Покрасьте мою шляпу в 3,5 цвета!

К. Кохась, А. Латышев

Задачу представляют: О. Бурсиан, Д. Кохась Д, К. Кохась, В. Ретинский

1 Знакомьтесь: игра в шляпы

Пусть дан неориентированный граф G, в каждой вершине которого находится один мудрец и один сундук со шляпами разного цвета. Мудрецы знакомы друг с другом, граф G, расположение мудрецов по вершинам графа и все цвета шляп в сундуках зафиксированы и известны всем. В частности, каждый мудрец понимает, в какой вершине находится каждый из остальных мудрецов. Судья проводит с мудрецами следующий тест. Он надевает каждому мудрецу шляпу из его сундука. Каждый мудрец видит только шляпы мудрецов, находящихся в соседних вершинах графа, но не видит своей шляпы и не знает ее цвета. Мудрецы не общаются во время теста. По команде судьи мудрецы одновременно записывают каждый на своей бумажке названия нескольких цветов (сколько именно цветов должен указывать мудрец, определяется дополнительным правилом). Считается, что мудрецы успешно прошли тест = «выиграли», если хотя бы один из них угадал хотя бы в одной из своих попыток.

Перед тестом мудрецам сообщили правила теста и дали возможность устроить совещание, на котором они должны определить публичную стратегию. Публичность означает, что все, включая судью, знают ее. Стратегия мудрецов должна быть детерминированной — каждый мудрец должен записывать на бумажку цвета, исходя только из того, какие цвета он видит у соседей. Будем говорить, что стратегия выигрышная, если при любой раскладке шляп хотя бы один мудрец угадает цвет надетой на него шляпы, т. е. упомянет этот цвет в своем списке. Также будем говорить, что мудрецы выигрывают, если они имеют выигрышную стратегию, и проигрывают, если не имеют.

Таким образом, игра в шляпы не есть игра в привычном понимании этого слова. Она длится всего один ход. Вот несколько задач на этот сюжет.

1.1. Каждому из двух мудрецов надевают шляпу белого, синего, красного или зеленого цвета. Каждый из них видит шляпу другого, но не видит свою. Они должны одновременно попытаться угадать цвет своей шляпы, написав на своей бумажке два цвета. Докажите, что мудрецы могут заранее договориться действовать так, чтобы хотя бы один из них угадал.

1.2. Каждому из двух мудрецов надевают шляпу одного из пяти возможных цветов. Каждый из них видит шляпу другого, но не видит свою. Они должны одновременно попытаться угадать цвет своей шляпы, написав на бумажке: первый — какие-то два цвета, второй какие-то три цвета. Докажите, что мудрецы могут заранее договориться действовать так, чтобы хотя бы один из них угадал.

1.3. Пять мудрецов стоят по кругу возле непрозрачного баобаба. Шах надел на голову каждого из мудрецов красную, синюю, желтую или зеленую шляпу. Мудрец не знает цвет своей шляпы и видит только двух соседних по кругу мудрецов. Не общаясь, мудрецы одновременно должны высказать предположение о цвете своей шляпы. При этом они боятся оказаться слишком удачливыми. Как им следует действовать, чтобы при любом раскладе шляп цвет своей шляпы угадало не более двух мудрецов?

1.4. Султан устроил экзамен шести придворным мудрецам. По правилу экзамена султан размещает 5 мудрецов в 5 ям, расположенных по кругу, а шестого мудреца сажает на вышку в центре круга. На лбу у каждого из первых пяти мудрецов султан пишет число 1, 2 или 3; на лбу у центрального мудреца султан пишет число от 1 до 243. Мудрец на вышке видит числа на всех остальных мудрецах, а те видят его число (но не видят друг друга). Все мудрецы должны одновременно попытаться угадать свои числа: для этого мудрецы в яме должны назвать по два числа, а мудрец на вышке — одно. Султан заранее объяснил мудрецам правила экзамена и дал им время посовещаться до начала экзамена. Могут ли мудрецы действовать так, чтобы хотя бы один из них заведомо угадал свое число?

Мы будем отождествлять вершину графа G и мудреца, который в ней находится. Будем считать, что цвета пронумерованы числами 0, 1, 2, 3, ... и что в сундуке мудреца v лежат шляпы с цветами от 0 до некоторого числа $h(v) - 1$.

Игрой в шляпы назовем тройку $\langle G, h, g\rangle$, где $G = \langle V, E\rangle$ — граф, $h\colon V \to \mathbb{N}$ — функция, сопоставляющая вершине количество (цветов) шляп, лежащих в сундуке в этой вершине, $g\colon V \to \mathbb{N}$ — функция, показывающая, сколько попыток угадывания имеет каждый мудрец. Функцию h мы будем называть «шляпностью», а g — функцией угадывания или числом попыток. Если h — натуральное число, символом $\star h$ будем обозначать функцию на V, принимающую постоянное значение h. Вместо обозначения $\langle G, h, \star 1\rangle$ мы будем использовать более короткое обозначение $\langle G, h\rangle$.

1.5. Докажите, что если игра $\langle G, h, g\rangle$ выигрышная, то для всех натуральных k игра $\langle G, k \cdot h, k \cdot g\rangle$ тоже выигрышная.

1.6. Дана игра $\langle G, h, g\rangle$. Пусть $K \subset G$ — антиклика (множество вершин, между которыми не проведено ни одного ребра) и для всех $v \in K$ $h(v) > g(v)$. Докажите, что существует расклад шляп, для которого ни один мудрец из K не угадывает.

1.7. Пусть h и g натуральные числа, $G = \langle G, \star h, \star g\rangle$ — выигрышная игра, $r' \leqslant \frac{h}{g}$ — рациональное число. Докажите, что существуют натуральные числа h' и g', для которых $\frac{h'}{g'} = r'$ и игра $\langle G, \star h', \star g'\rangle$ — выигрышная.

1.8. Сформулируйте и докажите аналог предыдущего утверждения для непостоянных функций шляпности и угадывания.

1.9. Обозначим через K_n полный граф на n вершинах. Докажите, что в игре $\langle K_n, h, g\rangle$ мудрецы выигрывают тогда и только тогда, когда $\sum\limits_{v \in K_n} \frac{g(v)}{h(v)} \geqslant 1$.

2 Пути и деревья

Теория игры в шляпы на полном графе из трех вершин исчерпывается утверждением задачи 1.9. Рассмотрим игру на более простом графе – пути P_3.

2.1. Докажите, что в игре $\langle P_3, \star 3, \star 1\rangle$ мудрецы проигрывают.

2.2. а) Докажите, что игра $\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{5}}{\bullet}$ — выигрышная (числитель дроби возле вершины обозначает количество попыток, а знаменатель — шляпность).

б) Докажите, что игра $\overset{\frac{3}{11}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{5}}{\bullet}$ — проигрышная.

в) Докажите, что игра $\overset{\frac{s}{t(s)}}{\bullet}\!\!-\!\!\overset{\frac{s}{t(s)}}{\bullet}\!\!-\!\!\overset{\frac{s}{t(s)}}{\bullet}$, где $t(s) = s^2 + s + 1$, — проигрышная.

Пусть дан граф G и натуральное число s. Наибольшее число шляп h, для которого игра $\langle G, \star h, \star s\rangle$ выигрышная, называется s-шляпным числом графа и обозначается $\mathrm{HG}_s(G)$. При $s = 1$ мы называем это число просто шляпным числом и обозначаем $\mathrm{HG}(G)$.

2.3. Докажите, что для любых натуральных n и s игра $\underset{A}{\overset{\frac{s}{2s}}{\bullet}}\!\!-\!\!\bullet\!\!-\!\!\bullet\cdots$ на пути P_n проигрышная. Все вершины, кроме крайней вершины A, имеют шляпность $4s - 1$ и s попыток.

2.4. Докажите, что существуют пути P_n, для которых $\mathrm{HG}_2(P_n) = 6$, $\mathrm{HG}_3(P_n) = 10$, $\mathrm{HG}_4(P_n) = 14$.

2.5. Докажите, что для любого натурального s игра $\langle P_n, \star(4s - 2), \star s\rangle$ выигрышная при $n \geqslant 2s$.

2.6. а) Пусть $t(s) = s^2 + s + 1$. Докажите, что для любого дерева T игра $\langle T, \star t(s), \star s\rangle$ проигрышная.

b) Пусть $K_{1,n}$ — граф «звезда» (дерево, состоящее из корня и n листьев). Докажите, что при больших n игра $\langle K_{1,n}, \star(s^2 + s), \star s\rangle$ — выигрышная.

c) Докажите, что для любого натурального h существует такое натуральное n, что игра на графе $K_{1,n}$ — выигрышная, если шляпности всех периферийных мудрецов равны 3 и все они имеют по одной попытке угадывания, а шляпность центрального мудреца равна h и у него две попытки.

3 Конструкторы

3.1. Пусть $\langle G, h, g\rangle$ — выигрышная игра, A_1 и A_2 — вершины графа G, не соединенные ребром, причем $h(A_1) = h(A_2)$, $\widetilde{G}$ — граф, получающийся из G склеиванием вершин A_1 и A_2 в одну вершину A. Пусть функции $\widetilde{h}$, $\widetilde{g}$ на вершинах графа $\widetilde{G}$ совпадают с h и g во всех вершинах, кроме A_1 и A_2, и $\widetilde{h}(A) = h(A_1)$, $\widetilde{g}(A) = g(A_1) + g(A_2)$. Тогда игра $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ тоже выигрышная. (И тогда, если игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ проигрышная, то и $\langle G, h, g\rangle$ проигрышная.)

Пусть $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$, $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — две игры, такие что $V_1 \cap V_2 = \{v\}$. Пусть $G = G_1 +_v G_2$ — объединение графов G_1 и G_2, в котором обе вершины v объединены в одну вершину. Зададим функции $h, g\colon V_1 \cup V_2 \to \mathbb{N}$:

$$h(u) = \begin{cases} h_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ h_1(v)h_2(v), & u = v, \end{cases} \qquad g(u) = \begin{cases} g_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ g_1(v)g_2(v), & u = v. \end{cases}$$

Игру $\mathcal{G} = \langle G, h, g\rangle$ будем обозначать $\mathcal{G}_1 \times_v \mathcal{G}_2$ (рис. 1).

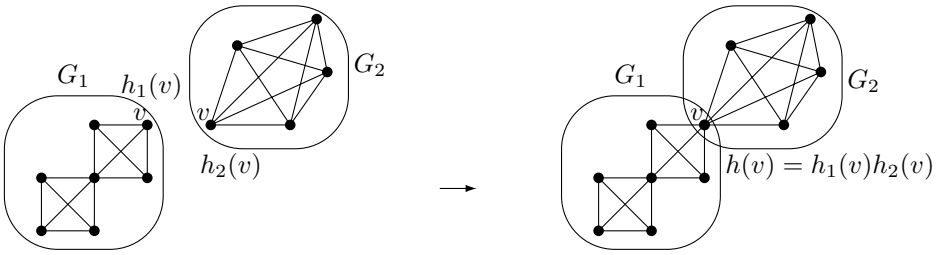


Рис. 1. Игра $G_1 \times_v G_2$

3.2. Теорема о произведении. Если мудрецы выигрывают в играх $\mathcal{G}_1$ и $\mathcal{G}_2$, то они выигрывают и в игре $\mathcal{G}_1 \times_v \mathcal{G}_2$.

3.3. Пусть $G = G_1 +_A G_2$, где G_1 и G_2 — графы, у которых $V(G_1) \cap V(G_2) = \{A\}$, а игры $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ и $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — проигрышные, и при этом

$$g_1(A) = g_2(A) = s, \qquad h_1(A) \geqslant h_2(A) = s + 1.$$

Тогда игра $\mathcal{G} = \langle G_1 +_A G_2, h, g\rangle$ — проигрышная, где

$$h(x) = \begin{cases} h_i(x), & x \in V_i \setminus \{A\},\ (i = 1, 2),\\ h_1(A), & x = A, \end{cases} \qquad g(x) = \begin{cases} g_i(x), & x \in V_i \setminus \{A\},\ (i = 1, 2),\\ s, & x = A. \end{cases}$$

3.4. Удаление полуребра. Пусть $\langle G, h, g\rangle$ — выигрышная игра, AB — ребро графа G, $\widetilde{G}$ — граф, получающийся из G заменой ребра AB на ориентированное ребро $B \to A$ (т е. мудрец A не видит мудреца B, но B видит A). Пусть функция $\widetilde{g}$ на вершинах графа G совпадает с g во всех вершинах, кроме A, и $\widetilde{g}(A) = h(B)g(A)$. Тогда игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ тоже выигрышная. (И тогда, если игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ проигрышная, то и $\langle G, h, g\rangle$ проигрышная.)

