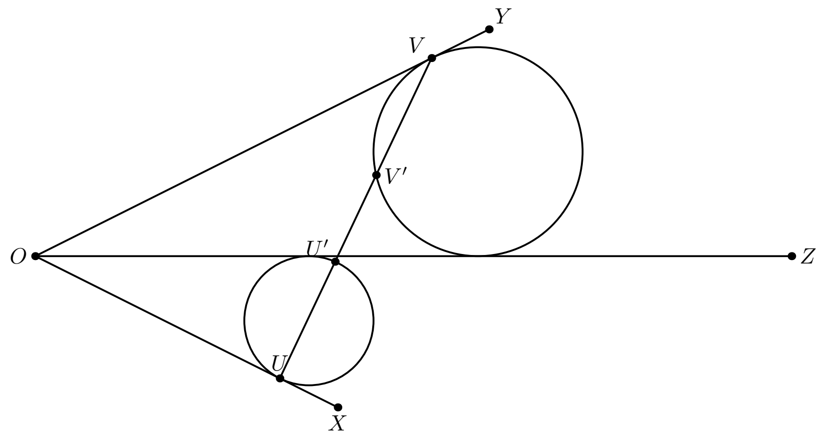
Лемма 1. Даны три окружности, каждая из которых лежит вне двух других. К каждой паре окружностей проведена одна из общих внутренних касательных. Оказалось, что три эти прямые пересекаются в одной точке. Тогда три другие общие внутренние касательные также пересекаются в одной точке.

Указание. Точки пересечения троек касательных изогонально сопряжены относительно треугольника, образованного центрами окружностей.

Согласно лемме 1, прямые a, b, c пересекаются в одной точке X.

Напомним довольно известный факт (его переформулировкой является задача M1918.).

Лемма 2. Пусть OZ — биссектриса угла XOY. Окружность ω_1, вписанная в угол XOZ, касается прямой OX в точке U, а окружность ω_2, вписанная в угол YOZ, касается прямой OY м точке V. Тогда касательная, проведенная из U к ω_2, равна касательной, проведенной из V к ω_1.



Теперь нетрудно показать, что каждый из четырехугольников $XA'CB'$, $XB'AC'$, $XC'BA'$ является описанным. Действительно, разность длин, например, отрезков XA' и XB' равна разности длин касательных к окружности, вписанной в треугольник IAB, проведенных из A' и B'. Поскольку эти касательные равны касательным, проведенным из C' к окружностям, вписанным в треугольники IBC и IAC, их разность есть просто длина общей внутренней касательной к этим окружностям, которая, очевидно, равна $CA' - CB'$.

Осталось показать, что вписанные в эти четырехугольники окружности касаются друг друга. Заметим, что окружность, вписанная в треугольник IAB вписана в треугольник, образованный прямыми a, b и AB, а каждая из окружностей, вписанных в четырехугольники $XB'AC'$ и $XC'BA'$ касается двух сторон этого треугольника и прямой XC', разрезающей его на два треугольника. Найдя отрезки касательных к этим окружностям из вершины C', убеждаемся, что они равны. □

Задача 14. Около треугольника ABC описана окружность Ω. Полувписанная окружность касается Ω в точке P и касается сторон AB и BC. Вписанная окружность треугольника APC касается стороны AC в точке F. Докажите, что вторая общая внутренняя касательная к вписанным окружностям треугольников APB и BPC проходит через F.

Доказательство. Воспользуемся сформулированным выше обобщением задачи 12. Точка P изогонально сопряжена бесконечно удаленной точке нагелианы из вершины B. Поэтому общая касательная к окружностям, вписанным в треугольники APB и BPC, проходит через точку касания AC с окружностью β, касающейся прямых a и c, параллельных нагелиане и проходящих через A и C соответсвенно. Очевидно, что биссектрисы углов между прямыми a и AP, c и CP проходят через I. Но биссектриса угла APC также проходит через I, следовательно, точки касания β и окружности, вписанной в треугольник APC, с AC совпадают. □

Задача 15. Диагонали описанного четырехугольника $ABCD$ пересекаются в точке P. Докажите, что центры вписанных окружностей треугольников PAB, PBC, PCD и PDA лежат на одной окружности.

Доказательство. Известно, что вписанные окружности треугольников ABC и ADC касаются в некоторой точке E. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. По Задаче 2(b) прямая PE — радикальная ось окружностей (PI_1I_2) и (PI_3I_4). (Это утверждение — вырожденный случай задачи 7).

Пусть J_1 и J_2 — центры вписанных окружностей треугольников ABD и CBD. По теореме Дезарга для треугольников AI_1J_1 и CI_2J_2 прямые AC, J_1J_2 и I_1I_2 пересекаются в одной точке T или параллельны. Аналогично, прямая I_3I_4 проходит через T, откуда $TI_1 \cdot TI_2 = TP \cdot TE = TI_3 \cdot TI_4$ (в случае параллельности $I_1I_2I_3I_4$ будет равнобокой трапецией).

Другое решение можно найти в «Решение задачи 1524»// Квант. 1996. N 3. □

Задача 16. Четырехугольник $ABCD$ вписан в окружность с центром O и описан около окружности. Докажите, что центры вписанных окружностей треугольников OAB, OBC, OCD и ODA лежат на одной окружности.

Доказательство. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников OAB, OBC, OCD, ODA соответственно; а J_1, J_2, J_3, J_4 — центры вневписанных окружностей этих же треугольников, лежащие напротив вершины O. Заметим, что инверсия относительно описанной окружности Ω переводит I_k в J_k.

По Задаче 7 внешняя биссектриса ℓ угла AOC проходит через вторую точку пересечения окружностей (OI_1I_2) и (OI_3I_4). Аналогично, ℓ проходит через вторую точку пересечения окружностей (OJ_1J_2) и (OJ_3J_4). Сделав инверсию относительно Ω, получим, что прямые I_1I_2 и I_3I_4 пересекаются в некоторой точке T на ℓ, или параллельны ей, откуда $TI_1 \cdot TI_2 = TP \cdot TE = TI_3 \cdot TI_4$ (в случае параллельности $I_1I_2I_3I_4$ будет равнобокой трапецией).

Другое решение можно найти в *Заславский А.* «О вписанно-описанных четырёхугольниках, моделях геометрии Лобачевского и «лемме Нилова»» // Математическое просвещение. Сер. 3. Вып. 25. М.: МЦНМО. 2020. С. 163–166. □

Часть 3

Задача 17. Четырехугольник $ABCD$ описан около окружности с центром I. Внутри него взята точка P. Пусть PL и PK — биссектрисы треугольников PAC и PBD. Пусть I_1, I_2, I_3, I_4 — центры вписанных окружностей треугольников PAB, PBC, PCD, PDA соответственно. Тогда следующие четыре утверждения эквивалентны:

(1) Точки L, K и I лежат на одной прямой.

(2) Прямые I_1I_2 и I_3I_4 пересекаются на внешней биссектрисе угла APC.

(3) Точки I_1, I_2, I_3, I_4 лежат на одной окружности.

(4) Образы точек A, B, C, D при инверсии с центром P являются вершинами описанного четырехугольника.

Доказательство. Равносильность утверждений (2) и (3) следует из задачи 8.

Равносильность утверждений (2) и (4) следует из аналога задачи 7 для центров вневписанных окружностей напротив вершины P.

Докажем равносильность утверждений (1) и (4). Легко видеть, что (4) равносильно равенству

$$\frac{AB}{AP \cdot BP} + \frac{CD}{CP \cdot DP} = \frac{BC}{BP \cdot CP} + \frac{AD}{DP \cdot DP} \qquad (*)$$

Точка L делит отрезок AC в отношении PA/PC, а точка K делит отрезок BD в отношении PB/PD. Будем обозначать ориентированную площадь треугольника XYZ через S_{XYZ}. Из линейности ориентированной площади получаем

$$S_{KIL} = \frac{PC \cdot S_{KIA} + PA \cdot S_{KIC}}{PA + PC} =$$

$$= \frac{PC \cdot PD \cdot S_{BIA} + PC \cdot PB \cdot S_{DIA} + PA \cdot PD \cdot S_{BIC} + PA \cdot PB \cdot S_{DIC}}{(PA + PC)(PB + PD)} =$$

$$= \pm\frac{r}{2} \cdot \frac{PC \cdot PD \cdot AB - PC \cdot PB \cdot DA - PA \cdot PD \cdot BC + PA \cdot PB \cdot CD}{(PA + PC)(PB + PD)}$$

(где r — радиус вписанной окружности), поскольку треугольники BIA и DIC ориентированы в одну сторону, а треугольники DIA и BIC — в другую. Получаем, что равенство $S_{KIL} = 0$ равносильно равенству $(*)$. Остается заметить, что равенство $S_{KIL} = 0$ равносильно утверждению (1) задачи. □

Задача 18. Четырехугольник $ABCD$ описан около окружности ω. Точка P такова, что $ABCP$ — выпуклый четырехугольник, содержащий точку D, и $\angle APD = \angle BPC$. Пусть ω_1, ω_2, ω_3, ω_4 — вписанные окружности треугольников PAB, PBC, PCD, PDA, а I_1, I_2, I_3, I_4 — их центры, соответственно. Тогда

(a) Окружности ω_1, ω_3 и ω имеют общую касательную (а также ω_2, ω_4 и ω имеют общую касательную).

(b) Окружности ω_1, ω_2, ω_3, ω_4 имеют общую касательную.

(c) Точки I_1, I_2, I_3, I_4 лежат на одной окружности с центром на прямой PI.

(d) Точка Микеля четырехугольника $I_1I_2I_3I_4$ совпадает с P.

Доказательство. (Схема решения)

(c), (d).

Заметим, что PI — общая биссектриса углов APC и BPD. (Доказать это можно, например, из свойств изогонального сопряжения: I изогональна самой себе отосительно $ABCD$, поэтому I изогональна самой себе относительно угла APC, где P — на кубике фокусов $ABCD$. Другое доказательство можно получить из двойственной ТДИ: отражение относильно биссектрисы углоа APC и BPD задает проективную инволюцию $\Pi(P) \to \Pi(P)$. Эта инволюция должна менять местами касательные из P к окружности ω, откуда сразу следует требуемое: биссектриса PI угла между касательными совпадает с биссектриой биссектриса углоа APC и BPD.)

Видим, что для P выполнено условие, аналогичное 17 (1). Из него (аналогично задаче 17, условие (24) можно получить, что I_1, I_2, I_3, I_4 — на одной окружности.

Можно получить (аналогично задаче 17, условие (2)), что точки X, Y пересечения продолжений противоположных сторон вписанного четырехугольника $I_1I_2I_3I_4$ лежат на внешней биссектрисе угла APC. На этой биссектрисе, помимо X и Y есть только одна точка, из которой AB и DC видны под равными (ориентированными) — это точка Микеля вписанного четырехугольника $I_1I_2I_3I_4$. (Этот факт можно вывести и по-другому: доказать равенство $PI_1 \cdot PI_3 = PI_2 \cdot PI_4$, и вместе с ним тот факт, что PI_1I_4 и PI_2I_3 совмещаются поворотной гомотетией, центр которой — точка Микеля.)

Так как для вписанного четырехугольника точка Микеля — проекция центра описанной окружности на XY, то этот центр лежит на перпендикуляре к XY, проходящем через P, т.е. на биссектрисе угла PAC.

(b)

Можно показать, что прямая Обера m четырехугольника $I_1I_2I_3I_4$ — нужная нам общая касательная к окружностям ω_i. Идея — рассмотреть четыре окружности ω_i' с центрами I_i, касающиеся m. Далее отражая m относительно прямых I_1I_2, I_2I_3, I_3I_4, I_4I_1, получим прямые a, b, c, d — общие касательные к парам окружностей I_4 и I_1, I_1 и I_2, I_2 и I_3, I_3 и I_4 соответственно. При этом все 4 прямые a, b, c, d проходят через P (так как отражение точки Микеля относительно сторон попадает на прямую Обера), а из-за вписанности $I_1I_2I_3I_4$ углы $\angle(a,c)$ и $\angle(b,d)$ имеют общую биссектрису. Несложно понять, что полученные условия фиксируют четверку окружностей ω_i' однозначно. поэтому каждая из ω_i' совпадает с ω_i, что завершает решение.

(Другой подход состоит в следующем: отразив общую касательную PB окружностей ω_3 и ω_4 относительно линии центров I_3I_4, получим другую общую касательную t окружностей ω_3 и ω_4. Аналогично строим общую касательную s окружностей ω_1 и ω_2. Теперь параллельность $t \parallel s$ нетрудно получить из счета углов — так как P — точка Микеля, мы знаем, что угол между I_3I_4 и I_1I_2 равен углу поворотной гомотетии $PI_1I_2 \sim PI_4I_3$, т.е половине угла BPD. Далее можно понять, что на самом деле t и s совпадают, найдя хотя бы одну общую точку этих прямых.)

(a) (Г. Галяпин).

Общея касательная m из пункта (b) получается отражением PA относительно I_1I_4, или отражением PB относительно I_2I_4. Отсюда находится $\angle I_4I_1I_2 = (\pi - \angle ADC)/2 = \pi - \angle AI_1B$. Полученное равенство означает, что точка I_1 имеет изогонально сопряженную точку относительно четырехугольника AI_4I_2B. Простой счет углов показывает, что AI_1 и AI — изогонали в угле I_4AB, а BI_1 и BI — изогонали в угле I_2BA. Значит, эта изогонально сопряженная точка — I. Отсюда пониаем, что $\angle I_4II_2 = \pi - \angle AIB = \angle DIC$. Далее счет углов показывает, что отражение общей касатльной AD окружностей ω и ω_4 относительно линии центров I_4I параллельно отражению общей касатльной BC окружностей ω и ω_2 относительно линии центров I_2I, т.е. это будет одна и та же касательная к ω, которая также касается ω_2 и ω_4.

$\square$

Часть 4

Задача 19. Пусть чевианы AA_1, BB_1, CC_1 треугольника ABC пересекаются в точке P. Докажите, что в следующих случаях центры вписанных окружностей треугольников APB_1, APC_1, BPC_1, BPA_1, CPA_1, CPB_1 лежат на одной конике:

(a) если P — центр вписанной окружности треугольника ABC;

(b) если P — точка Торричелли треугольника ABC.

Доказательство. Обозначим центры вписанных окружностей $w_1, \ldots, w_6$ треугольников APC_1, BPC_1, BPA_1, CPA_1, CPB_1, APB_1 через $I_1, \ldots, I_6$ соответственно,

(a) (Г.Галяпин) Обозначим основания биссектрис $L_1 = II_1 \cap AB$, $L_2 = II_2 \cap AB$, $L_3 = II_3 \cap BC$, $L_4 = II_4 \cap BC$, $L_5 = II_5 \cap CA$, $L_6 = II_6 \cap CA$.

Лемма 1. BI_1 и BI_4 изогональны в угле ABC.

Доказательство. Пусть окружность w_1' симметрична w_1 относительно биссектрисы BI. Тогда центры гомотетии с отрицательным коэффициентом для w_1 и w_4 — это I, для w_1 и w_1' — лежит на BI, поэтому центр гомотетии с положительным коэффициентом для w_1' и w_4 лежит на BI, а так как BC — общая касательная w_1' и w_4, то этот центр гомотетии — это B. Видим, что окружности w_1 и w_4 видны из B под равными углами. Отсюда следует утверждение леммы. $\square$

Лемма 2. $L_1, \ldots, L_6$ — на одной конике.

Доказательство. По теореме Паскаля, примененной к $L_1L_6L_3L_4L_5L_2$, достаточно понять , что $L_1L_6 \cap L_4L_5 \in BI$. Это можно доказать, применив свойство биссектрисы и теорему Менелая для треугольников ABB_1 и CBB_1 с секущими L_1L_6 и L_4L_5 соответственно. $\square$

Согласно ТДИ, пучок коник $< L_2L_3L_5L_6 >$ задает проективную инволюцию f на прямой L_1L_4. Взяв в этом пучке конику из леммы 2 и вырожденную конику $L_2L_5 \cap L_3L_6$, видим, что f меняет местами L_1 и L_4, и $f(I) = I$. Симметрия относительно биссектрисы BI задает проективную инволюцию на пучке прямых $\Pi(B)$, которая, в свою очередь, задает проективную инволюцию g на прямой L_1L_4. Видим, что $g(I) = I$ и g меняет местами L_1 и L_4, а также, согласно лемме 1, g меняет местами I_1 и I_4. Тогда $f = g$ (совпадают образы в трех точках), а равенство $g(I_1) = I_4$ будет означать, что $L_2, L_3, L_5, L_6, I_1, I_4$ — на одной конике.

Далее берем пучок $< L_3L_6I_1I_4 >$ и прямую L_2L_5. Проводим, аналогичные рассуждения, используя конику $L_2, L_3, L_5, L_6, I_1, I_4$, и понимаем, что $L_3, L_6, I_1, I_4, I_2, I_5$ — на одной конике.

Наконец берем пучок $< I_2I_5I_1I_4 >$ и прямую L_3L_6. Проводим, аналогичные рассуждения, используя конику $L_3, L_6, I_1, I_4, I_2, I_5$, и понимаем, что $I_1, I_4, I_2, I_5, I_3, I_6$ — на одной конике.

Другое решение можно найти в *Толовиков М.* «Геометрическое доказательство теоремы об инцентрах и её аналогов», Математическое просвещение, выпуск 29, 2022 год, с. 171-182.

(b) Пусть J_a, J_b, J_c — центры вписанных окружностей треугольников BPC, CPA, APB, они лежат на AA_1, BB_1, CC_1 соответственно. По Задаче 3 прямые I_2I_3, J_bJ_c and I_4I_1 пересекаются в некоторой точке X_a. Кроме того, $\frac{J_bX_a}{X_aJ_c} = \frac{J_bP}{PJ_c}$. Определим точки X_b и X_c аналогично. По теореме Менелая для треугольника $J_aJ_bJ_c$ точки X_a, X_b, X_c лежат на одной прямой. Задачи теперь следует из теоремы Паскаля для шестиугольника $I_2I_3I_6I_1I_4I_5$. $\square$

On incircles

I.Frolov
Presented by P.Kozhevnikov, A.Zaslavsky

Part 1

Problem 1. (a) Let P and Q be points on the sides AB and BC of a triangle ABC such that $AP = CQ$. Prove that the circle (BPQ) passes through the midpoint of the arc ABC.