3.5. Теорема о подстановке. Пусть $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ и $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — выигрышные игры. Пусть A — произвольная вершина графа G_2. Рассмотрим новый граф G, который получается из G_2 заменой вершины A на граф G_1 (каждая вершина G_1 соединяется новыми ребрами с бывшими соседями вершины A, см. рис. 2). Тогда игра $\langle G, h, g\rangle$ — выигрышная, где

$$h(u) = \begin{cases} h_2(u), & u \in V(G_2) \setminus \{A\},\\ h_1(u)h_2(A), & u \in V(G_1), \end{cases} \qquad g(u) = \begin{cases} g_2(u), & u \in V(G_2) \setminus \{A\},\\ g_1(u)g_2(A), & u \in V(G_1). \end{cases}$$

3.6. Подстановка с сокращением. Пусть $\mathcal{G} = \langle G, h, \star s\rangle$, $\mathcal{G}' = \langle G', h', g'\rangle$ — выигрышные игры. Пусть A — вершина графа G', причем $h'(A) = s$. Пусть $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ — выигрышная игра, получающаяся

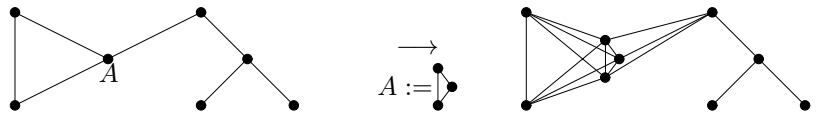


Рис. 2. Подстановка графа на место вершины A.

подстановкой игры $\mathcal{G}$ на место вершины A в игру $\mathcal{G}'$ (как в задаче 3.5). По правилу подстановки для всех подставленных вершин v

$$\widetilde{h}(v) = h(v)h'(A) = s \cdot h(v), \qquad \widetilde{g}(v) = g(v)g'(A) = s \cdot g'(A).$$

Рассмотрим новые функции h^*, g^* на графе $\widetilde{G}$, которые отличаются от $\widetilde{h}$, $\widetilde{g}$ только значениями в подставленных вершинах v, и это отличие — сокращение на s:

$$h^*(v) = h(v), \qquad g^*(v) = g'(A).$$

Тогда игра $\langle \widetilde{G}, h^*, g^* \rangle$ — тоже выигрышная.

3.7. Раздувание вершины. Пусть $\mathcal{G} = \langle G, h, g \rangle$ — выигрышная игра, $A \in V(G)$, $\widetilde{G}$ — граф, получающийся из G подстановкой на место вершины A клики B, состоящей из $g(A)$ вершин. Тогда игра $\langle \widetilde{G}, \widetilde{h}, \widetilde{g} \rangle$ тоже выигрышная, где

$$\widetilde{h}(v) = \begin{cases} h(v), & v \in V(G) \setminus \{A\} \\ h(A), & v \in B, \end{cases} \qquad \widetilde{g}(v) = \begin{cases} g(v), & v \in V(G) \setminus \{A\} \\ 1, & v \in B. \end{cases}$$

4 «Лепестки» и «петунии»

Лепестком будем называть граф, изображенный на рис. 3, вершину лепестка степени $n-1$ (т. е. верхнюю вершину на рис. 3) будем называть *черенком* лепестка.

Будем строить из лепестков более сложные графы. Возьмем два лепестка L_1 и L_2, обозначим в каждом из них одну из вершин буквой v_1 и построим граф $M_2 = L_1 +_{v_1} L_2$. Возьмем граф M_2 и лепесток L_3, обозначим в каждом из них одну из вершин буквой v_2 и рассмотрим граф $M_3 = M_2 +_{v_2} L_3$ и т. д. Графы, которые можно получить с помощью конечного числа таких операций, будем называть *петуниями*.

Петунию будем называть *королевской* петунией (рис. 4), если на каждом шаге ее построения вершина v_i была черенком лепестка L_{i+1}.

4.1. Пусть G — лепесток из n вершин, см. рис. 3, а функция шляпности h задается так: шляпность верхней вершины равна 2, шляпности остальных вершин равны 7. Докажите, что в игре $\langle G, h \rangle$ мудрецы проигрывают.

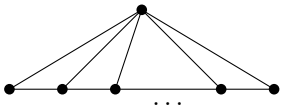


Рис. 3. Лепесток из n вершин

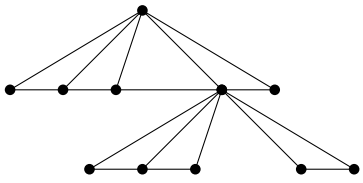


Рис. 4. Королевская петуния

4.2. Пусть G — лепесток из n вершин. Положим $f(s) = s^2 + s$. Докажите, что $\mathrm{HG}_s(G) \leqslant f(f(s))$.

4.3. Пусть M — петуния, h_s — наибольшее натуральное число, для которого игра $\langle M, \star h_s, \star s \rangle$ выигрышная. Докажите, что $h_s \leqslant f(f(f(s)))$.

4.4. a) Докажите, что $\mathrm{HG}_s(G) = 4s(s+1) - 2$, где G — лепесток из n вершин, где n достаточно велико (рис. 3).

b) Докажите это же равенство, если G — королевская петуния с достаточно крупными лепестками.

5 Дополнительные задачи

В серию 1

5.1. Пусть $K_{1,n}$ — граф «звезда», а $h = (h_0, \dots, h_n)$, $g = (g_0, \dots, g_n)$ — произвольные функции количеств шляп и числа попыток, где $1 \leqslant g_i \leqslant h_i$ при всех i, нулевой индекс соответствует центральной вершине графа. Докажите, что существование k, для которого $\langle K_{1,n}, k \cdot h, k \cdot g\rangle$ является выигрышной, равносильно неравенству

$$\frac{g_0}{h_0} \geqslant \prod_{i=1}^{n} \left(1 - \frac{g_i}{h_i}\right).$$

В серию 2

5.2. Пусть h и g натуральные числа, причем $g^2 - 3gh + h^2 < 0$. Докажите, что игра $\langle P_3, \star h, \star g\rangle$ — выигрышная.

Дробным шляпным числом графа G назовем величину $\hat{\mu}(G) = \sup\{\frac{h}{g}\colon$ игра $\langle G, \star h, \star g\rangle$ — выигрышная$\}$.
Как следует из задачи 1.9, $\mathrm{HG}(K_n) = \hat{\mu}(K_n) = n$, $\mathrm{HG}_s(K_n) = sn$. В общем случае, $\hat{\mu}(K_n) \geqslant \frac{1}{s}\mathrm{HG}_s(G) \geqslant \mathrm{HG}(G)$.

5.3. Докажите, что $\hat{\mu}(K_3) = \frac{3+\sqrt{5}}{2}$.

В серию 3

5.4. Пусть $\langle G_2, h_2\rangle$ — проигрышная игра, $H_2 \subset G_2$ — клика в G_2. Пусть G_1 полный граф. Зададим на нем функцию шляпности h_1 так, чтобы выполнялось соотношение

$$\left(\sum_{u \in G_1} \frac{1}{h_1(u)}\right)\left(\prod_{v \in H_2} h_2(v)\right) < 1$$

Пусть G — это граф, получающийся объединением графов G_1 и G_2 и добавлением всех ребер между вершинами G_1 и H_2 (рис. 5). Докажите, что игра $\langle G, h\rangle$ — проигрышная, если

$$h(v) = \begin{cases} h_1(v), & v \in G_1, \\ h_2(v), & v \in G_2. \end{cases}$$

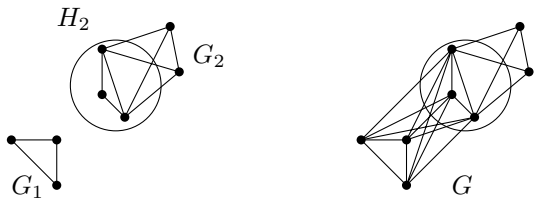


Рис. 5. Пример к задаче 5.4. Число вершин в G_1 и H_2 не обязано совпадать

5.5. Пусть $\mathcal{G} = \langle G, h\rangle$ — проигрышная игра, A — любая вершина графа G. Рассмотрим граф $G' = \langle V', E'\rangle$, получающийся добавлением к графу G новой висячей вершины B: $V' = V \cup \{B\}$, $E' = E \cup \{AB\}$. Тогда мудрецы проигрывают в игре $\langle G', h'\rangle$, где $h'(B) = 2$, $h'(A) = 2h(A) - 1$ и $h'(u) = h(u)$ для остальных вершин $u \in V$.

5.6. Пусть $\mathcal{G} = \langle G, h, g\rangle$ — некоторая игра, $A \in V(G)$ соединена ребрами со всеми остальными вершинами графа G, $h(A) = s + 1$, $g(A) = s$, и $\mathcal{G}' = \langle G \setminus \{A\}, h', (s+1) \cdot g'\rangle$, где $h' = h\Big|_{V(G)\setminus\{A\}}$, $g' = g\Big|_{V(G)\setminus\{A\}}$. Тогда игры $\mathcal{G}$ и $\mathcal{G}'$ эквивалентны (мудрецы выигрывают в $\mathcal{G}$ тогда и только тогда, когда они выигрывают в $\mathcal{G}'$).

Серия 5

5.7. a) Выигрышный граф G содержит «длинный мост» — двузвенный путь ABC, при удалении которого граф распадается на две компоненты: G_1 (содержащую вершину A) и G_2 (содержащую вершину C). Пусть шляпность вершины B равна 5. Докажите, что хотя бы одна из игр $\langle G_1, h\big|_{G_1}\rangle$, $\langle G_2, h\big|_{G_2}\rangle$ выигрышная.

b) Пусть граф $\widetilde{G}$ получен подразбиением произвольного графа G (т. е. каждое ребро графа G заменили на двузвенный путь). Докажите, что игра $\langle \widetilde{G}, \star 5\rangle$ — проигрышная.

5.8. Пусть $\mathcal{G} = \langle G, h\rangle$ — выигрышная игра, причем максимальная в следующем смысле: при увеличении функции шляпности в любой вершине мудрецы проигрывают и, кроме того, с функцией шляпности h мудрецы не могут выиграть ни на каком подграфе графа G. Допустим, что граф G содержит ребро-мост AB. Докажите, что игра $\mathcal{G}$ представима в виде произведения игр.

5.9. Мудрецы A и B имеют по одной попытке угадывания, видят друг друга и всех остальных мудрецов в графе (а те видят их), $h(A) = 2$, $h(B) = 3$. Докажите, что если заменить этих двух мудрецов на одного мудреца C, который видит остальных, а остальные его, и при этом $h(C) = 6$, $g(C) = 5$, то результат игры не изменится.

5.10. Даны натуральные числа s и d. Пусть G — произвольный граф, вершины которого разбиты на два множества $V(G) = A \cup B$, причем каждая вершина из A имеет не более d соседей из B. Докажите, что $\mathrm{HG}_s(G) \leqslant \mathrm{HG}_{s'}(G[A])$, где $s' = s(\mathrm{HG}_s(G[B])+1)^d$, а $G[A]$ и $G[B]$ — индуцированные подграфы на множествах A и B.

Покрасьте мою шляпу в 3,5 цвета!

К. Кохась, А. Латышев

Задачу представляют: О. Бурсиан, Д. Кохась Д, К. Кохась, В. Ретинский

1 Знакомьтесь: игра в шляпы

Пусть дан неориентированный граф G, в каждой вершине которого находится один мудрец и один сундук со шляпами разного цвета. Мудрецы знакомы друг с другом, граф G, расположение мудрецов по вершинам графа и все цвета шляп в сундуках зафиксированы и известны всем. В частности, каждый мудрец понимает, в какой вершине находится каждый из остальных мудрецов. Судья проводит с мудрецами следующий тест. Он надевает каждому мудрецу шляпу из его сундука. Каждый мудрец видит только шляпы мудрецов, находящихся в соседних вершинах графа, но не видит своей шляпы и не знает ее цвета. Мудрецы не общаются во время теста. По команде судьи мудрецы одновременно записывают каждый на своей бумажке названия нескольких цветов (сколько именно цветов должен указывать мудрец, определяется дополнительным правилом). Считается, что мудрецы успешно прошли тест = «выиграли», если хотя бы один из них угадал хотя бы в одной из своих попыток.

Перед тестом мудрецам сообщили правила теста и дали возможность устроить совещание, на котором они должны определить публичную стратегию. Публичность означает, что все, включая судью, знают ее. Стратегия мудрецов должна быть детерминированной — каждый мудрец должен записывать на бумажку цвета, исходя только из того, какие цвета он видит у соседей. Будем говорить, что стратегия выигрышная, если при любой раскладке шляп хотя бы один мудрец угадает цвет надетой на него шляпы, т. е. упомянет этот цвет в своем списке. Также будем говорить, что мудрецы выигрывают, если они имеют выигрышную стратегию, и проигрывают, если не имеют.

Таким образом, игра в шляпы не есть игра в привычном понимании этого слова. Она длится всего один ход. Вот несколько задач на этот сюжет.