(b) Points P and Q are chosen on the sides AB and BC of a triangle ABC such that $AP + CQ = AC$. Prove that the circle (BPQ) passes through the incenter of the triangle ABC.

Problem 2. The incircle of a triangle ABC is tangent to the side AC at D. Let P be a point on the side AC.

(a) Prove that one of the common internal tangent lines to the incircles of the triangles ABP and CBP passes through D.

(b) Let I_1 and I_2 be the incenters of the triangles ABP and CBP. Prove that the points I_1, I_2, D and P are concyclic.

Problem 3. Let P be a point inside an angle ABC. Let I_1 and I_2 be the incenters of the triangles PAB and PBC, and let BL_1 and BL_2 be the angles bisectors of these triangles (L_1 lies on PA and L_2 lies on PC). Prove that the lines I_1I_2, L_1L_2 and the external bisector of the angle APC are concurrent.

Problem 4. Let $ABCD$ be a cyclic quadrilateral and let ℓ be the second common external tangent line to the incircles of the triangles ABC and ABD. Prove that $\ell \parallel CD$.

Problem 5. Let $ABCD$ be a cyclic quadrilateral and let I_1 and I_2 be the incenters of the triangles ABC and ABD. Let J_1 be the C-excenter of the triangle ACD and let J_2 be the D-excenter of the triangle BCD. Prove that the points I_1, I_2, J_1, J_2 are collinear.

Problem 6. Let P be a point on the side AD of a circumscribed quadrilateral $ABCD$. Prove that

(a) the point P and the incenters of the triangles PAB, PBC, PCD are concyclic;

(b) the incircles of the triangles PAB, PBC, PCD have a common tangent line.

Part 2

Problem 7. Let P be a point inside a circumscribed quadrilateral $ABCD$. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Prove that the external bisector of the angle APC passes through the second intersection point of the circles (PI_1I_2) and (PI_3I_4).

Problem 8. Let P be a point inside a convex quadrilateral $ABCD$, which does not lie on AC and BD. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Suppose that the lines I_1I_2, I_3I_4 and the external bisector of the angle APC are concurrent. Prove that the lines I_2I_3, I_1I_4 and the external bisector of the angle BPD are concurrent.

Problem 9. Let $ABCD$ be a circumscribed quadrilateral with incircle ω and incenter I. Let ω_1 and ω_2 be the incircles of the triangles IAB and IBC. Let ω_3 be the C-excircle of the triangle ICD. Prove that

(a) the circles ω_1, ω_3 and ω have a common tangent line;

(b) the circles ω_1, ω_2 and ω_3 have a common tangent line;

(c) the centers of ω_1, ω_2, ω_3 and the A-excenter of the triangle IDA are concyclic.

Problem 10. Let P be a point inside a parallelogram $ABCD$ such that $\angle PDA = \angle PBA$. Let ω_1 and ω_4 be the A-excircles of the triangles PAB and PDA. Let ω_2 and ω_3 be the incircles of the triangles PBC and PCD. Prove that

(a) one of the common tangent lines to ω_1 and ω_3 is parallel to AD;

(b) the circles ω_1, ω_2, ω_3, ω_4 have a common tangent line which passes through the center of the parallelogram;

(c) the centers of the circles ω_1, ω_2, ω_3, ω_4 are concyclic.

Problem 11. Let $ABCD$ be a convex quadrilateral with $\angle A = \angle C$. Prove that one of the common tangent lines to the incircles of the triangles ABD and BCD passes through the midpoint of AC.

Problem 12. Let I be the incenter of a trianlge ABC. The incircle of the triangle AIC is tangent to AC at E. Prove that the second common internal tangent line to the incircles of the triangles AIB and BIC passes through E.

The next problem provides a way to construct the Malfatti circles in a triangle.

Problem 13. Let I be the incenter of a trianlge ABC. Let ω_a, ω_b, ω_c be pairwise tangent circles, inscribed in angles A, B, C respectively. Prove that the second common internal tangent line to ω_b and ω_c is tangent to the incircles of the triangles AIB and AIC.

Problem 14. Let Ω be the circumcircle of a triangle ABC. A mixtilinear incircle is tangent to Ω at a point P and tangent to the sides AB and BC. The incircle of the triangle APC is tangent to AC at F. Prove that the second common internal tangent line to the incircles of the triangles APB and BPC passes through F.

Problem 15. The diagonals of a circumscribed quadrilateral $ABCD$ intersect at P. Prove that the incenters of the triangles PAB, PBC, PCD, PDA are concyclic.

Problem 16. Let O be the circumcenter of a bicentric quadrilateral $ABCD$. Prove that the incenters of the triangles OAB, OBC, OCD, ODA are concyclic.

On incircles

Part 3

Problem 17. Let P be a point inside a circumscribed quadrilateral $ABCD$. Let PL and PK be the angle bisectors of the triangles PAC and PBD. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Prove that the following four conditions are equivalent:

(1) The points L, K and I are collinear.

(2) The lines I_1I_2, I_3I_4 and the external bisector of the angle APC are concurrent.

(3) The points I_1, I_2, I_3, I_4 are concyclic.

(4) The images of the points A, B, C, D under inversion with center P are vertices of a circumscribed quadrilateral.

Problem 18. Let $ABCD$ be a circumscribed quadrilateral with incircle ω. Let P be a point such that $ABCP$ is a convex quadrilateral containing D and $\angle APD = \angle BPC$. Let ω_1, ω_2, ω_3, ω_4 be the incircles of the triangles PAB, PBC, PCD, PDA, and let I_1, I_2, I_3, I_4 respectively be their centers. Prove that

(a) The circles ω_1, ω_3 and ω have a common tangent line (and so do the circles ω_2, ω_4 and ω).

(b) The circles ω_1, ω_2, ω_3, ω_4 have a common tangent line.

(c) The points I_1, I_2, I_3, I_4 lie on a circle whose center lies on the line PI.

(d) The Miquel point of $I_1I_2I_3I_4$ coincides with P.

Part 4

Problem 19. Let AA_1, BB_1, CC_1 be cevians of a triangle ABC intersecting at point P. Prove that the incenters of the triangles APB_1, APC_1, BPC_1, BPA_1, CPA_1, CPB_1 lie on a conic in the following cases

(a) if P is the incenter of the triangle ABC;

(b) if P is the Fermat–Torricelli point of the triangle ABC.

On incircles

I.Frolov

Presented by P.Kozhevnikov, A.Zaslavsky

Solutions

Part 1

Problem 1. (a) Let P and Q be points on the sides AB and BC of a triangle ABC such that $AP = CQ$. Prove that the circle (BPQ) passes through the midpoint W of the arc ABC.

(b) Points P and Q are chosen on the sides AB and BC of a triangle ABC such that $AP+CQ = AC$. Prove that the circle (BPQ) passes through the incenter I of the triangle ABC.

Proof. (a) The triangles APW and CQW are congruent because $\angle PAW = \angle QCW$ and $AW = CW$. Therefore $\angle BPW = \angle BQW$ and the result follows.

(b) Let C_1 and A_1 be the common points of the incircle and the sides AB, BC respectively. Since $AC_1+CA_1 = AC$, we have $C_1P = A_1Q$. Thus the triangles C_1PI and A_1QI are congruent and $\angle PIQ = \angle A_1IC_1 = 180° - \angle PBQ$. □

Problem 2. The incircle of a triangle ABC is tangent to the side AC at D. Let P be a point on the side AC.

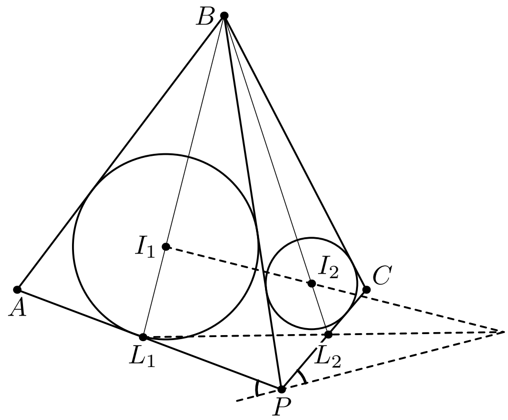
(a) Prove that one of the common internal tangent lines to the incircles of the triangles ABP and CBP passes through D.

(b) Let I_1 and I_2 be the incenters of the triangles ABP and CBP. Prove that the points I_1, I_2, D and P are concyclic.

Proof. (a) Let the second common internal tangent line to these incircles intersect AC and BP at points D' and X respectively. Then $D'A - AB = D'X - XB = D'C - CB$. It easy to see that D is the only point on AC satisfying $DA - AB = DC - CB$, hence $D = D'$.

(b) It is clear that $\angle I_1PI_2 = 90°$ and part (a) implies that $\angle I_1DI_2 = 90°$. □

Problem 3. Let P be a point inside an angle ABC. Let I_1 and I_2 be the incenters of the triangles PAB and PBC, and let BL_1 and BL_2 be the angles bisectors of these triangles (L_1 lies on PA and L_2 lies on PC). Prove that the lines I_1I_2, L_1L_2 and the external bisector of the angle APC are concurrent.



Proof. Let the external angle bisector of the angle APC intersect the line L_1L_2 at T. By a well-known property of angle bisectors

$$\frac{BI_1}{I_1L_1} = \frac{BP}{PL_1}, \qquad \frac{BI_2}{I_2L_2} = \frac{BP}{PL_2}, \qquad \frac{L_1T}{TL_2} = \frac{PL_1}{PL_2}$$

The result now follows from the Menelaus's theorem for the triangle BL_1L_2. □

Problem 4. Let $ABCD$ be a cyclic quadrilateral and let ℓ be the second common external tangent line to the incircles of the triangles ABC and ABD. Prove that $\ell \parallel CD$.

Proof. Let I_1 and I_2 be the incenters of the triangles ABC and ABD. The lines CI_1 and DI_2 intersect at the midpoint M of the arc AB of the circumcircle. Let N be the midpoint of the arc CD. Since $MI_1 = MI_2$, we have $I_1I_2 \perp MN$. This implies that $\angle(AB, MN) = \angle(MN, \ell)$, since $\angle(AB, I_1I_2) = \angle(I_1I_2, \ell)$. It is easy to see that $\angle(AB, MN) = \angle(MN, CD)$, thus $\ell \parallel CD$. □

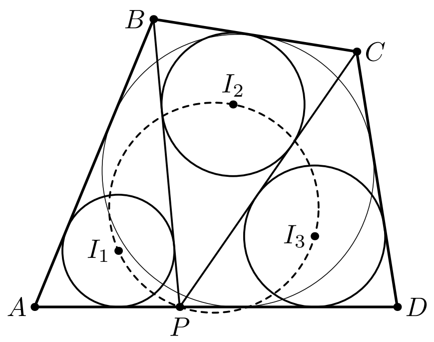
Problem 5. Let $ABCD$ be a cyclic quadrilateral and let I_1 and I_2 be the incenters of the triangles ABC and ABD. Let J_1 be the C-excenter of the triangle ACD and let J_2 be the D-excenter of the triangle BCD. Prove that the points I_1, I_2, J_1, J_2 are collinear.

Proof. In the solution to the previous problem we proved that $I_1I_2 \perp MN$, where M and N are the midpoints of the arcs AB and CD of the circumcircle. Let K and L be the midpoints of the arcs AD and BC. It is well-known that $MN \perp KL$. Since $KJ_1 = KA = KI_2$ and KL is the external bisector of the angle J_1KI_2, we have $J_1I_2 \parallel KL$. Therefore J_1 lies on I_1I_2, similarly for J_2. □

Problem 6. Let P be a point on the side AD of a circumscribed quadrilateral $ABCD$. Let ω_1, ω_2, ω_3 be the incircles of the triangles PAB, PBC, PCD and let I_1, I_2, I_3 be their centers. Prove that

(a) the points I_1, I_2, I_3 and P are concyclic;

(b) the circles ω_1, ω_2, ω_3 have a common tangent line.



Sketch of first proof. (a) Let I be the incenter of $ABCD$. Since $\angle BIC + \angle I_1II_3 = 180°$, the point I has an isogonal conjugate with respect to the quadrilateral BCI_3I_1. It must be the point I_2 since $\angle CBI = \angle I_1BI_2$ and $\angle BCI = \angle I_3CI_2$. Thus $\angle BI_2C + \angle I_1I_2I_3 = 180°$ and the problem follows by angle chase.

(b) Let m be the reflection of BP about I_1I_2 (i.e. the second internal common tangent to ω_1 and ω_2), and let n be the reflection of CP about I_2I_3. Using part (a) and angle chase one can see that $m \parallel n$, hence m coincides with n and we are done. □

Sketch of second proof. (b) Let ℓ be the second external tangent line to ω_1 and ω_3. Denote the intersection points of ℓ with BP and CP by K and L. Denote the common points of ω_1 with AB, BP, AD, ℓ by X_1, X_2, X_3, X_4 and the common points of ω_3 with CD, CP, AD, ℓ by Y_1, Y_2, Y_3, Y_4 respectively. Then

$$0 = AB + CD - AD - BC = X_1B + CY_1 - X_3Y_3 - BC = X_2B + CY_2 - X_4Y_4 - BC = KB + CL - KL - BC$$

Therefore the quadrilateral $BCLK$ is circumscribed, as required.

(a) Follows from part (b) by angle chase. □

On incircles

Solutions

Part 2

Problem 7. Let P be a point inside a circumscribed quadrilateral $ABCD$. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Prove that the external bisector of the angle APC passes through the second intersection point of the circles (PI_1I_2) and (PI_3I_4).

Sketch of proof. Use problem 1 several times. ☐

Problem 8. Let P be a point inside a convex quadrilateral $ABCD$, which does not lie on AC and BD. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Suppose that the lines I_1I_2, I_3I_4 and the external bisector of the angle APC are concurrent. Prove that the lines I_2I_3, I_1I_4 and the external bisector of the angle BPD are concurrent.

Sketch of proof. Perform an inversion in P and apply previous problem with its converse. ☐

Problem 9. Let $ABCD$ be a circumscribed quadrilateral with incircle ω and incenter I. Let ω_1 and ω_2 be the incircles of the triangles IAB and IBC. Let ω_3 be the C-excircle of the triangle ICD. Prove that

(a) the circles ω_1, ω_3 and ω have a common tangent line;

(b) the circles ω_1, ω_2 and ω_3 have a common tangent line;

(c) the centers of ω_1, ω_2, ω_3 and the A-excenter of the triangle IDA are concyclic.

Proof. Denote the center of ω_k as I_k.

(a) The common tangent to ω and ω_1 is the reflection of AB about II_1, and the common tangent of ω and ω_3 is the reflection of CD about II_3. It is easy to see that $\angle I_1II_3 = \angle AID$. Since AB and CD are the reflections of AD about IA, ID respectively, they are also the reflections about II_1, II_3 of the line obtained from AD by a rotation around I to the doubled angle AII_1. This line is the common tangent of three circles.

(b) Denote the lengths of tangents to ω from A, B, C, D as a, b, c, d respectively. Then the common tangent to ω and ω_1 equals $b - (a + b + BI - AI)/2$, the common tangent to ω and ω_3 equals $(c + d + CI + DI)/2 - c$, and the common tangents to ω_1 and ω_3 equals to the difference of these circles (by (a)). Finding similarly the lengths of common tangents to ω_1 and ω_2. ω_2 and ω_3 we can see that one of these segments is the sum of the remaining ones.

(c) The common tangent to ω_1, ω_2, and ω_3 is the reflection of IB, IC about I_1I_2 and I_2I_3 respectively. This allows to find the angle $I_1I_2I_3$. Finding similarly the angle $I_1I_4I_3$, where I_4 is the center of the fourth circle we see that these four centers are concyclic. ☐

Problem 10. Let P be a point inside a parallelogram $ABCD$ such that $\angle PDA = \angle PBA$. Let ω_1 and ω_4 be the A-excircles of the triangles PAB and PDA. Let ω_2 and ω_3 be the incircles of the triangles PBC and PCD. Prove that

(a) one of the common tangent lines to ω_1 and ω_3 is parallel to AD;

(b) the circles ω_1, ω_2, ω_3, ω_4 have a common tangent line which passes through the center of the parallelogram;

(c) the centers of the circles ω_1, ω_2, ω_3, ω_4 are concyclic.

Proof. (Sketch) We have that the radii of circles PAD and PAB are equal. Then the circles PBC and PCD also have the same radii.

(a) Translating by the vector $\vec{PQ} = \vec{AD}$ we obtain the following problem: Let $CPDQ$ be a cyclic quadrilateral. Then one of common tangents to the incircle of triangle PCD and the excircle of triangle CDQ opposite to D is parallel to PQ.

This follows from the known fact: the line joining the corresponding incenters (excenters) of triangles PCD, QCD is parallel to the bisector of the angle between CD and PQ (and this follows from the trident theorem).

See details in Towns Tournament, autumn 2021, A-level, 10-11.5.

(b) This ix equivalent to next problem.

(c) Follows from (b), similarly to part (c) of previous problem.

☐

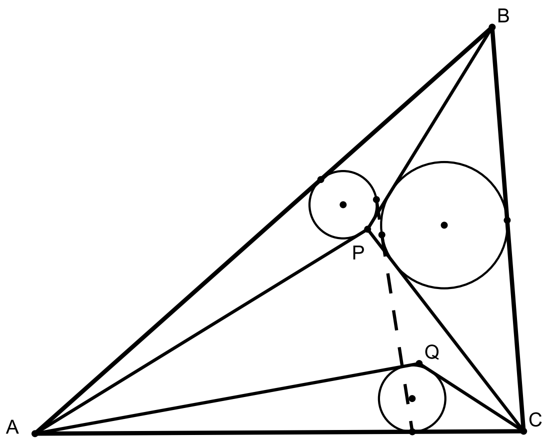
Problem 11. Let $ABCD$ be a convex quadrilateral with $\angle A = \angle C$. Prove that one of the common tangent lines to the incircles of the triangles ABD and BCD passes through the midpoint of AC.

Proof. See Sharygin olympiad 2022, problem 10.4. ☐

Problem 12. Let I be the incenter of a trianlge ABC. The incircle of the triangle AIC is tangent to AC at E. Prove that the second common internal tangent line to the incircles of the triangles AIB and BIC passes through E.