1.1. Каждому из двух мудрецов надевают шляпу белого, синего, красного или зеленого цвета. Каждый из них видит шляпу другого, но не видит свою. Они должны одновременно попытаться угадать цвет своей шляпы, написав на своей бумажке два цвета. Докажите, что мудрецы могут заранее договориться действовать так, чтобы хотя бы один из них угадал.

1.2. Каждому из двух мудрецов надевают шляпу одного из пяти возможных цветов. Каждый из них видит шляпу другого, но не видит свою. Они должны одновременно попытаться угадать цвет своей шляпы, написав на бумажке: первый — какие-то два цвета, второй какие-то три цвета. Докажите, что мудрецы могут заранее договориться действовать так, чтобы хотя бы один из них угадал.

1.3. Пять мудрецов стоят по кругу возле непрозрачного баобаба. Шах надел на голову каждого из мудрецов красную, синюю, желтую или зеленую шляпу. Мудрец не знает цвет своей шляпы и видит только двух соседних по кругу мудрецов. Не общаясь, мудрецы одновременно должны высказать предположение о цвете своей шляпы. При этом они боятся оказаться слишком удачливыми. Как им следует действовать, чтобы при любом раскладе шляп цвет своей шляпы угадало не более двух мудрецов?

1.4. Султан устроил экзамен шести придворным мудрецам. По правилу экзамена султан размещает 5 мудрецов в 5 ям, расположенных по кругу, а шестого мудреца сажает на вышку в центре круга. На лбу у каждого из первых пяти мудрецов султан пишет число 1, 2 или 3; на лбу у центрального мудреца султан пишет число от 1 до 243. Мудрец на вышке видит числа на всех остальных мудрецах, а те видят его число (но не видят друг друга). Все мудрецы должны одновременно попытаться угадать свои числа: для этого мудрецы в яме должны назвать по два числа, а мудрец на вышке — одно. Султан заранее объяснил мудрецам правила экзамена и дал им время посовещаться до начала экзамена. Могут ли мудрецы действовать так, чтобы хотя бы один из них заведомо угадал свое число?

Мы будем отождествлять вершину графа G и мудреца, который в ней находится. Будем считать, что цвета пронумерованы числами 0, 1, 2, 3, ... и что в сундуке мудреца v лежат шляпы с цветами от 0 до некоторого числа $h(v) - 1$.

Игрой в шляпы назовем тройку $\langle G, h, g\rangle$, где $G = \langle V, E\rangle$ — граф, $h\colon V \to \mathbb{N}$ — функция, сопоставляющая вершине количество (цветов) шляп, лежащих в сундуке в этой вершине, $g\colon V \to \mathbb{N}$ — функция, показывающая, сколько попыток угадывания имеет каждый мудрец. Функцию h мы будем называть «шляпностью», а g — функцией угадывания или числом попыток. Если h — натуральное число, символом $\star h$ будем обозначать функцию на V, принимающую постоянное значение h. Вместо обозначения $\langle G, h, \star 1\rangle$ мы будем использовать более короткое обозначение $\langle G, h\rangle$.

1.5. Докажите, что если игра $\langle G, h, g\rangle$ выигрышная, то для всех натуральных k игра $\langle G, k \cdot h, k \cdot g\rangle$ тоже выигрышная.

1.6. Дана игра $\langle G, h, g\rangle$. Пусть $K \subset G$ — антиклика (множество вершин, между которыми не проведено ни одного ребра) и для всех $v \in K$ $h(v) > g(v)$. Докажите, что существует расклад шляп, для которого ни один мудрец из K не угадывает.

1.7. Пусть h и g натуральные числа, $G = \langle G, \star h, \star g\rangle$ — выигрышная игра, $r' \leqslant \frac{h}{g}$ — рациональное число. Докажите, что существуют натуральные числа h' и g', для которых $\frac{h'}{g'} = r'$ и игра $\langle G, \star h', \star g'\rangle$ — выигрышная.

1.8. Сформулируйте и докажите аналог предыдущего утверждения для непостоянных функций шляпности и угадывания.

1.9. Обозначим через K_n полный граф на n вершинах. Докажите, что в игре $\langle K_n, h, g\rangle$ мудрецы выигрывают тогда и только тогда, когда $\sum\limits_{v \in K_n} \frac{g(v)}{h(v)} \geqslant 1$.

2 Пути и деревья

Теория игры в шляпы на полном графе из трех вершин исчерпывается утверждением задачи 1.9. Рассмотрим игру на более простом графе – пути P_3.

2.1. Докажите, что в игре $\langle P_3, \star 3, \star 1\rangle$ мудрецы проигрывают.

2.2. а) Докажите, что игра $\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{5}}{\bullet}$ — выигрышная (числитель дроби возле вершины обозначает количество попыток, а знаменатель — шляпность).

б) Докажите, что игра $\overset{\frac{3}{11}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{5}}{\bullet}$ — проигрышная.

в) Докажите, что игра $\overset{\frac{s}{t(s)}}{\bullet}\!\!-\!\!\overset{\frac{s}{t(s)}}{\bullet}\!\!-\!\!\overset{\frac{s}{t(s)}}{\bullet}$, где $t(s) = s^2 + s + 1$, — проигрышная.

Пусть дан граф G и натуральное число s. Наибольшее число шляп h, для которого игра $\langle G, \star h, \star s\rangle$ выигрышная, называется s-шляпным числом графа и обозначается $\mathrm{HG}_s(G)$. При $s = 1$ мы называем это число просто шляпным числом и обозначаем $\mathrm{HG}(G)$.

2.3. Докажите, что для любых натуральных n и s игра $\underset{A}{\overset{\frac{s}{2s}}{\bullet}}\!\!-\!\!\bullet\!\!-\!\!\bullet\cdots$ на пути P_n проигрышная. Все вершины, кроме крайней вершины A, имеют шляпность $4s - 1$ и s попыток.

2.4. Докажите, что существуют пути P_n, для которых $\mathrm{HG}_2(P_n) = 6$, $\mathrm{HG}_3(P_n) = 10$, $\mathrm{HG}_4(P_n) = 14$.

2.5. Докажите, что для любого натурального s игра $\langle P_n, \star(4s - 2), \star s\rangle$ выигрышная при $n \geqslant 2s$.

2.6. а) Пусть $t(s) = s^2 + s + 1$. Докажите, что для любого дерева T игра $\langle T, \star t(s), \star s\rangle$ проигрышная.

b) Пусть $K_{1,n}$ — граф «звезда» (дерево, состоящее из корня и n листьев). Докажите, что при больших n игра $\langle K_{1,n}, \star(s^2 + s), \star s\rangle$ — выигрышная.

c) Докажите, что для любого натурального h существует такое натуральное n, что игра на графе $K_{1,n}$ — выигрышная, если шляпности всех периферийных мудрецов равны 3 и все они имеют по одной попытке угадывания, а шляпность центрального мудреца равна h и у него две попытки.

3 Конструкторы

3.1. Пусть $\langle G, h, g\rangle$ — выигрышная игра, A_1 и A_2 — вершины графа G, не соединенные ребром, причем $h(A_1) = h(A_2)$, $\widetilde{G}$ — граф, получающийся из G склеиванием вершин A_1 и A_2 в одну вершину A. Пусть функции $\widetilde{h}$, $\widetilde{g}$ на вершинах графа $\widetilde{G}$ совпадают с h и g во всех вершинах, кроме A_1 и A_2, и $\widetilde{h}(A) = h(A_1)$, $\widetilde{g}(A) = g(A_1) + g(A_2)$. Тогда игра $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ тоже выигрышная. (И тогда, если игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ проигрышная, то и $\langle G, h, g\rangle$ проигрышная.)

Пусть $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$, $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — две игры, такие что $V_1 \cap V_2 = \{v\}$. Пусть $G = G_1 +_v G_2$ — объединение графов G_1 и G_2, в котором обе вершины v объединены в одну вершину. Зададим функции $h, g\colon V_1 \cup V_2 \to \mathbb{N}$:

$$h(u) = \begin{cases} h_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ h_1(v)h_2(v), & u = v, \end{cases} \qquad g(u) = \begin{cases} g_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ g_1(v)g_2(v), & u = v. \end{cases}$$

Игру $\mathcal{G} = \langle G, h, g\rangle$ будем обозначать $\mathcal{G}_1 \times_v \mathcal{G}_2$ (рис. 1).

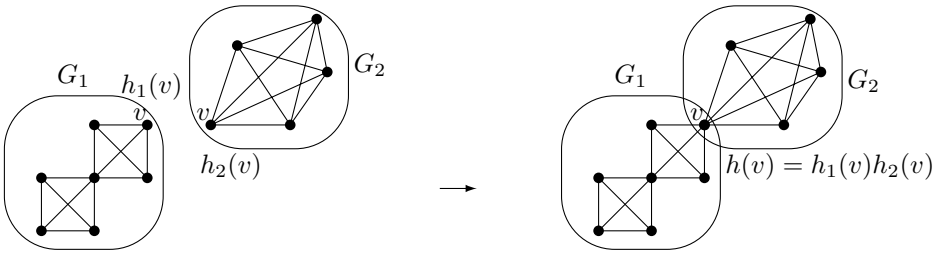


Рис. 1. Игра $G_1 \times_v G_2$

3.2. Теорема о произведении. Если мудрецы выигрывают в играх $\mathcal{G}_1$ и $\mathcal{G}_2$, то они выигрывают и в игре $\mathcal{G}_1 \times_v \mathcal{G}_2$.

3.3. Пусть $G = G_1 +_A G_2$, где G_1 и G_2 — графы, у которых $V(G_1) \cap V(G_2) = \{A\}$, а игры $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ и $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — проигрышные, и при этом

$$g_1(A) = g_2(A) = s, \qquad h_1(A) \geqslant h_2(A) = s + 1.$$

Тогда игра $\mathcal{G} = \langle G_1 +_A G_2, h, g\rangle$ — проигрышная, где

$$h(x) = \begin{cases} h_i(x), & x \in V_i \setminus \{A\},\ (i = 1, 2),\\ h_1(A), & x = A, \end{cases} \qquad g(x) = \begin{cases} g_i(x), & x \in V_i \setminus \{A\},\ (i = 1, 2),\\ s, & x = A. \end{cases}$$

3.4. Удаление полуребра. Пусть $\langle G, h, g\rangle$ — выигрышная игра, AB — ребро графа G, $\widetilde{G}$ — граф, получающийся из G заменой ребра AB на ориентированное ребро $B \to A$ (т е. мудрец A не видит мудреца B, но B видит A). Пусть функция $\widetilde{g}$ на вершинах графа G совпадает с g во всех вершинах, кроме A, и $\widetilde{g}(A) = h(B)g(A)$. Тогда игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ тоже выигрышная. (И тогда, если игра $\langle\widetilde{G}, h, \widetilde{g}\rangle$ проигрышная, то и $\langle G, h, g\rangle$ проигрышная.)

3.5. Теорема о подстановке. Пусть $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ и $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ — выигрышные игры. Пусть A — произвольная вершина графа G_2. Рассмотрим новый граф G, который получается из G_2 заменой вершины A на граф G_1 (каждая вершина G_1 соединяется новыми ребрами с бывшими соседями вершины A, см. рис. 2). Тогда игра $\langle G, h, g\rangle$ — выигрышная, где

$$h(u) = \begin{cases} h_2(u), & u \in V(G_2) \setminus \{A\},\\ h_1(u)h_2(A), & u \in V(G_1), \end{cases} \qquad g(u) = \begin{cases} g_2(u), & u \in V(G_2) \setminus \{A\},\\ g_1(u)g_2(A), & u \in V(G_1). \end{cases}$$

3.6. Подстановка с сокращением. Пусть $\mathcal{G} = \langle G, h, \star s\rangle$, $\mathcal{G}' = \langle G', h', g'\rangle$ — выигрышные игры. Пусть A — вершина графа G', причем $h'(A) = s$. Пусть $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ — выигрышная игра, получающаяся

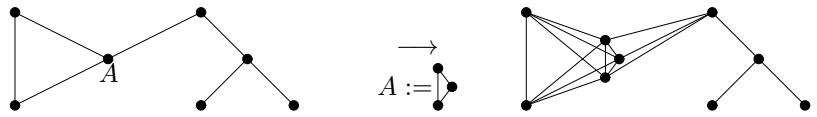


Рис. 2. Подстановка графа на место вершины A.

подстановкой игры $\mathcal{G}$ на место вершины A в игру $\mathcal{G}'$ (как в задаче 3.5). По правилу подстановки для всех подставленных вершин v

$$\widetilde{h}(v) = h(v)h'(A) = s \cdot h(v), \qquad \widetilde{g}(v) = g(v)g'(A) = s \cdot g'(A).$$

Рассмотрим новые функции h^*, g^* на графе $\widetilde{G}$, которые отличаются от $\widetilde{h}$, $\widetilde{g}$ только значениями в подставленных вершинах v, и это отличие — сокращение на s:

$$h^*(v) = h(v), \qquad g^*(v) = g'(A).$$

Тогда игра $\langle \widetilde{G}, h^*, g^* \rangle$ — тоже выигрышная.