Sketch. Let D be the touch point of the incircle of ABC with AC, and let ℓ be the second common inner tangent to the incircles of AIB and BIC. Apply Problem 9(b) to (degenerate) circumscribed quadrilateral $ABCD$. We obtain that ℓ is tangent to excircles of AID and CID opposite to A and C, respectively. Now it suffices to apply analogue of Problem 2(a) for excircles to triangle AIC and a point D on AC. □

Remark. G.Galyapin proved the following generalization of this problem. If P and Q are isogonally conjugated with respect to triangle ABC, then the common internal tangent to the incircles of triangles APB and BPC distinct from PB passes through the touching point of AC with the incircle of triangle AQC.

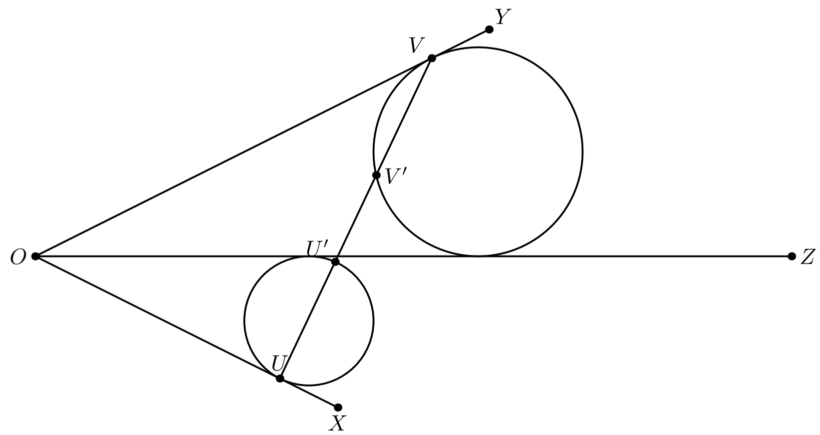


The next problem provides a way to construct the Malfatti circles in a triangle.

Problem 13. Let I be the incenter of a trianlge ABC. Let ω_a, ω_b, ω_c be pairwise tangent circles, inscribed in angles A, B, C respectively. Prove that the second common internal tangent line to ω_b and ω_c is tangent to the incircles of the triangles AIB and AIC.

Proof. Recall the following known fact

Lemma. Let OZ be the bisector of angle XOY. A circle ω_1 inscribed into angle XOZ touches OX at point U, and a circle ω_2 inscribed into angle YOZ touches OY at point V. Then the tangent from U to ω_2, equals the tangent from V to ω_1.



Now it is easy to see that each of quadrilaterals $XA'CB'$, $XB'AC'$, $XC'BA'$ (in notations of previous problem) is circumscribed. In fact, for example the difference of lengths of segments XA' and XB' equals the difference of lengths of tangents to the incircle of triangle IAB from A' and B'. Since these tangents are equal to the tangents from C' to the incircles of triangles IBC and IAC, this difference equals to the length of the common tangent og these circles, which equals $CA' - CB'$.

Now we have to prove that the incircles of these quadrilaterals are tangent. Note that the incircle of triangle IAB is also the incircle of triangle formed by a, b, and AB, and each of incircles of quadrilaterals $XB'AC'$ and $XC'BA'$ touches two sides of this triangle and the line XC' dividing it into two triangles. Finding the lengths of tangents to these circles from C' we see that they are equal. □

Problem 14. Let Ω be the circumcircle of a triangle ABC. A mixtilinear incircle is tangent to Ω at a point P and tangent to the sides AB and BC. The incircle of the triangle APC is tangent to AC at F. Prove that the second common internal tangent line to the incircles of the triangles APB and BPC passes through F.

Proof. Use the generalization of problem 12. The point P is isogonally conjugated to the infinite point of the nagelian from B. Thus the common tangent to the incircles of triangles APB and BPC passes through the touching point of AC with a circle β touching lines a and c parallel to the nagelian and passing through A and C respectively. It is clear that the bisectors of angles between a and AP, c and CP pass through I. But the bisector of angle APC also passes through I, therefore the touching points of β and the incircle of triangle APC with AC coincide. □

Problem 15. The diagonals of a circumscribed quadrilateral $ABCD$ intersect at P. Prove that the incenters of the triangles PAB, PBC, PCD, PDA are concyclic.

Proof. It is known that incircles of ABC and ADC touch at some point E. Let I_1, I_2, I_3, I_4 be the incenters of PAB, PBC, PCD, PDA, respectively. By Problem 2(b), PE is the radical axis of circles (PI_1I_2) and (PI_3I_4). (This statement is a degenerate case of Problem 7).

Let J_1 and J_2 be incenters of triangles ABD and CBD. By Desargue theorem applied to trinagles AI_1J_1 and CI_2J_2, lines AC, J_1J_2 and I_1I_2 are concurrent at T or parallel. Similarly, I_3I_4 passes through T, hence $TI_1 \cdot TI_2 = TP \cdot TE = TI_3 \cdot TI_4$ (in case of parallel lines $I_1I_2I_3I_4$ is an isosceles trapezoid).

Another solution could be found in Kvant, 1996. N 3 (problem M1524). □

Problem 16. Let O be the circumcenter of a bicentric quadrilateral $ABCD$. Prove that the incenters of the triangles OAB, OBC, OCD, ODA are concyclic.

Proof. Let I_1, I_2, I_3, I_4 be the incircles of OAB, OBC, OCD, ODA, respectively, and let J_1, J_2, J_3, J_4 be the excenters of these circles opposite to O. Note that the inversion in the circumcenter Ω maps I_k to J_k.

By Problem 7, the outer bisector ℓ of angle AOC passes through the second intersection point of circles (OI_1I_2) and (OI_3I_4). Similarly, ℓ passes through the second intersection point of circles (OJ_1J_2) and (OJ_3J_4). Perform inversion in Ω and obtain that I_1I_2 and I_3I_4 meet at some point T of ℓ, or parallel to ℓ. Therefore, $TI_1 \cdot TI_2 = TP \cdot TE = TI_3 \cdot TI_4$ (in case of parallel lines $I_1I_2I_3I_4$ is an isosceles trapezoid).

Another solution could be found in *A.Zaslavsky* On bicentric quadrilaterals, models of Lobachevsky geometry, and ¡¡the Nilov lemma¿¿ // Matematicheskoe Prosveschenie. Ser. 3. N. 25. Moscow.: MCCME. 2020. P. 163–166. □

Part 3

Problem 17. Let P be a point inside a circumscribed quadrilateral $ABCD$. Let PL and PK be the angle bisectors of the triangles PAC and PBD. Let I_1, I_2, I_3, I_4 be the incenters of the triangles PAB, PBC, PCD, PDA respectively. Prove that the following four conditions are equivalent:

(1) The points L, K and I are collinear.

(2) The lines I_1I_2, I_3I_4 and the external bisector of the angle APC are concurrent.

(3) The points I_1, I_2, I_3, I_4 are concyclic.

(4) The images of the points A, B, C, D under inversion with center P are vertices of a circumscribed quadrilateral.

Proof. Equivalency of (2) and (3) follows from Problem 8.

Equivalency of (2) and (4) follows from an analogue of Problem 7 for the P-excenters.

Let us prove equivalency of (1) and (4). Easy to see that (4) is equivalent to equality

$$\frac{AB}{AP \cdot BP} + \frac{CD}{CP \cdot DP} = \frac{BC}{BP \cdot CP} + \frac{AD}{DP \cdot DP} \qquad (*)$$

Hence L divides AC in ratio PA/PC, and K divides BD in ratio PB/PD. Denote the oriented area of triangle XYZ by S_{XYZ}. By linearilty,

$$S_{KIL} = \frac{PC \cdot S_{KIA} + PA \cdot S_{KIC}}{PA + PC} =$$

$$= \frac{PC \cdot PD \cdot S_{BIA} + PC \cdot PB \cdot S_{DIA} + PA \cdot PD \cdot S_{BIC} + PA \cdot PB \cdot S_{DIC}}{(PA + PC)(PB + PD)} =$$

$$= \pm\frac{r}{2} \cdot \frac{PC \cdot PD \cdot AB - PC \cdot PB \cdot DA - PA \cdot PD \cdot BC + PA \cdot PB \cdot CD}{(PA + PC)(PB + PD)}$$

(here r is the inradius of $ABCD$), since BIA and DIC equally oriented, while DIA and BIC are oriented differently. We obtain that equality $S_{KIL} = 0$ is equivalent to equality $(*)$. It suffices to note that $S_{KIL} = 0$ is equivalent to (1). □

Problem 18. Let $ABCD$ be a circumscribed quadrilateral with incircle ω. Let P be a point such that $ABCP$ is a convex quadrilateral containing D and $\angle APD = \angle BPC$. Let ω_1, ω_2, ω_3, ω_4 be the incircles of the triangles PAB, PBC, PCD, PDA, and let I_1, I_2, I_3, I_4 respectively be their centers. Prove that

(a) The circles ω_1, ω_3 and ω have a common tangent line (and so do the circles ω_2, ω_4 and ω).

(b) The circles ω_1, ω_2, ω_3, ω_4 have a common tangent line.

(c) The points I_1, I_2, I_3, I_4 lie on a circle whose center lies on the line PI.

(d) The Miquel point of $I_1I_2I_3I_4$ coincides with P.

Proof. (Sketch of solution)

(c), (d).