3.7. Раздувание вершины. Пусть $\mathcal{G} = \langle G, h, g \rangle$ — выигрышная игра, $A \in V(G)$, $\widetilde{G}$ — граф, получающийся из G подстановкой на место вершины A клики B, состоящей из $g(A)$ вершин. Тогда игра $\langle \widetilde{G}, \widetilde{h}, \widetilde{g} \rangle$ тоже выигрышная, где

$$\widetilde{h}(v) = \begin{cases} h(v), & v \in V(G) \setminus \{A\} \\ h(A), & v \in B, \end{cases} \qquad \widetilde{g}(v) = \begin{cases} g(v), & v \in V(G) \setminus \{A\} \\ 1, & v \in B. \end{cases}$$

4 «Лепестки» и «петунии»

Лепестком будем называть граф, изображенный на рис. 3, вершину лепестка степени $n-1$ (т. е. верхнюю вершину на рис. 3) будем называть *черенком* лепестка.

Будем строить из лепестков более сложные графы. Возьмем два лепестка L_1 и L_2, обозначим в каждом из них одну из вершин буквой v_1 и построим граф $M_2 = L_1 +_{v_1} L_2$. Возьмем граф M_2 и лепесток L_3, обозначим в каждом из них одну из вершин буквой v_2 и рассмотрим граф $M_3 = M_2 +_{v_2} L_3$ и т. д. Графы, которые можно получить с помощью конечного числа таких операций, будем называть *петуниями*.

Петунию будем называть *королевской* петунией (рис. 4), если на каждом шаге ее построения вершина v_i была черенком лепестка L_{i+1}.

4.1. Пусть G — лепесток из n вершин, см. рис. 3, а функция шляпности h задается так: шляпность верхней вершины равна 2, шляпности остальных вершин равны 7. Докажите, что в игре $\langle G, h \rangle$ мудрецы проигрывают.

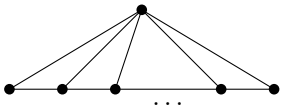


Рис. 3. Лепесток из n вершин

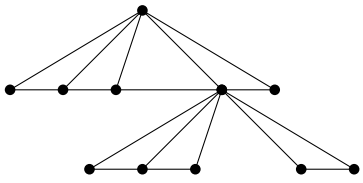


Рис. 4. Королевская петуния

4.2. Пусть G — лепесток из n вершин. Положим $f(s) = s^2 + s$. Докажите, что $\mathrm{HG}_s(G) \leqslant f(f(s))$.

4.3. Пусть M — петуния, h_s — наибольшее натуральное число, для которого игра $\langle M, \star h_s, \star s \rangle$ выигрышная. Докажите, что $h_s \leqslant f(f(f(s)))$.

4.4. a) Докажите, что $\mathrm{HG}_s(G) = 4s(s+1) - 2$, где G — лепесток из n вершин, где n достаточно велико (рис. 3).

b) Докажите это же равенство, если G — королевская петуния с достаточно крупными лепестками.

5 Дополнительные задачи

В серию 1

5.1. Пусть $K_{1,n}$ — граф «звезда», а $h = (h_0, \dots, h_n)$, $g = (g_0, \dots, g_n)$ — произвольные функции количеств шляп и числа попыток, где $1 \leqslant g_i \leqslant h_i$ при всех i, нулевой индекс соответствует центральной вершине графа. Докажите, что существование k, для которого $\langle K_{1,n}, k \cdot h, k \cdot g\rangle$ является выигрышной, равносильно неравенству

$$\frac{g_0}{h_0} \geqslant \prod_{i=1}^{n} \left(1 - \frac{g_i}{h_i}\right).$$

В серию 2

5.2. Пусть h и g натуральные числа, причем $g^2 - 3gh + h^2 < 0$. Докажите, что игра $\langle P_3, \star h, \star g\rangle$ — выигрышная.

Дробным шляпным числом графа G назовем величину $\hat{\mu}(G) = \sup\{\frac{h}{g}\colon$ игра $\langle G, \star h, \star g\rangle$ — выигрышная$\}$.
Как следует из задачи 1.9, $\mathrm{HG}(K_n) = \hat{\mu}(K_n) = n$, $\mathrm{HG}_s(K_n) = sn$. В общем случае, $\hat{\mu}(K_n) \geqslant \frac{1}{s}\mathrm{HG}_s(G) \geqslant \mathrm{HG}(G)$.

5.3. Докажите, что $\hat{\mu}(K_3) = \frac{3+\sqrt{5}}{2}$.

В серию 3

5.4. Пусть $\langle G_2, h_2\rangle$ — проигрышная игра, $H_2 \subset G_2$ — клика в G_2. Пусть G_1 полный граф. Зададим на нем функцию шляпности h_1 так, чтобы выполнялось соотношение

$$\left(\sum_{u \in G_1} \frac{1}{h_1(u)}\right)\left(\prod_{v \in H_2} h_2(v)\right) < 1$$

Пусть G — это граф, получающийся объединением графов G_1 и G_2 и добавлением всех ребер между вершинами G_1 и H_2 (рис. 5). Докажите, что игра $\langle G, h\rangle$ — проигрышная, если

$$h(v) = \begin{cases} h_1(v), & v \in G_1, \\ h_2(v), & v \in G_2. \end{cases}$$

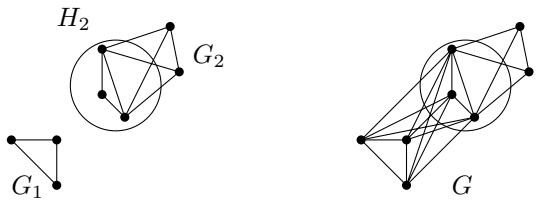


Рис. 5. Пример к задаче 5.4. Число вершин в G_1 и H_2 не обязано совпадать

5.5. Пусть $\mathcal{G} = \langle G, h\rangle$ — проигрышная игра, A — любая вершина графа G. Рассмотрим граф $G' = \langle V', E'\rangle$, получающийся добавлением к графу G новой висячей вершины B: $V' = V \cup \{B\}$, $E' = E \cup \{AB\}$. Тогда мудрецы проигрывают в игре $\langle G', h'\rangle$, где $h'(B) = 2$, $h'(A) = 2h(A) - 1$ и $h'(u) = h(u)$ для остальных вершин $u \in V$.

5.6. Пусть $\mathcal{G} = \langle G, h, g\rangle$ — некоторая игра, $A \in V(G)$ соединена ребрами со всеми остальными вершинами графа G, $h(A) = s + 1$, $g(A) = s$, и $\mathcal{G}' = \langle G \setminus \{A\}, h', (s+1) \cdot g'\rangle$, где $h' = h\Big|_{V(G)\setminus\{A\}}$, $g' = g\Big|_{V(G)\setminus\{A\}}$. Тогда игры $\mathcal{G}$ и $\mathcal{G}'$ эквивалентны (мудрецы выигрывают в $\mathcal{G}$ тогда и только тогда, когда они выигрывают в $\mathcal{G}'$).

Серия 5

5.7. a) Выигрышный граф G содержит «длинный мост» — двузвенный путь ABC, при удалении которого граф распадается на две компоненты: G_1 (содержащую вершину A) и G_2 (содержащую вершину C). Пусть шляпность вершины B равна 5. Докажите, что хотя бы одна из игр $\langle G_1, h\big|_{G_1}\rangle$, $\langle G_2, h\big|_{G_2}\rangle$ выигрышная.

b) Пусть граф $\widetilde{G}$ получен подразбиением произвольного графа G (т. е. каждое ребро графа G заменили на двузвенный путь). Докажите, что игра $\langle \widetilde{G}, \star 5\rangle$ — проигрышная.

5.8. Пусть $\mathcal{G} = \langle G, h\rangle$ — выигрышная игра, причем максимальная в следующем смысле: при увеличении функции шляпности в любой вершине мудрецы проигрывают и, кроме того, с функцией шляпности h мудрецы не могут выиграть ни на каком подграфе графа G. Допустим, что граф G содержит ребро-мост AB. Докажите, что игра $\mathcal{G}$ представима в виде произведения игр.

5.9. Мудрецы A и B имеют по одной попытке угадывания, видят друг друга и всех остальных мудрецов в графе (а те видят их), $h(A) = 2$, $h(B) = 3$. Докажите, что если заменить этих двух мудрецов на одного мудреца C, который видит остальных, а остальные его, и при этом $h(C) = 6$, $g(C) = 5$, то результат игры не изменится.

5.10. Даны натуральные числа s и d. Пусть G — произвольный граф, вершины которого разбиты на два множества $V(G) = A \cup B$, причем каждая вершина из A имеет не более d соседей из B. Докажите, что $\mathrm{HG}_s(G) \leqslant \mathrm{HG}_{s'}(G[A])$, где $s' = s(\mathrm{HG}_s(G[B])+1)^d$, а $G[A]$ и $G[B]$ — индуцированные подграфы на множествах A и B.

Решения

1.1. Назовём белый и красный цвета светлыми, а синий и зелёный — тёмными. Тогда пусть первый назовёт оба тёмных цвета, если на втором надет светлый, и наоборот; а второй — назовёт оба светлых цвета, если на первом надет светлый, и наоборот. Нетрудно понять, что в данной стратегии хотя бы один из мудрецов угадывает свой цвет.

1.2. Перенумерум цвета шляп от 1 до 5. Тогда пусть первый игрок назовёт цвета в предположении, что сумма номеров на шляпах первого и второго даёт остаток 0 или 1 при делении на 5, а второй — в предположении, что эта же сумма даёт остаток 2, 3 или 4 при делении на 5. Так как реальная сумма существует и даёт какой-то остаток, то мудрец с верным предположением угадает свой цвет.

1.3. Сначала напомним, как играть в игру, если мудрецов всего два, шляпы могут быть лишь двух цветов (обозначим их 0 и 1) и требуется, чтобы обязательно кто-то угадал. Стратегия здесь такая — один мудрец (назовем его уравнитель) проверяет гипотезу «цвета шляп одинаковы», другой (различитель) — «цвета шляп различны». Отметим, что по этой стратегии для любого расклада шляп один из мудрецов угадает, а другой нет.

Введем граф видимости — мудрецы это вершины, пары соседних мудрецов — ребра, по условию этот граф — цикл из пяти вершин. Обозначим ребра a, b, c, d, e. Будем считать, что цвет шляпы мудреца – это двузначное бинарное число: 00, 01, 10 или 11, причем записывая это число, будем помечать его разряды метками ребер, инцидентных вершине, где сидит мудрец. Например, если из вершины выходят ребра a и b, то мы подписываем снизу под одним из разрядов «a», а под другим «b» (под каким разрядом какая метка — неважно, главное, чтобы все мудрецы пользовались этими пометками единообразно).

В начале для каждого ребра мудрецы договариваются, кто на этом ребре уравнитель, а кто различитель. При угадывании на каждом ребре x происходит следующее: каждый мудрец на этом ребре смотрит лишь на разряд x в цвете своего соседа и вычисляет цвет своего разряда x в соответствии со своей ролью на этом ребре. Таким образом, каждый мудрец, посмотрев налево и направо, вычисляет оба разряда для цвета своей шляпы и называет полученный цвет в качестве ответа.

Очевидно, мудрец угадает цвет своей шляпы, только если он правильно угадал оба бита. Поскольку граф содержит лишь 5 ребер, лишь 5 битов были угаданы правильно, и следовательно, не более двух мудрецов верно указали цвет своей шляпы.

1.4. Сопоставим каждому цвету центрального мудреца последовательность из 5 цифр, каждая из которых — 1, 2 или 3. Стратегия i-го мудреца в яме: посмотреть на i-ю цифру центрального мудреца и назвать 2 остальные. Стратегия центрального: назвать цвет, i-я цифра которого равна цифре i-го мудреца из ямы. Тогда если никакой мудрец из ямы не угадал, то центральный верно назовёт свой цвет.

1.5. Для каждого мудреца v рассмотрим $k \cdot h(v)$ цветов шляп и разобьём их на $h(v)$ групп по k цветов, которые мы будем называть мегацветами. Тогда в игре $\langle G, k \cdot h, k \cdot g\rangle$ каждый мудрец v может понять мегацвета всех своих соседей, и, согласно стратегии для игры $\langle G, h, g\rangle$, назвать $g(v)$ своих мегацветов. Но эти $g(v)$ мегацветов соответствуют $k \cdot g(v)$ обычным цветам. Нетрудно поверить, что если стратегия для игры $\langle G, h, g\rangle$ была выигрышной, то полученная стратегия также будет выигрышной.

1.6. Дадим произвольные шляпы мудрецам не из K. Тогда для мудрецов из K станет ясно, какой ответ дает каждый из них по своей стратегии. Осталось каждому дать такую шляпу, чтобы он не угадал.

1.7. Пусть $r' = \frac{p}{q}$. Если $G = \langle G, \star h, \star g\rangle$ — выигрышная, то игра $\langle G, \star ph, \star pg\rangle$ — тоже выигрышная. А так как $\frac{p}{q} \leqslant \frac{h}{g}$, то $pg \leqslant qh$, откуда игра $\langle G, \star ph, \star qh\rangle$ — также выигрышная, так как увеличение количества попыток работающую стратегию не портит. Тогда $h' = ph$, $q' = qh$ являются искомыми.

1.8. Пусть $G = \langle G, h, g\rangle$ — выигрышная игра, $r'\colon V \to \mathbb{Q}$ — функция, удовлетворяющая условию $0 < r'(v) \leqslant \frac{h(v)}{g(v)}$ для каждого v. Докажите, что существуют функции h' и g', для которых $\frac{h'(v)}{g'(v)} = r'(v)$ для каждого v и игра $\langle G, h', g'\rangle$ — выигрышная.

Доказательство. Пусть $r'(v) = \frac{p(v)}{q(v)}$. Положим $P = \prod\limits_v p(v)$. Тогда по утверждению задачи 1.5 игра $\langle G, P \cdot h, P \cdot g\rangle$ — выигрышная. Так как $\frac{p(v)}{q(v)} \leqslant \frac{h(v)}{g(v)}$, то, увеличив количество попыток в некоторых вершинах, мы получаем, что игра $\left\langle G, P \cdot h, \frac{P}{p} \cdot qh\right\rangle$ — выигрышная. Следовательно, $h' = P \cdot h$, $g'(v) = \frac{P}{p(v)} \cdot q(v)h(v)$ являются искомыми.

1.9. *Необходимость.* Заметим, что мудрец v угадывает в $\frac{g(v)}{h(v)}$ доле расстановок всех шляп. А так как в каждой расстановке должен угадать хотя бы один мудрец, то и сумма этих выражений должна быть не меньше одного.

Достаточность. Покажем, что если неравенство выполнено, то у мудрецов есть выигрышная стратегия.

Пусть $H = \prod\limits_v h(v)$. Закодируем цвета шляп числами от 0 до $H - 1$: если мудрец v получает шляпу цвета $i \in \{0, 1, \ldots, h(v) - 1\}$, сопоставим ей «номер» — остаток $\frac{iH}{h(v)}$ по модулю H. Таким образом, возможным шляпам мудреца v сопоставлены остатки

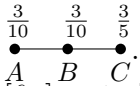
$$0, \quad \frac{H}{h(v)}, \quad \frac{2H}{h(v)}, \quad \ldots, \quad \frac{(h(v)-1)H}{h(v)} \pmod H. \qquad (*)$$

Когда мудрецам будут выданы шляпы, подсчитаем величину S — сумму номеров всех выданных шляп по модулю H. Мудрецы не знают значения S, но каждый мудрец v может вычислить величину S_v — сумму номеров всех шляп, выданных остальным мудрецам, по модулю H.

Стратегия мудрецов состоит в следующем: каждому мудрецу v дадим промежуток $[a_v, b_v)$ длины $\frac{Hg(v)}{h(v)}$, содержащий $\frac{Hg(v)}{h(v)}$ последовательных остатков по модулю H, и пусть мудрец v проверяет гипотезу $S \in [a_v, b_v)$. Для этого он решает «неравенство»: находит, при каких x выполняется включение $S_v + x \in [a_v, b_v)$. Решив эту задачу, он получит $\frac{Hg(v)}{h(v)}$ последовательных вариантов значения остатка x, но номеров своей шляпы, т. е. остатков из списка $(*)$, среди них будет лишь $g(v)$. Тогда мудрец v назовет $g(v)$ соответствующих цветов.

Данное неравенство равносильно тому, что сумма длин всех отрезков не меньше H. Если это выполнено, то, очевидно, мы можем назначить каждому мудрецу по отрезку так, чтобы каждый остаток по модулю H принадлежал хотя бы одному из отрезков. Это гарантирует победу мудрецов: какой бы ни оказалась сумма шляп, хотя бы один из мудрецов сделает правильное предположение и угадает свой цвет.

2.1. Мудрецы не смогут выиграть даже в игре $\langle P_3, \star 3k, \star k\rangle$. Это следует из неравенства задачи 5.1.

2.2. а) Обозначим мудрецов через A, B и C: 

. Предъявим выигрышную стратегию мудрецов. Пусть мудрец C назовет цвета $[\frac{c_B}{2}]$, $[\frac{c_B}{2}] + 1$, $[\frac{c_B}{2}] + 2 \bmod 5$, а мудрец A — c_B, $c_B + 3$, $c_B + 6 \bmod 10$. Мудрец B, посмотрев на соседей, догадывается, что они оба не угадывают, только если

$$c_B \notin S = \{c_A, c_A - 3, c_A - 6, 2c_c, 2c_C + 1, 2c_C + 2, 2c_C + 3, 2c_C + 4, 2c_C + 5\}.$$

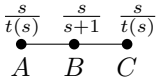
Осталось заметить, что для остатков по модулю 10 включение

$$\{c_A, c_A - 3, c_A - 6\} \subset \{2c_c, 2c_C + 1, 2c_C + 2, 2c_C + 3, 2c_C + 4, 2c_C + 5\}$$

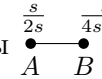
невозможно ни при каких c_A и c_C. Поэтому множество S содержит не менее 7 элементов, и мудрец B сможет назвать в своем ответе три (или менее) не входящих в него остатка.

б) Для каждого возможного цвета c_B мудрец A называет три своих возможных цвета, т.е. он называет 30 ответов из 11-элементного множества цветов шляпы мудреца A. Значит, какой-то

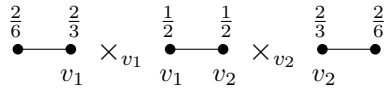
цвет он называет 1 или 2 раза. Дадим мудрецу A шляпу этого цвета. Тогда мудрец B догадается, какие 8 возможных цветов шляпы должны у него быть, чтобы мудрец A не угадал. Но заметим, что игра  проигрышная, а любая стратегия, которой пользуются наши мудрецы в возникшей ситуации, сразу редуцируется к стратегии в этой проигрышной игре.

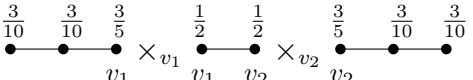
в) Достаточно проверить, что игра  проигрышная. Применим для вершины B утверждение конструктора «удаление половины ребра» (задача 3.4), сделав эту вершину невидимой для A и C. В результате вершины A и C никого не видят, имеют шляпность s^2+s+1 и s^2+s попыток угадывания. Значит, судья может дать им такую шляпу, что они не угадают. После этого стратегия мудреца B полностью определена, он имеет шляпность $s+1$ и s попыток угадывания, поэтому он тоже не угадает.

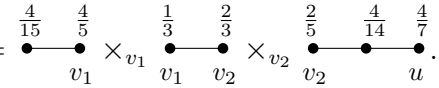
Другое решение получится, если применить стандартные «вероятностные» соображения: количество раскладов шляп, для которых мудрец v угадывает, не превосходит долю $g(v)/h(v)$ от общего числа раскладов. Осталось заметить, что для нашего графа $\frac{3s}{s^2+s+1}<1$ при $s>1$.

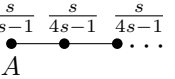
2.3. Для каждого натурального s докажем утверждение индукцией по n. База $n=1$, т. е. проигрышность игры  следует из утверждения задачи 1.9.

Переход. Рассмотрим три крайние вершины A, B, C. Рассмотрим всевозможные назначения цвета шляпы мудрецу B. Мудрец A называет в совокупности $s(4s-1)$ цветов из множества $\{0,1,\dots,2s-1\}$. Значит, какой-то цвет c_A встречается в его ответах не более $[\frac{s(4s-1)}{2s}]=2s-1$ раз. Выдадим мудрецу A шляпу этого цвета. Мудрец B видит шляпу c_A и знает, для каких $2s-1$ цветов его шляпы мудрец A назовет цвет c_A. Поэтому мудрец B может считать, что цвет его шляпы берется из множества C_B, состоящего из $4s-1-(2s-1)=2s$ цветов. В этот момент чертик объявляет, что построит расклад шляп на оставшемся графе, выдав мудрецу B какой-то цвет из C_B, и сообщает остальным мудрецам, что это за множество цветов. Тогда на оставшемся графе происходит игра из индукционного предположения.

2.4. Неравенство $\mathrm{HG}_2(P_4)\geqslant 6$ выполняется в силу того, что игра  выигрышная.

Неравенство $\mathrm{HG}_3(P_6)\geqslant 10$ выполняется в силу того, что игра  выигрышная (множители по краям выигрышные о утверждению задачи 2.2).

Наконец, неравенство $\mathrm{HG}_4(P_{10})\geqslant 14$ выполняется в силу того, что игра $G(u)\times_u$  $\times_w G(w)$ выигрышная, где $G(u)=$  .

В силу утверждения задачи 2.3 любая игра вида  проигрышная (по сравнению с задачей 2.3 здесь увеличена шляпность вершины A). При $s=2$, 3, 4 это дает, кстати, при всех n неравенства $\mathrm{HG}_2(P_n)\leqslant 6$, $\mathrm{HG}_3(P_n)\leqslant 10$, $\mathrm{HG}_4(P_n)\leqslant 14$.

2.5. Рассмотрим на графе P_s функцию шляпности h:

$$h(v_i)=\begin{cases}4s-2 & \text{при } 1\leqslant i<s,\\ 2s-1 & \text{при } i=s.\end{cases}$$

Для доказательства утверждения задачи достаточно проверить, что игра $\langle P_s,h,\star s\rangle$ выигрышная. Чтобы предъявить стратегию мудрецов, мы докажем вспомогательное утверждение — теорему об игре с подсказкой.

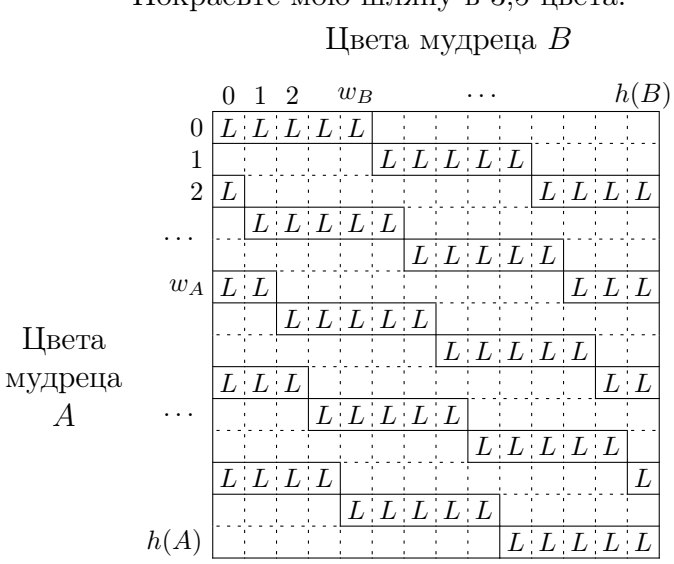


Рис. 6. Стратегия мудреца A. Здесь $h(A) = 14$, $h(B) = 14$, $w_A = 6$, $w_B = 5$. В конструкции таблицы это не требуется, но для полноты картины можно считать, что $g(A) = 4$, $g(B) = 4$.

Пусть игра $\mathcal{G} = \langle G, h, g\rangle$ является выигрышной при условии, что во время игры осуществляется следующая подсказка. Для одной из вершин $B \in V(G)$ задано натуральное число $w_B \leqslant h(B)$ и известно, что во время игры чертик подойдет к мудрецу B и назовет ему w_B последовательных остатков (т. е. набор остатков вида x, $x+1$, …, $x+w_B$, суммирование по модулю $h(B)$), среди которых находится цвет его шляпы; остальные мудрецы не слышат эту подсказку. Вершина B, число w_B и правило оглашения подсказки мудрецам известны заранее. Обозначим игру с подсказкой через $\langle G, h, g, B, w_B\rangle$.

Например, игра $\langle G, h, g, B, w_B\rangle$ заведомо выигрышная в случае $w_B \leqslant g(B)$.

Т е о р е м а. Пусть граф G содержит вершину B, а граф $\tilde G$ получается из графа G добавлением новой вершины A и ребра AB. Пусть на графе $\tilde G$ заданы функции шляпности $\tilde h$ и числа попыток $\tilde g$, и пусть $h = \tilde h\Big|_{V(G)}$, $g = \tilde g\Big|_{V(G)}$. Пусть для некоторых натуральных чисел w_A, w_B, таких что $g(A) \leqslant w_A \leqslant h(A)$ и $g(B) \leqslant w_B \leqslant h(B)$, выполняются условия

(i) игра с подсказкой $\langle G, h, g, B, w_B\rangle$ выигрышная,

(ii) $w_B \cdot h(A)$ делится на $h(B)$,

(iii) $w_A w_B \geqslant (w_A - g(A))h(B)$.

Тогда игра с подсказкой $\langle \tilde G, \tilde h, \tilde g, A, w_A\rangle$ выигрышная.