Note that PI bisects angles APC and BPD. (This follows for example from the properties of isogonal conjugation: I is conjugated to itself with respect to $ABCD$, hence I is conjugated to itself with respect to angle APC for any point P on the foci cubic of $ABCD$. Another proof can be obtained from the Desargue involution theorem: the bisectors of angles APC and BPD define a projective involution $\Pi(P) \to \Pi(P)$. This involution transposes the tangents from P to ω, which yields the required assertion: the bisector PI of angle between the tangents coincides with the bisectors of angles APC and BPD.)

We see that P coinside to the assumption 1 of problem 17. Therefore I_1, I_2, I_3, I_4 are concyclic.

Similarly to problem 17 (assumption 2) we can obtain that the meeting points X, Y of opposite sidelines of $I_1I_2I_3I_4$ lie on the external bisector of angle APC. There exists a unique point of this bisector distinct from X and Y such that AB and DC are seen from it with equal angles — this is the Miquel point of $I_1I_2I_3I_4$. (This also can be obtained from equality $PI_1 \cdot PI_3 = PI_2 \cdot PI_4$, and the fact that PI_1I_4 can be transformed to PI_2I_3 by the spiral similarity centered at the Miquel point.)

Since the Miquel point of a cyclic quadilateral is the projection of the circumcenter to XY, this circumcenter lies on the perpendicular to XY from P, i.e. on the bisector of angle PAC.

(b)

We can see that the Aubert line m of $I_1I_2I_3I_4$ is the required common tangent to ω_i. The idea is to consider four circles ω_i' centered at I_i and touching m. Reflecting m about I_1I_2, I_2I_3, I_3I_4, I_4I_1 we obtain lines a, b, c, d — common tangents to I_4 and I_1, I_1 and I_2, I_2 and I_3, I_3 and I_4 respectively. All lines a, b, c, d pass through P (because the reflections of Miquel point about the sidelines lie on the Aubert line), And since $I_1I_2I_3I_4$ is cyclic $\angle(a, c)$ and $\angle(b, d)$ have a common bisector. This define the circles ω_i' uniquely, hence each ω_i' coincide with ω_i.

(Another approach: reflecting the common tangent PB of circles ω_3 and ω_4 about I_3I_4 we obtain the second common tangent t of circles ω_3 and ω_4. Similarly construct the common tangent s of ω_1 and ω_2. Now it is easy to obtain that $t \parallel s$: since P the angle between I_3I_4 and I_1I_2 equals to the angle of spiral similarity $PI_1I_2 \sim PI_4I_3$, i.e a half of angle BPD. Also we can see that t and s coincide finding some common point of these lines.)

(a) (G.Galyapin).

The common tangent m from (b) is the reflection of PA about I_1I_4, or the reflection of PB about I_2I_4. From this $\angle I_4I_1I_2 = (\pi - \angle ADC)/2 = \pi - \angle AI_1B$. This means that there exists a point isogonally conjugated to I_1 with respect to AI_4I_2B. It is easy to see that AI_1 and AI are isogonals with respect to angle I_4AB, and BI_1 and BI are isogonals with respect to angle I_2BA. Thus this point is I. Therefore $\angle I_4II_2 = \pi - \angle AIB = \angle DIC$. Now the count of angles yields that the reflection of the common tangent AD of circles ω and ω_4 with respect to I_4I is parallel to the reflection of the common tangent BC of circles ω and ω_2 with respect to I_2I, i.e. this is the same tangent to ω touching also ω_2 and ω_4.

□

Part 4

Problem 19. Let AA_1, BB_1, CC_1 be cevians of a triangle ABC intersecting at point P. Prove that the incenters of the triangles APB_1, APC_1, BPC_1, BPA_1, CPA_1, CPB_1 lie on a conic in the following cases

(a) if P is the incenter of the triangle ABC;

(b) if P is the Fermat–Torricelli point of the triangle ABC.

Proof. Denote the incircles of the triangles APC_1, BPC_1, BPA_1, CPA_1, CPB_1, APB_1 by $w_1, \ldots, w_6$ and their incenters by $I_1, \ldots, I_6$ respectively.

(a) (G.Galyapin) Let $L_1 = II_1 \cap AB$, $L_2 = II_2 \cap AB$, $L_3 = II_3 \cap BC$, $L_4 = II_4 \cap BC$, $L_5 = II_5 \cap CA$, $L_6 = II_6 \cap CA$ be the feet of bisectors.

Lemma 1. BI_1 and BI_4 are isogonals with respect to ABC.

Proof. Let w_1' be the reflection of w_1 about BI. Then I is the internal homothety center of w_1 and w_4, and the internal homothety center of w_1 and w_1' lies on BI, hence the external homothety center of w_1' and w_4 lies on BI, but BC is the common tangent of w_1' and w_4, thus this center coincide with B. Since the angles between the tangents from B to w_1 and w_4 are equal we obtain the required assertion. $\square$

Lemma 2. $L_1, \dots, L_6$ lie on a conic.

Proof. Applying the Pascal theorem to $L_1L_6L_3L_4L_5L_2$ we obtain that it is sufficient to prove that $L_1L_6 \cap L_4L_5 \in BI$. This follows from the bisector property and the Menelaos theorem for the triangles ABB_1, CBB_1 and the lines L_1L_6, L_4L_5 respectively. $\square$

By the Desargues involution theorem the pencil of conics $< L_2L_3L_5L_6 >$ define a projective involution f of the line L_1L_4. Taking a conic from lemma 2 and the degenerated conic $L_2L_5 \cap L_3L_6$ we obtain that f transposes L_1 and L_4, and $f(I) = I$. The reflection about BI define a projective involution of the pencil $\Pi(B)$, and so a projective involution g of line L_1L_4. We see that $g(I) = I$, and g transposes L_1 and L_4, also by lemma 1 g transposes I_1 and I_4. Therefore $f = g$, and $g(I_1) = I_4$ yields that $L_2, L_3, L_5, L_6, I_1, I_4$ lie on a conic.

Similarly considering the pencil $< L_3L_6I_1I_4 >$, the line L_2L_5, and the conic $L_2, L_3, L_5, L_6, I_1, I_4$, we obtain that $L_3, L_6, I_1, I_4, I_2, I_5$ lie on a conic.

Finally taking the pencil $< I_2I_5I_1I_4 >$, the line L_3L_6, and the conic $L_3, L_6, I_1, I_4, I_2, I_5$, we obtain that $I_1, I_4, I_2, I_5, I_3, I_6$ lie on a conic.

Another solution can be found in *M. Tolovikov*, "Geometric proof of the incenter theorem and its analogues" Matematicheskoe Prosveshhenie, no 29, 2022, p. 171-182 (in Russian).

(b) Let J_a, J_b, J_c be the incenters of the triangles BPC, CPA, APB, the lie on AA_1, BB_1, CC_1 respectively. By Problem 3 the lines I_2I_3, J_bJ_c and I_4I_1 intersect at some point X_a. Moreover, $\frac{J_bX_a}{X_aJ_c} = \frac{J_bP}{PJ_c}$. Define points X_b and X_c similarly. By Menelaus's theorem for the triangle $J_aJ_bJ_c$ the points X_a, X_b and X_c are collinear. The result now follows from the Pascal theorem for the hexagon $I_2I_3I_6I_1I_4I_5$. $\square$

Задача Арнольда о конфигурациях прямых и теорема Чеканова

Юрий Чеканов, Алексей Белов-Канель, Федор Нилов, Илья Иванов-Погодаев, Антон Белецкий

A Введение. Конфигурации прямых и плоскостей

A1 n прямых общего положения делят плоскость на части. Сколько получится частей?

A2 n лучей делят плоскость на части. Каково максимальное возможное число частей?

A3 n плоскостей общего положения делят пространство на части. Сколько получится частей?

A4 Тот же вопрос для k-мерного пространства.

A5 n полуплоскостей делят пространство на части. Каково минимальное возможное число частей?

A6 n полуплоскостей делят пространство на части. Каково максимальное возможное число частей?

A7 Тот же вопрос для четырехмерного пространства.

A8 Тот же вопрос для k-мерного пространства.

A9 n прямых общего положения делят плоскость на части. Докажите, что среди частей разбиения будет по крайней мере а) $n/3$ б) $(2n-1)/3$ треугольников.

A10 n прямых общего положения делят плоскость на части. Приведите пример, когда среди частей разбиения будет $n-2$ треугольника.

A11 n гиперплоскостей общего положения делят k-мерное пространство на части. Приведите пример, когда среди частей разбиения будет $n-k$ симплексов.

A12 $n>2$ прямых общего положения (т.е. больших кругов) делят сферу на части. Докажите, что среди частей разбиения будет хотя бы $2n$ треугольников. Докажите, что минимум достигается.

A13 Обобщите задачу для k-мерной сферы.

A14 n прямых общего положения делят плоскость на части. Докажите, что среди частей разбиения будет хотя бы $n-2$ треугольника.

Указание. Для каждой прямой L рассмотрим $n-1$ точек, в которых она пересекает другие прямые. После этого для каждых двух последовательных точек $A=L\cap S$ и $B=L\cap T$ пересечения и прямых и рассмотрим треугольник, образованный прямыми L,S и T, после чего поставим метку $*$ внутри этого треугольника рядом с серединой стороны AB. Таким образом, вдоль прямой L? имеется $n-2$ меток, и следовательно всего получается $n(n-2)$ меток. С другой стороны, докажите любая нетреугольная часть P из тех, на которые плоскость разбита данными прямыми, может содержать не более двух меток. При подсчете числа частей учтите, что ровно $2n$ из них неограничены.