Д о к а з а т е л ь с т в о. Чтобы описать стратегию мудреца A, построим таблицу $h(A) \times h(B)$, в которой часть клеток пустые, а в остальных поставлены буквы «L» по следующему правилу. Пронумеруем строки таблицы числами от 0 до $h(A)-1$, номера строк мы отождествляем с возможными цветами шляпы мудреца A, пронумеруем столбцы таблицы числами от 0 до $h(B)-1$, номера столбцов мы отождествляем с возможными цветами шляпы мудреца B. Пусть в строке с номером i ($0 \leqslant i \leqslant h(A)-1$) в столбцах с номерами

$$iw_B, \quad iw_B + 1, \quad \ldots, \quad iw_B + w_B - 1 \pmod{h(B)} \tag{1}$$

находятся буквы «L» (т. е. всего w_B букв «L»), см. рис. 6. Построенную таблицу можно считать тороидальной: вычисления по модулю $h(B)$ в правиле (1) позволяют отождествлять $h(B)$-й столбец с нулевым столбцом, а условие (ii) позволяет отождествить $h(A)$-ю строку с нулевой строкой.

Л е м м а. Рассмотрим произвольные w_A последовательных строк этой таблицы (с учетом ее тороидальной природы, т. е. можно взять несколько нижних строк и добавить к ним подходящее

количество верхних). Тогда каждый столбец таблицы содержит в этих строках не более $g(A)$ пустых клеток.

Доказательство. В силу тороидального характера таблицы достаточно проверить это утверждение для набора из первых w_A строк. Рассмотрим столбец номер j. Очевидно, этот столбец содержит букву «L» на пересечении с i-строкой ($0 \leqslant i \leqslant w_A - 1$) в том и только том случае, если

$$0 \leqslant (j - iw_B) \bmod h(B) \leqslant w_B - 1. \tag{2}$$

В целочисленной последовательности $d_i(j) = j - iw_B$ расстояние между $d_0(j)$ и $d_{w_A-1}(j)$ равно

$$(w_A - 1)w_B.$$

В силу условия (iii) выполняется неравенство

$$(w_A - 1)w_B \geqslant (w_A - g(A))h(B) - w_B$$

которое означает, что для каждого j неравенство (2) имеет не меньше $w_A - g(A)$ решений относительно переменной i, т. е. каждый столбец таблицы содержит не меньше $w_A - g(A)$ букв «L» в выбранных w_A строках. Значит, в нем содержится не больше $g(A)$ пустых клеток. □

Подсказка, которую мудрец A получает от чертика, — это фактически набор из w_A последовательных строк таблицы. Тогда стратегия мудреца A состоит в том, что он называет цвета, соответствующие номерам строк пустых клеток в j-м столбце таблицы, где j — цвет шляпы мудреца B. Мудрец A сможет это сделать, так как по утверждению леммы в указанном чертиком диапазоне из w_A строк j-й столбец содержит не более $g(A)$ пустых клеток.

Опишем стратегию мудреца B. Он видит цвет i шляпы мудреца A и сразу делает вывод, что A не угадывает только в тех случаях, когда цвет мудреца B соответствует столбцам, содержащим в i-й строке букву «L». Таким образом, B может думать, что его цвет задается множеством из этих w_B столбцов и, получив эту подсказку, он играет с этой подсказкой по стратегии для графа G.

Теорема доказана.

Вернемся к решению задачи. Предъявим стратегию мудрецов.

Для $k = 1, 3, \ldots, s-1$ обозначим через P_k подграф графа P_s, представляющий собой путь на вершинах $v_1, \ldots, v_k$. Функция h позволяет нам задать шляпности вершин $v_1, \ldots, v_k$. Проверим индукцией по k ($1 \leqslant k \leqslant s$), что игра с подсказкой $\langle P_k, h, \star s, v_k, s+k-1\rangle$, выигрышная (напомним, что в этой игре чертик указывает мудрецу v_k диапазон из $s + k - 1$ последовательных цветов, в котором находится цвет его шляпы).

База индукции $k = 1$: в игре $\langle P_1, h, \star s, v_1, s\rangle$ единственный игрок v_1, выигрывающий благодаря подсказке.

Индукционный переход $k \to k+1$, $k \leqslant s-2$. Пусть известно, что игра с подсказкой $\langle P_k, h, \star s, v_k, s+k-1\rangle$ выигрышная. Тогда по доказанной теореме игра $\langle P_{k+1}, h, \star s, v_{k+1}, s + k\rangle$ тоже выигрышная: здесь $B = v_k$, $w_B = s + k - 1$, $G = \langle P_k, h, \star s, v_k, s + k - 1\rangle$, $A = v_{k+1}$, $w_A = s + k$, $\tilde{G} = \langle P_{k+1}, h, \star s, v_{k+1}, s+k\rangle$. Условие ii) из теоремы выполняется по тривиальной причине $h(A) = h(B)$, а выполнение условия iii) обеспечивается неравенством

$$w_A w_B = (s + k - 1)(s + k) \underset{(*)}{\geqslant} k(4s - 2) = (w_A - g(A))h(B),$$

где неравенство $(*)$ сводится к очевидному неравенству $(s - k)^2 \geqslant s - k$.

Последний шаг $k = s - 1 \to s$ тоже выполняется по доказанной теореме. Это проверяется аналогично с тем лишь отличием, что условие ii) выполняется в силу того, что число $w_B = 2s-2$ — четное, и поэтому $w_B \cdot h(A) = (2s - 2)(2s - 1)$ делится на $h(B) = 4s - 2$.

Таким образом, мы доказали, что игра с подсказкой $\langle P_s, h, \star s, v_s, 2s-1\rangle$ выигрышная. Но тогда очевидно и игра $\langle P_s, h, \star s\rangle$ тоже выигрышная.

2.6. a) Решение 1. Индукция по числу вершин дерева. Индукционный переход. Добавление к проигрышному дереву очередной висячей вершины можно интерпретировать как склейку двух проигрышных игр конструктором задачи 3.3, где одна из игр — это игра на дереве $\langle T, \star t(s), \star s\rangle$, а другая — игра на графе K_2, в котором одна вершина имеет шляпность $s+1$ и s попыток угадывания, а вторая — шляпность s^2+s+1 и тоже s попыток.

Решение 2. Будем доказывать утверждение индукцией по числу вершин дерева. База $n=1$ тривиальна. Докажем переход.

Пусть мудрецы выбрали некоторую стратегию f в игре $\langle T, \star t(s), \star s\rangle$. Имеют место следующие два утверждения.

Утверждение I. Для любого мудреца A не менее чем $t(s)-s$ цветов его шляп, могут использоваться для построения опровергающих раскладов. Иными словами, можно выбрать $t(s)-s$ цветов и для каждого из них построить опровергающий расклад шляп, в котором шляпа A имеет выбранный цвет.

Утверждение II. Для любого мудреца A и любого комплекта C из $s+1$ его шляпы можно так задать цвета шляп на множестве $N(A)$, что при добавлении к этому раскладу любой шляпы $\alpha \in C$ для мудреца A полученный частичный расклад шляп можно дополнить до такого расклада шляп на всем дереве T, что никто из мудрецов на $T \setminus \{A\}$ не угадывает.

Ясно, что утверждение I следует из II. Кроме того, из II сразу следует индукционный переход: возьмем любого мудреца A и любой комплект C из $s+1$ его шляпы, тогда утверждение II задает расклад шляп на множестве $N(A)$, который однозначно определяет, какие s цветов называет мудрец A в этой игре. Дадим мудрецу A неназванный цвет из комплекта C, тогда A не угадает. По утверждению II можно сделать так, что и остальные мудрецы не угадают.

Докажем утверждение II.

Возьмем произвольного мудреца A и произвольный комплект C из $s+1$ его шляпы. Сделаем *эксперимент*: дадим мудрецу A любую шляпу $\alpha \in C$ и удалим его (мысленно) из дерева T. Дерево распадется на компоненты связности, для которых выполняется индукционное предположение. Очевидно, в каждой компоненте имеется по одному мудрецу из $N(A)$. Пусть B — один из таких мудрецов, T_B — его компонента связности. Поскольку мы уже задали цвет шляпы A, стратегия f определяет стратегию мудреца T для игры на T_B, остальные мудрецы из T_B тоже могут пользоваться стратегией f. По утверждению I эту стратегию можно опровергнуть, дав мудрецу B шляпу из некоторого множества, содержащего $t(s)-s$ цветов.

Указанный эксперимент можно провести $s+1$ способом. Получающиеся игры на T_B отличаются стратегией мудреца B и для каждой из этих игр мудрец B имеет опровергающее множество из $t(s)-s$ цветов. Осталось заметить, что пересечение этих $s+1$ множеств содержит не меньше чем $t(s)-(s+1)s=1$ элементов, т. е. оно непусто. Назначим мудрецу B цвет, лежащий в этом пересечении. Аналогично поступим в остальных компонентах связности. В результате мы построили расклад шляп на множестве $N(A)$, для которого выполняется утверждение II.

b) Это решение сообщил нам С. Берлов. Докажем, что при $n=(s^2+s)!$ мудрецы выигрывают. Пусть A — центральный мудрец. Рассмотрим таблицу $(s+1)\times s$. Каждому способу заполнить её различными числами от 0 до s^2+s-1 сопоставим отдельного мудреца. Стратегия мудрецов следующая. Каждый «периферийный» мудрец находит в своей таблице строку, содержащую число c_A, и называет все числа этой строки. Далее, мудрец A для каждого числа i от 1 до $(s^2+s)!$ проверяет, выигрывает ли кто-то из остальных мудрецов, если $c_A=i$ (это легко сделать, так как A знает цвет шляпы каждого мудреца и знает его табличку). Пусть $i_1, i_2, \ldots, i_k$ — список значений c_A, для которых ни один из остальных мудрецов не выигрывает. Если $k \leqslant s$, то A просто назовет эти значения, и мудрецы победят. Предположим, что $k \geqslant s+1$. Так как у мудрецов встречаются все возможные таблицы, то найдется мудрец B, в таблице которого числа $i_1, i_2, \ldots, i_{s+1}$ стоят в разных строках. Но в одной из строк стоит число равное c_B, и если это строка, содержащая число i_ℓ, то мудрец B должен выигрывать при $c_A=i_\ell$. Противоречие.

c) Аналогично п. b). Назовем «свалкой» три кучи камней, содержащие в совокупности h камней, причем камни пронумерованы от 0 до $h-1$, а кучи пронумерованы числами 0, 1, 2 (т. е.

возможными цветами шляпы периферийных мудрецов). Пусть n — это количество всевозможных свалок. Зададим стратегию мудрецов на графе $K_{1,n}$. Каждому мудрецу B_i выдадим уникальную свалку. Стратегия B_i состоит в том, что он называет номер кучи, в которой лежит камень с номером c_A. Стратегия мудреца A состоит в том, что он составляет список тех цветов своей шляпы, для которых никто из B_i не угадал, и называет все цвета из этого списка. В этом списке не может быть больше двух цветов. Действительно, если список содержит цвета c_1, c_2, c_3, то рассмотрим любую свалку, в которых камни c_1, c_2, c_3 лежат в первой, второй и третьей куче соответственно. Не умаляя общности можно считать, что владелец свалки получил шляпу первого цвета. Но тогда он заведомо угадает свой цвет, если мудрец A получил шляпу цвета c_1.

3.1. Это очевидно: на графе $\widetilde{G}$ мудрец A должен сначала назвать $g(A_1)$ цветов, которые он называет по стратегии вершины A_1 графа G (при этом он учитывает только цвета соседей A_1), а потом еще $g(A_2)$ цветов по стратегии вершины A_2 (глядя только на соседей A_2). Мудрецы, которые на графе G видят только одного из A_i, играют так, словно A и есть этот A_i. Что касается тех мудрецов, которые видели в графе G и A_1, и A_2, а теперь видят лишь одного мудреца A, они должны играть, полагая, что на A_1 и на A_2 надеты шляпы одинакового цвета.

3.2. Шляпность мудреца v равна $h_1(v)h_2(v)$. Поэтому можно считать, что шляпа мудреца v имеет «композитный цвет», т. е. её цвет — это упорядоченная пара (c_1, c_2), где c_i — цвет шляпы v в игре $\mathcal{G}_i$. Зафиксируем выигрышные стратегии для игр $\mathcal{G}_1$ и $\mathcal{G}_2$ и построим стратегию для игры $\mathcal{G}_1 \times_v \mathcal{G}_2$. Пусть все мудрецы из графа $G_i \setminus \{v\}$ играют по выигрышной стратегии для игры $\mathcal{G}_i$ (при этом соседи v по графу G_i смотрят лишь на компоненту c_i цвета мудреца v). Что касается мудреца v, он будет играть сразу по обеим стратегиям: смотря только на своих соседей из графа G_1, мудрец v по выигрышной стратегии для игры $\mathcal{G}_1$ найдет $g_1(v)$ первых компонент своего цвета, а по выигрышной стратегии для игры $\mathcal{G}_2$ — $g_2(v)$ вторых компонент. Перебрав все возможные пары найденных цветов, он сделает $g_1(v)g_2(v)$ попыток угадать свой цвет, что по определению равняется $g(v)$.

Построенная стратегия выигрышная, потому что либо кто-то из $G_1 \setminus \{v\}$ или из $G_2 \setminus \{v\}$ угадает цвет, либо v угадает обе компоненты своего цвета.

3.3. Пусть это не так, и f — выигрышная стратегия мудрецов в игре $\mathcal{G}$. Обозначим через N_1 множество соседей вершины A в графе G_1. Для любого расклада шляп φ на вершинах графа G_1 определен ответ по стратегии f всех мудрецов из множества $V(G_1)\setminus A$. Покажем, что на графе G_1 существует $s+1$ раскладов шляп φ_i $(i = 1, \ldots, s+1)$, при $i \neq j$ удовлетворяющих свойствам

$$\varphi_i\big|_{N_1} = \varphi_j\big|_{N_1}, \qquad \varphi_i(A) \neq \varphi_j(A),$$

и таких, что если мудрецы из G_1 будут играть по стратегии f, то для всех этих раскладов ни один мудрец из множества $V(G_1) \setminus A$ не угадает цвет своей шляпы.

Для каждого расклада шляп α на вершинах из N_1 обозначим через $C(\alpha)$ множество тех цветов шляп мудреца A, такое что для всех раскладов β на G_1, у которых

$$\beta\big|_{N_1} = \alpha, \qquad \beta(A) \in C(\alpha),$$

ни один мудрец из множества $V(G_1) \setminus A$ не угадает свой цвет по стратегии f. Предположим, что утверждение из предыдущего абзаца не выполняется. Тогда каждое множество $C(\alpha)$ содержит не более s цветов. Рассмотрим тогда следующую стратегию для игры $\mathcal{G}_1$: пусть все мудрецы из G_1, кроме A, играют по стратегии f, а мудрец A называет цвета из множества $C(\alpha)$ (дополняя произвольными цветами, если в $C(\alpha)$ меньше s элементов). Это выигрышная стратегия, так как если никто из $V(G_1)\setminus A$ не угадал, то на A надета шляпа из $C(\alpha)$, и он угадывает. Противоречие.

Рассмотрим эти $s+1$ раскладов φ_i. Зафиксируем расклад шляп $\alpha = \varphi_i\big|_{N_1}$ на N_1 и ограничимся лишь теми раскладами шляп на G_2, где мудрец A получает шляпу одного из $s+1$ цветов $\varphi_i(A)$, $i = 1, \ldots, s+1$. Тогда стратегия f задает действия мудрецов на графе G_2, т. е. в проигрышной игре $\mathcal{G}_2$ с той лишь оговоркой, что в случае $h_1(A) > s+1$ мудрец A по этой стратегии может называть больше $s+1$ цвета, т. е. больше, чем его шляпность в игре G_2. Однако в этом

случае упоминание «посторонних» цветов не способствует выигрышу. Значит, на G_2 существует опровергающий расклад ψ. Если $\psi(A) = \varphi_j(A)$, то $\psi \cup \varphi_j\big|_{V(G_1)\setminus A}$ — расклад, опровергающий стратегию f в игре $\mathcal{G}$.

3.4. Это очевидно: на графе $\widetilde{G}$ мудрец A должен сначала назвать $g(A)$ цветов, которые он называет по стратегии для графа G, если у мудреца B первый цвет шляпы, потом еще $g(A)$ цветов, которые он называет, если у мудреца B второй цвет шляпы, и т. д.

3.5. Для каждого натурального N множество $\{0, 1, \ldots, N-1\}$ обозначим для краткости через $[N]$.

Для каждой вершины u подставляемого графа G_1 определим её цвет в игре $\langle G, h, g\rangle$, как композитный цвет из множества $[h_1(u)] \times [h_2(A)]$. Первую компоненту u будет искать по своей изначальной стратегии из игры $\mathcal{G}_1$, а вторую — по стратегии A из игры $\mathcal{G}_2$. Соседи вершины A из графа G_2 в новом графе G видят весь подграф G_1, и потому могут определить, кто угадал свою первую компоненту цвета. Пусть B — первый из таких мудрецов (в лексикографическом порядке), вершины графа $G_2 \setminus \{A\}$ могут играть по стратегии игры $\mathcal{G}_2$, используя вторую компоненту цвета B в качестве цвета A. Поскольку $\mathcal{G}_2$ — выигрышная игра, какая-то из вершин побеждает. Если это вершина из $G_2 \setminus \{A\}$, то она угадывает свой цвет и в графе G. Если же в $\mathcal{G}_2$ побеждала вершина A, то B правильно нашла и вторую компоненту своего цвета.

3.6. Для доказательства мы модифицируем стратегию конструктора подстановки из предыдущей задачи. В силу этой конструкции вершина v после подстановки получает композитный цвет из множества $[h(v)] \times [h'(A)]$, а стратегия мудреца v состоит в том, что он вычисляет G-компоненту своего ответа, т. е. выбирает $s = g(v)$ цветов $c_1, \ldots, c_s \in [h(v)]$, вычисляет G'-компоненту своего ответа, т. е. выбирает $g'(A)$ цветов $e_1, \ldots, e_{g'(A)} \in [h'(A)]$, после чего называет все пары цветов вида (c_i, e_j).

Введем изменение в конструкцию подстановки и опишем, как играют мудрецы в изменившейся ситуации. Изменение затрагивает только подставляемых мудрецов v и состоит в том, что им назначается $h^*(v) = h(v)$ и $g^*(v) = g'(A)$. Таким образом, шляпа мудреца v вместо композитного цвета будет иметь цвет «всего лишь» из множества $[h(v)]$, каковое по-прежнему воспринимается его соседями из $N_G(v)$ и $N_{G'}(A)$ как G-компонента его цвета.

Стратегия каждого подставляемого мудреца v состоит из двух фаз. Первая фаза: поглядев на соседей в G, мудрец v вычисляет «G-компоненту» своего ответа, т. е. некоторый набор из s цветов $c_1, \ldots, c_s \in [h(v)]$. Далее мудрец v отождествляет построенный набор с множеством $[h'(A)]$ (по правилу $c_i \mapsto i$; напомним, что $h'(A) = s$). После этого происходит вторая фаза: он смотрит на своих соседей в графе G' и применяет стратегию мудреца A, называя $g'(A)$ цветов из своего новообретенного множества $[h'(A)]$.

Осталось описать стратегию мудрецов из $N_{G'}(A)$. Все они видят целиком граф G, поэтому знают, какой набор цветов каждый мудрец v отождествил с множеством $[h'(A)]$. Кроме того, все они знают, кто из $V(G)$ правильно угадал G-компоненту своего цвета, допустим, первым из таких мудрецов (в лексикографическом порядке) является мудрец w. То, что мудрец w угадал G-компоненту своего цвета, означает, что цвет его шляпы лежит в построенном им множестве $[h'(A)]$. Тогда на второй фазе мудрецы графа $G' \setminus \{A\}$ просто разыгрывают выигрышную стратегию игры $\mathcal{G}'$, подставляя w с его построенным множеством $[h'(A)]$ на место A, а мудрец w, как определено выше, тоже фактически играет по этой стратегии. В результате кто-то из них угадает.

3.7. Каждый мудрец из $V(G) \setminus \{A\}$, который видит мудрецов B, рассчитывает «виртуальный цвет мудреца A»

$$c_A = \sum_{v \in B} c_v \pmod{h(A)}$$

и играет по стратегии из игры $\mathcal{G}$. Что касается мудрецов из B, они берут себе по одному ответу a_i из стратегии мудреца A, и мудрец v_i называет цвет

$$a_i - \sum_{v \in B, v \neq v_i} c_v \pmod{h(A)}$$

(таким образом i-й мудрец проверяет гипотезу $c_A = a_i$).

4.1. Пусть B — вершина шляпности 2. Применим для вершины B утверждение конструктора «удаление половины ребра» (задача 3.4), сделав эту вершину невидимой для остальных вершин. Тогда остальные мудрецы не видят B, имеют по две попытки, и проигрывают по утверждению задачи 2.6 б). Выдав им опровергающий расклад шляп, судья сделает так, что и мудрец B не угадает.

4.2. Зафиксируем число s. Рассмотрим случай, когда верхняя вершина лепестка имеет шляпность $s+1$, а остальные вершины — шляпность h. Действуя, как в предыдущей задаче, мы делаем верхнюю вершину невидимой для остальных, от этого число попыток угадывания у остальных вершин, расположенных на пути P_{n-1}, становится равно $s(s+1) = f(s)$. Отсюда по утверждению задачи 2.6 б) мы получаем, что при $h > f(f(s))$ мудрецы проигрывают. Следовательно, $t_s \leqslant f(f(s))$.

4.3. Будем доказывать индукцией по числу лепестков, что при $h > f(f(f(s)))$ игра проигрышная. База индукции — один лепесток G — с запасом доказана в п. а): игра $\langle G, \star h, \star s\rangle$ проигрышная уже при $h > f(f(s))$.

Но нам понадобится одно близкое утверждение – «модифицированная база индукции»: игра $\langle G, \star\bar{h}, \star s\rangle$ проигрышная при $h > f(f(f(s)))$, где через $\star\bar{h}$ обозначена функция шляпности, равная h во всех вершинах лепестка G, кроме одной вершины B, шляпность которой равна $s+1$.

Докажем это утверждение. Если B — верхняя вершина лепестка G, это опять утверждение базы. Пусть B — произвольная вершина лепестка в нижнем ряду (рис. 7, слева). Пользуясь конструктором «удаление половины ребра» задачи 3.4, сделаем вершину B невидимой для остальных вершин, в результате число попыток у ее соседей станет равно $f(s)$. Теперь вершину B можно вообще удалить из G — ее никто не видит, у нее шляпность $s+1$ и всего s попыток угадывания, ей не суждено угадать. Как нетрудно видеть, оставшийся граф представляет собой объединение двух лепестков с общей верхней вершиной (или один лепесток, но этот случай тривиален) и с увеличенным до $f(s)$ количеством попыток угадывания у некоторых вершин (рис. 7, в центре). Добавим к графу горизонтальное ребро между бывшими соседями B (рис. 7, справа), оно могло бы помочь мудрецам выиграть. В результате получился лепесток, вершины которого имеют не более $f(s)$ попыток угадывания, а их шляпности больше $f(f(f(s)))$. По утверждению базы мудрецы все-таки проигрывают.

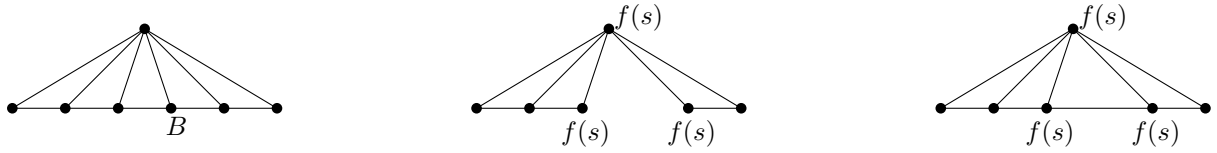


Рис. 7. Удаляем вершину B из лепестка G

Теперь докажем индукционный переход. Рассмотрим петунию $M_n = M_{n-1} +_{v_n} L_n$. В силу модифицированного утверждения базы игра $\langle L_n, \star\bar{h}, \star s\rangle$ проигрышная при $h > f(f(f(s)))$, где через $\star\bar{h}$ обозначена функция шляпности, равная h во всех вершинах лепестка G, кроме v_n, а шляпность v_n равна $s+1$. Игра $\langle M_{n-1}, \star h, \star s\rangle$ проигрышная по предположению индукции. Осталось заметить, что игра $\langle M_n, \star h, \star s\rangle$ может быть получена с помощью конструктора задачи 3.3 из проигрышных игр $\langle M_{n-1}, \star h, \star s\rangle$ и $\langle L_n, \star\bar{h}, \star s\rangle$ и поэтому тоже является проигрышной.

4.4. а) Оценка $\mathrm{HG}_s(G) < 4s(s+1)-1$. Пусть A — черенок лепестка, причем $h(A) = s+1$, а остальные вершины v имеют шляпность $h(v) = 4s(s+1) - 1$. Достаточно проверить проигрышность игры $\langle G, h, \star s\rangle$. По утверждению задачи 5.6, эта игра эквивалентна игре на пути P_n, где у всех вершин шляпность равна $4s(s+1)-1$, а число попыток — $s(s+1)$. Но как следует из задачи 2.3, эта игра проигрышная.

Покажем, что игра $\langle G, \star 4s(s+1) - 2, \star s\rangle$ — выигрышная при больших n.

Пусть $\mathcal{G}_0 = \langle P_k, \star 4s(s+1)-2, \star s(s+1)\rangle$. Будем считать, что число k достаточно велико, тогда по результату задачи 2.5, игра $\mathcal{G}_0$ выигрышная.