A15 Альтернативное доказательство содержится в статье

http://kvant.mccme.ru/1992/11/treugolniki_i_katastrofy.htm Обобщите его для разбиения пространства гиперплоскостями необщего положения.

A16 Обобщите доказательство, намеченное в указании. Впрочем, осуществить это авторам проекта не удалось.

B Вводные задачи. Эллиптические кривые (кубики) и сложение точек.

B1 Рассмотрим окружность $S : x^2 + y^2 = 1$. Из точки $(0, 1)$ провели рациональную прямую L. Докажите, что все точки пересечения $L \cap S$ рациональны и что все рациональные точки на S так могут получиться.

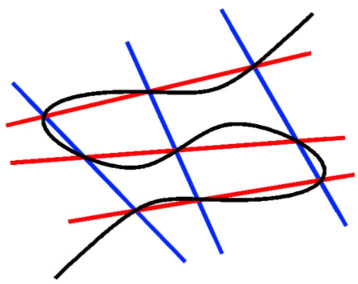
B2 Пусть x, y, z – взаимно простые натуральные числа, такие что $x^2 + y^2 = z^2$, x четно. Докажите, что тогда $x = 2uv, y = u^2 - v^2$, $z = u^2 + v^2$ для некоторых целых u, v.

B3 Обобщите результат для уравнения $x^2 + 2y^2 = z^2$.

B4 Постарайтесь получить возможно более общие результаты.

B5 Пусть $C : y^2 = ax^3 + bx^2 + cx + d$ – кубическая кривая с рациональными коэффициентами. Докажите, что прямая, соединяющая две рациональные точки на C содержит еще одну. Если три точки X, Y, Z на кривой C лежат на одной прямой будем это обозначать так: $X + Y + Z = 0$. ($X = Y$ означает касание).

B6 (Теорема о девяти точках). Если 8 из 9 точек пересечения двух троек прямых (на рисунке – синих и красных) лежат на кубике (кривой 3 порядка, чёрной), то девятая тоже лежит на ней.



B7 Выведите **теорему Паскаля**: *Если шестиугольник вписан в коническое сечение, то точки пересечения трёх пар противоположных сторон лежат на одной прямой.*

B8 Если многоугольник с $4n + 2$ сторонами вписан в коническое сечение и противоположные его стороны продолжены таким образом, чтобы пересечься в $2n + 1$ точке, то если $2n$ этих точек лежат на прямой, последняя точка будет лежать на той же прямой.

B9 (**Теорема Шаля**) Если в проективной плоскости две кубики имеют 9 общих точек, то любая другая кубика, проходящая через 8 из них, проходит и через девятую.

B10 Точки A, B, C, D, E, F лежат на одном коническом сечении. Тогда прямые Паскаля шестиугольников $ABFDCE, AEFBDC$ и $ABDFEC$ пересекаются в одной точке.

B11 (**Теорема Паппа**) Пусть A, B, C – три точки на одной прямой, A', B', C' – три точки на другой прямой. Пусть три прямые AB', BC', CA' пересекают три прямые $A'B, B'C, C'A$, соответственно, в точках X, Y, Z. Тогда точки X, Y, Z лежат на одной прямой.

B12 Зафиксируем на кубической кривой точку O. Если $A + B + O = 0$, то положим $B = -A$. Если $A + B + (-C) = 0$, то положим $C = A + B$. Ясно, что наша операция сложения коммутативна. Выведите из теоремы о 9 точках ее ассоциативность.

C Теорема Сильвестра

C1 (**Двойственная теорема Сильвестра**) Если на плоскости дано такое конечное множество прямых, что через любую точку пересечения двух данных прямых проходит еще одна из них, то все они проходят через одну точку или параллельны.

C2 (**Теорема Сильвестра**) На плоскости дано конечное число точек, причём такое, что любая прямая, проходящая через две из данных точек, содержит еще одну данную точку. Тогда все данные точки лежат на одной прямой.

Аналогично пространствам $\mathbb{R}^n$, состоящим из упорядоченных наборов n действительных чисел, рассматривают аналогичные пространства, где действительные числа заменены остатками по модулю p (поле $\mathbb{Z}_p$) или комплексными числами (поле комплексных чисел). Тогда говорят о *пространстве над* соответствующим полем. Прямые и подпространства определяются аналогично.

C3 Верно ли аналогичное утверждение для плоскости над полем $\mathbb{Z}_p$?

C4 Верно ли аналогичное утверждение для комплексных чисел?

C5 Верно ли аналогичное пространственное утверждение: *В пространстве дано конечное число точек, причём такое, что любая плоскость, проходящая через три из данных точек, содержит еще одну данную точку. Тогда все данные точки лежат на одной плоскости.*

C6 Докажите, что через 5 точек общего положения проходит единственная квадрика (кривая второго порядка).

C7 Докажите, что через 9 точек общего положения проходит единственная кубика (кривая третьего порядка).

C8 Обобщите утверждение для гиперповерхностей степени k в n-мерном пространстве.

C9 *Цикл* – это прямая либо окружность. На плоскости дано конечное число точек такое, что любой цикл, проходящий через три из них, проходит еще через одну данную точку. Тогда все данные точки лежат на одном цикле.

C10 На плоскости дано конечное число точек, причём такое, что любая квадрика, проходящая через пять из них, содержит еще одну. Тогда все данные точки лежат на одной квадрике.

D Задача Арнольда

D1 (**В.И.Арнольд**) Раскрасим области, на которые d прямых общего положения делят плоскость, в два цветам белый и черный (соседние области окрасим в разные цвета). Тогда число черных областей асимптотически не превосходит удвоенного числа белых.

Иными словами, число черных минус удвоенное число белых областей для конфигурации из n прямых либо отрицательно, либо асимптотически меньше общего числа областей.

Величины a_n и b_n *асимптотически равны*, если $a_n/b_n \to 1$ при $n \to \infty$, величина a_n растет *асимптотически быстрее* b_n, если $b_n/a_n \to 0$ (обозначение $b_n = o(a_n)$).

D2 (**Основная лемма**) На плоскости можно расположить p точек так, чтобы асимптотически $p^2/6$ прямых ($p \to \infty$) проходили ровно через три точки.

D3 Выведете из основной леммы, что оценка из D1 асимптотически достигается.

Указание. Проективно-двойственное расположение состоит из p прямых, пересекающихся по три в $p^2/6$ точках. Выберем достаточно малое ε и заменим каждую прямую двумя прямыми, отстоящими от нее на ε. Получится искомая конфигурация из $d = 2p$ прямых.

D4 Докажите, что для любого p можно найти подгруппу точек кубики, изоморфную $\mathbb{Z}_p$.

D5 Получите D2 из D4.

D6 Найдите асимптотику максимально возможного числа треугольников при разбиении плоскости n прямыми.

Задача Арнольда о конфигурациях прямых и теорема Чеканова. Дополнительные задачи

Юрий Чеканов, Алексей Белов-Канель, Федор Нилов, Илья Иванов-Погодаев, Антон Белецкий

Теорема Сильвестра

C11 На плоскости отмечено несколько точек, не все на одной прямой. Тогда можно указать такие три из них, что строго внутри окружности, проходящей через эти три точки, нет отмеченных точек.

C12 На плоскости отмечено несколько точек, не все на одной прямой. Тогда можно указать такие три из них, что внутри или на границе окружности, проходящей через эти три точки, лежат все отмеченные точки.

C13 Исследуйте пространственные обобщения.

C14 **Набросок доказательства Штейнберга теоремы Сильвестра.** Доказываем от противного. Рассмотрим конечное множество точек M. Любую прямую, проходящую через две точки множества M, мы будем называть *соединительной*. Прямую, проходящую ровно через две точки множества M, мы будем называть *прямой Сильвестра*. Выберем точку X из M и прямую L, проходящую через X, не содержащую других точек M. Пусть ни одна из соединительных прямых, проходящих через точку X, не является прямой Сильвестра. Среди точек пересечения соединительных прямых с прямой L выберем точку Y такую, что отрезок XY не пересекается другими соединительными прямыми. Докажите, что соединительная прямая, проходящая через точку Y, является прямой Сильвестра.

C15 a) Пусть ABC – треугольник на плоскости, а PQR – вписанный в него треугольник. Докажите, что площадь одного из трех треугольников, остающихся после выкидывания треугольника PQR, не превышает площади треугольника PQR;

b) **Набросок доказательства Элкинса и Зайденберга.** Докажите двойственную теорему Сильвестра, используя предыдущее утверждение.

C16 На плоскости дано конечное число окружностей. Известно, что любые две окружности имеют две или одну общие точки. a) Верно ли, что найдется точка пересечения, через которую проходит не более трех окружностей?

b)* А если любые две окружности имеют ровно две точки пересечения?

C17 На плоскости дано конечное число коник. Известно, что любые две коники имеют 4 различные общие точки. a) Верно ли, что найдется точка пересечения, через которую проходит не более четырех коник; b)* не более пяти коник? c)* А если некоторые из общих точек могут совпадать?

C18 На плоскости дано несколько окружностей. Отметили все точки их пересечения. Оказалось, что на каждой окружности лежит ровно n отмеченных точек, а через каждую отмеченную точку проходят ровно n окружностей. Может ли n быть равно a) 4; b) 5; c)* больше 5?

C19 В пространстве даны несколько точек и несколько плоскостей. Известно, что через любые две точки проходят ровно две плоскости, а каждая плоскость содержит не меньше четырех точек. Верно ли, что все точки лежат на одной прямой?

C20 Имеется 9 точек на плоскости: три красные, три синие, три зелёные. Никакие 4 не лежат на одном цикле (окружности или прямой). *Дугами циклов* будем называть дуги окружностей и отрезки прямых. Докажите, что существуют три непересекающиеся дуги цикла, на каждой из которых лежит по точке каждого цвета.

Задача Арнольда

D7 Постарайтесь получить аналогичное D1 утверждение для пространства.

D8 Тот же вопрос для n-мерного пространства.

D9 Постарайтесь получить оценки для максимального числа тетраэдров в трехмерном пространстве.

D10 Тот же вопрос для n-мерного пространства.

D11 а) n окружностей делят плоскость на части. Эти части правильно раскрасили в черный и белый цвета. Каким может быть отношение числа черных частей к числу белых? б) Тот же вопрос для случая, когда окружности попарно пересекаются. Постарайтесь получить разумные оценки.

Arnold problem for line configurations and Chekanov theorem

Yu. Chekanov, A. Ya. Kanel-Belov, F. Nilov, I. Ivanov-Pogodaev, A. Beletsky

A Introduction. Configurations of lines and planes

A1 n lines in general position split the plane into parts. How many parts will there be?

A2 n rays split the plane into parts. What is the largest possible number of parts?

A3 n planes in general position split the space into parts. How many parts will there be?

A4 The same question, but for the k-dimensional space.

A5 n half-planes split the space into parts. What is the minimal possible number of parts?

A6 n half-planes split the space into parts. What is the maximal possible number of parts?

A7 The same question, but for the 4-dimensional space.

A8 The same question, but for the $k-$-dimensional space.

A9 n lines in general position split the plane into parts. Prove that among these parts there will be at least a) $n/3$; b) $(2n-1)/3$ triangles.

A10 n lines in general position split the plane into parts. Give an example where exactly $n-2$ of these parts are triangles.

A11 n hyperplanes in general position split the k-dimensional space into parts. Give an example where exactly $n-k$ of these parts are (k-dimensional) simplexes.

A12 $n > 2$ lines (i.e. great circles) in general positions split the sphere into parts. Prove that among these parts there will be at least $2n$ triangles. Prove that this bound can be obtained.

A13 The same question, but for the k-dimensional sphere.

A14 n lines in general position split the plane into parts. Prove that among these parts there will be at least $n-2$ triangles.

Hint. For each line L consider $n-1$ points of intersection of L with other lines. Now, for any two consecutive points $A = L \cap S$ and $B = L \cap T$ on L consider a triangle formed by L, S and T, a place a mark $*$ inside this triangle near the middle of the segment AB. In the say, along L we have $n-2$ marks, giving $n(n-2)$ marks in total. Now, prove that any non-triangular part P contains at most 2 marks. Keep in mind that exactly $2n$ parts are unbounded.

A15 Alternative proof (in Russian) can be found here:

http://kvant.mccme.ru/1992/11/treugolniki_i_katastrofy.htm

Generalize it to the case of the k-dimensional space and hyperplanes that are not necessarily in general position.

A16 Generalize the hinted proof to this case. Keep in mind that the authors couldn't do that, though.

B Introductory problems. Elliptic curves (cubics) and addition on them.

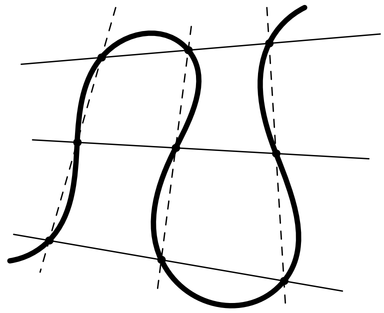
B1 Consider a circle $S : x^2 + y^2 = 1$. Consider a *rational* line L trough a point $(0, 1)$ (i.e. its slope is rational). Prove that all points of intersection $L \cap S$ are rational and that all rational points on S canbe obtained in this way.

B2 Let x, y, z be coprime, and let $x^2 + y^2 = z^2$, where x is even. Prove that we have $x = 2uv, y = u^2 - v^2$, $z = u^2 + v^2$ for some $u, v \in \mathbb{Z}$.

B3 Generalize this result to the case of the equation $x^2 + 2y^2 = z^2$.

B4 Find further possible generalizations.

B5 Let $C : y^2 = ax^3 + bx^2 + cx + d$ be cubic curves with rational coefficients. Prove that a line going through 2 rational points on C contains one more such rational point. Whenever points X, Y, and Z on C lie on the line, we denoted it by $X + Y + Z = 0$.



B6 (Nine points on a cubic curve theorem). If 8 among the 9 points of intersection of the two line triplets (see the picture) lie on a cubic curve, then the last point also lies on that curve.

B7 Prove **Pascal's theorem**: *If all vertices of a hexagon lie on the conic curve, then the points of intersection of pairs of its opposite sides lie on the line.*

B8 If all vertices of a polygon with $4n + 2$ edges lies on a conic curve, and each pair of its opposites sides is continued to their intersection, then if $2n$ of these intersection points lie on the line, then the last intersetion point also lies on that line.

B9 (**Cayley-Bacharach theorem**) Assume that two cubics C_1 and C_2 in the projective plane meet in nine (different) points. Then every cubic that passes through any eight of the points also passes through the ninth point.

B10 Points A, B, C, D, E, F lie on the conic. Then Pascal's lines (see B7) $ABFDCE, AEFBDC$ Pë $ABDFEC$ intersect at one point.

B11 (**Pappu's hexagon theorem**) let A, B, C be three points on a line, and A', B', C' be three points on another line. Denote intersections of AB', BC', CA' with $A'B, B'C, C'A$ by X, Y, Z. Then X, Y, Z lie on the line.

B12 Fix some point O on the cubic curve. If $A + B + O = 0$, we write $B = -A$. If $A + B + (-C) = 0$, we write $C = A + B$. It is clear that this operation is commutatove. Derive its associativity from B6.

C Sylvester-Gallai theorem

C1 (**Dual Sylvester-Gallai theorem**) For any finite set of lines on the plane, if any point of intersection of these lines has at least three lines passing through it, then all of those lines are either parallel or pass through a single point.

C2 (**Sylvester-Gallai theorem**) For any finite set of of points in the plane, if there is no line that passes through exactly 2 points, then all of those points lie on a single line.

Analogous to the space $\mathbb{R}^n$, consisting of tuples of n real numbers, we can consider the spaces $\mathbb{Z}_p^n$ and $\mathbb{C}^n$, where numbers are taken from either $\mathbb{Z}_p$ or $\mathbb{C}$. Lines and subspaces are defined in the same way. These are called vector spaces over $\mathbb{Z}_p$ and vector spaces over $\mathbb{C}$, respectively.

C3 Does the Sylvester-Gallai theorem hold for the plane over $\mathbb{Z}_p$?

C4 Does Sylvester-Gallai theorem hold for the plane over $\mathbb{C}$?

C5 Is the same true in 3-dimensional space? *For any finite set of points in space, if any plane passing through three of these points passes through at least another one, then all of those points lie on a plane.*

C6 Prove that given five points in general position, there is a unique conic (i.e. quadratic curve) passing through all of them.

C7 Prove that given nine points in general position, there is a unique cubic (i.e. cubic curve) passing through all of them.

C8 Generalize this result to the case of hypersurfaces of degree k in n-diensional space.

C9 A *cycle* is either a line or a circle. Suppose you are given a finite set of points, such that every cycle passing through 3 of them passes through at least another one. Then all of these points lie on the single cycle.

C10 Suppose you are given a finite set of points, such that every quadric passing through 5 of them passes through at least another one. Then all of these points lie on the single quadric.

D Arnold's problem

D1 (**Arnold's problem**) n lines split the plane into parts. Color these parts in black and white, such that two parts sharing an edge have different colors. Then the number of black parts is asymptotically not more than twice the number of white parts.

In other words, number of black parts minus twice the number of white parts is either negative or asymptotically less than the total number of parts.

We call a_n and b_n *asymptotically equal* , if $a_n/b_n \to 1$ when $n \to \infty$, and we cay that a_n grows *asymptotically faster* than b_n, if $b_n/a_n \to 0$ (we write $b_n = o(a_n)$).

D2 (**Main lemma**) There exists a configuration of p points on a plane such that asymptotically $p^2/6$ lines ($p \to \infty$) go through exactly 3 points.

D3 Use main lemma to prove that the bound in D1 can be obtained.

Hint. Projective dual configuration consists of p lines that intersect in $p^2/6$ points. Fix small enough ε and replace each line with a pair of lines shifted by ε. the resulting configuration of $d = 2p$ lines is the answer.

D4 Show that for every p there exists a subgroup of points on a cubic curve that is isomorphic to $\mathbb{Z}_p$.

D5 Derive D2 from D4.

D6 Find (asymptotically) the maximal number of triangles when splitting the plane with n lines.