Аналогично задаче 2.6 c) можно доказать, что для любого натурального h существует такое натуральное n, что игра на графе $K_{1,n}$ — выигрышная, если шляпности всех периферийных мудрецов равны $s+1$ и все они имеют по одной попытке угадывания, а шляпность центрального мудреца равна h и у него s попыток. Положим $h = 4s(s+1) - 2$ и подберем подходящее n. Подставим с сокращением на место каждого периферийного мудреца игру $\mathcal{G}_0$. Мы получим выигрышную игру, где у всех вершин шляпности равны $4s(s+1)-2$, количества попыток равны s, а граф представляет собой подграф большого лепестка.

b) Как мы проверили в п. a), игра $\langle G, h, \star s\rangle$ — проигрышная, где G — лепесток с большим числом вершин, а h — функция, задающая черенку шляпность $s+1$, а остальным вершинам — шляпность $4s(s+1)-1$. По утверждению задачи 3.3 приклеивание такого лепестка по черенку к другой проигрышной игре (где число попыток в вершине, куда мы его приклеиваем, равно s) снова дает проигрышную игру. Но королевская петуния по определению задается последовательными черенковыми приклеиваниями лепестков! Таким образом, игра на королевской петунии с большими лепестками, где все вершины имеют шляпность $4s(s+1)-1$ и s попыток угадывания, кроме (первого, корневого) черенка, имеющего шляпность $s+1$ и s попыток угадывания, проигрышная. Это дает оценку $\mathrm{HG}_s(G) < 4s(s+1)-1$.

Тогда $\mathrm{HG}_s(G) = 4s(s+1)-2$, поскольку такая шляпность реализуется уже на лепестках, которые являются королевскими петуниями, хотя и не слишком развесистыми.

5.1. *Необходимость.* Рассмотрим один из h_0 цветов шляпы центрального мудреца. Тогда стратегии остальных вершин уже определены, и в $\prod\limits_{i=1}^{n}(h_i - g_i)$ случаев ни одна из висячих вершин не угадывает свой цвет. Следовательно, это должен делать центральный. Но центральный мудрец может это сделать суммарно только в $g_0\prod\limits_{i=1}^{n} h_i$ случаях. Отсюда и следует неравенство, равносильное неравенству из условия.

Достаточность. Покажем, что игра $\big\langle K_{1,n}, (N\cdot h_0; h_1, \ldots, h_n), (N\cdot g_0; g_1, \ldots, g_n)\big\rangle$ при $N = \prod\limits_{i=1}^{n} h_i$ — выигрышная.

Закодируем $h_0\cdot h_1\cdot\ldots\cdot h_n$ цветов центрального мудреца наборами $(c_0; c_1, \ldots, c_n)$, где $0 \leqslant c_i < h_i$. Пусть i-й мудрец, видя цвет $(c_0; c_1, \ldots, c_n)$, называет цвета $c_i, c_i+1, \ldots c_i+g_i-1 \pmod{h_i}$. Центральный же мудрец должен посмотреть на остальных и назвать все варианты, в которых ни один из них не угадает. Сколько их? Есть h_0 вариантов для нулевой компоненты и $h_i - g_i$ вариантов для каждой из остальных. Однако неравенство из условия равносильно неравенству $h_0\prod\limits_{i=1}^{n}(h_i - g_i) \leqslant N\cdot g_0$, поэтому центральному мудрецу попыток хватит.

5.2. Обозначим мудрецов через A, B и C: $\overset{\frac{g}{h}}{\bullet}\!\!-\!\!\overset{\frac{g}{h}}{\bullet}\!\!-\!\!\overset{\frac{g}{h}}{\bullet}$ $\begin{matrix}A & B & C\end{matrix}$. Предъявим выигрышную стратегию мудрецов. Пусть мудрец A назовет цвета c_B, c_B+1, …, $c_B+(g-1) \bmod h$, а мудрец C — c_B, $c_B+[\frac{h}{g}]$, …, $c_B+[(g-1)\frac{h}{g}] \bmod h$, где $[x]$ — округление до ближайшего целого числа. Таким образом, если на мудреце B шляпа из набора

$$I_A = \big(c_A, c_A-1, \ldots, c_A-(g-1)\big) \bmod h,$$

то мудрец A угадает, а если из набора

$$I_C = \Big(c_C, c_C - \Big[\frac{h}{g}\Big], \ldots, c_C - \Big[(g-1)\cdot\frac{h}{g}\Big]\Big) \bmod h,$$

то угадает мудрец C. Осталось доказать, что у мудреца B не более чем g цветов непокрытых множеством $I_A \cup I_C$, или, эквивалентно, что

$$h - |I_A| - |I_C| + |I_A \cap I_C| \leqslant g.$$

Поскольку $|I_A| = |I_C| = g$, это равносильно неравенству $|I_A \cap I_C| \leqslant 3g - h$.

Предположим, что это утверждение неверно и $|I_A \cap I_C| > 3g - h$. Тогда найдётся такое k, что оба числа $c_C - [k \cdot \frac{h}{g}]$ и $c_C - [(k + 3g - h) \cdot \frac{h}{g}]$ лежат в $I_A \cap I_C$ (элементы пересечения $I_A \cap I_C$ могут быть записаны двумя способами: $c_A - i = c_C - \big[\ell \cdot \frac{h}{g}\big]$, в качестве k можно число ℓ, соответствующее минимально возможному i). Поскольку оба элемента лежат в множестве I_A, состоящем из подряд идущих остатков, расстояние между ними не превосходит $g - 1$:

$$\Big(c_C - \Big[k \cdot \frac{h}{g}\Big]\Big) - \Big(c_C - \Big[(k + 3g - h) \cdot \frac{h}{g}\Big]\Big) \leqslant g - 1,$$

что равносильно

$$\Big[(k + 3g - h) \cdot \frac{h}{g}\Big] - \Big[k \cdot \frac{h}{g}\Big] \leqslant g - 1.$$

Избавляясь от округления, получаем следствие:

$$(k + 3g - h) \cdot \frac{h}{g} - 0.5 - k \cdot \frac{h}{g} - 0.5 \leqslant g - 1.$$

Последнее равносильно неравенству $(3g - h) \cdot \frac{h}{g} \leqslant g$, т. е. $0 \leqslant g^2 - 3gh + h^2$, что противоречит условию.

5.3. По утверждению задачи 5.1 существование k, при котором игра $\langle P_3, \star kh, \star kg\rangle = \langle K_{1,2}, \star kh, \star kg\rangle$ выигрышная, эквивалентна условию

$$\Big(1 - \frac{g}{h}\Big)\Big(1 - \frac{g}{h}\Big) \leqslant \frac{g}{h},$$

а это для неотрицательных h равносильно неравенству $g^2 - 3gh + h^2 \leqslant 0$, что при $1 \leqslant g \leqslant h$ эквивалентно неравенству

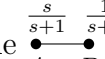
$$\frac{h}{g} \leqslant \frac{3 + \sqrt{5}}{2}.$$

Теперь утверждение задачи очевидно.

5.4. Рассмотрим произвольную стратегию мудрецов в игре $\langle G, h\rangle$. Произведение $\prod\limits_{v \in H_2} h_2(v)$ перечисляет расклады шляп на H_2, задание каждого из них фиксирует стратегию мудрецов на G_1. При фиксированном раскладе шляп на H_2 будем перебирать расклады шляп на G_1. Тогда сумма $\sum\limits_{u \in G_1} \frac{1}{h_1(u)}$ подсчитывает наибольшую возможную долю тех раскладов на G_1, где хотя бы один мудрец из G_1 угадывает. Тогда произведение $\Big(\sum\limits_{u \in G_1} \frac{1}{h_1(u)}\Big) \prod\limits_{v \in H_2} h_2(v)$ подсчитывает наибольшую возможную долю тех раскладов на G_1, где хотя бы один мудрец из G_1 угадывает, если мы каждому мудрецу даем $\prod\limits_{v \in H_2} h_2(v)$ попыток для угадывания. Таким образом, выполнение неравенства из условия задачи означает, что существует расклад шляп α на G_1, для которого ни один мудрец из G_1 не угадывает, какие бы шляпы при этом ни выдавались бы мудрецам из H_2. Если выдать мудрецам из G_1 расклад α, ни один из них не угадает и при этом будет полностью задана стратегия мудрецов на графе G_2, пригодная для игры $\langle G_2, h_2\rangle$. Поскольку эта игра проигрышная, расклад шляп α можно дополнить раскладом шляп на G_2, для которого никто из G_2 также не угадает.

5.5. Пусть мудрецы зафиксировали стратегию на графе G'. Построим проигрышный расклад шляп для этой стратегии. Стратегия мудреца B для каждого из $2h(A) - 1$ возможных цветов шляпы A предписывает назвать один из двух цветов. Какой-то из этих двух цветов называется не более чем $h(A) - 1$ раз. Дадим мудрецу B шляпу этого цвета, это фиксирует стратегию мудреца A на оставшемся графе G. Теперь, чтобы B не угадал, мы попытаемся дать A шляпу одного из оставшихся $h(A)$ цветов (если их осталось больше, оставим ровно $h(A)$). С этим ограничением нам удастся построить расклад шляп на графе G так, что никто на G не угадает, поскольку игра $\mathcal{G}$ проигрышная.

5.6. If $\mathcal{G}$ is a winning game, we remove by problem 3.4 all half-edges $\overrightarrow{vA}$ and obtain the winning game. In this game A has s guesses, $s+1$ colors and no infotmation, therefore we can assign A's color such that A does not guess. But now the remaining sages play the game $\mathcal{G}'$. Hence $\mathcal{G}'$ is winning.

If the game $\mathcal{G}'$ is winning, substitute $\mathcal{G}'$ in the winning game 

in place of vertex B by problem 3.6. We obtain a winning game $\mathcal{G}$.

5.7. a) Пусть $\mathcal{G}$ — проигрышная игра на пути ABC со шляпностями вершин $h(A) = h(C) = 2$, $h(B) = 5$. Если бы обе игры из условия оказались проигрышными, то исходная игра получалась бы из этих игр и игры $\mathcal{G}$ с помощью конструктора задачи 3.3 (где $s = 1$, $g_1 = g_2 = \star 1$) и тоже оказалась бы проигрышной.

b) Множество $V(\widetilde{G})$ состоит из вершин графа G и множества новых вершин V_1 (расположенных в середине двузвенных путей). Зададим функцию на $V(\widetilde{G})$:

$$h(v) = \begin{cases} 2, & v \in V(G), \\ 5, & v \in V_1. \end{cases}$$

Достаточно проверить, что игра $\langle \widetilde{G}, h\rangle$ проигрышная. Это очевидно. Действительно, каждый мудрец из V_1 имеет двух соседей в $\widetilde{G}$ со шляпностью 2, поэтому он называет по своей стратегии не более четырех цветов — сразу же дадим ему шляпу того цвета, который он не называет, и он не угадает. Теперь все ответы мудрецов из $V(G)$ детерминированы, и мы тоже дадим каждому мудрецу шляпу того цвета, который он не называет.

5.8. Пусть при удалении моста граф G распадается на компоненты G_1 (содержащую вершину B) и G_2 (содержащую вершину A). Введем функции шляпности h_1 и h_2 на этих графах по правилу

$$h_1(x) = \begin{cases} h(x), & x \in V(G_1) \setminus \{B\}, \\ \lceil \frac{h(B)}{2} \rceil, & x = B. \end{cases} \qquad h_2(x) = \begin{cases} h(x), & x \in V(G_2) \setminus \{A\}, \\ \lceil \frac{h(A)}{2} \rceil, & x = A. \end{cases}$$

Обозначим через $\mathcal{G}_{BA}$ игру на графе K_2 с вершинами B и A, где шляпности обеих вершин равны 2. Эта игра выигрышная. Наконец, пусть $\mathcal{G}_1' = \langle G_1, h\big|_{G_1}\rangle$ — проигрышная игра в силу свойств функции h.

Если игры $\mathcal{G}_1 = \langle G_1, h_1\rangle$ и $\mathcal{G}_2 = \langle G_2, h_2\rangle$ обе выигрышные, то игра $\mathcal{G}_1 \times_B \mathcal{G}_{BA} \times_A \mathcal{G}_2$ тоже выигрышная. Если при этом значения $h(A)$ и $h(B)$ четные, мы получаем требуемое разложение игры $\mathcal{G}$ в произведение игр. Если же хотя бы одно из чисел $h(A)$, $h(B)$ нечетное, то функция шляпности полученной игры мажорирует h и по свойствам функции h такая игра не может быть выигрышной.

Осталось разобрать случай, когда хотя бы одна игра $\mathcal{G}_1 = \langle G_1, h_1\rangle$ или $\mathcal{G}_2 = \langle G_2, h_2\rangle$ проигрышная, пусть это будет игра $\mathcal{G}_2$. Рассмотрим игру $\mathcal{G}_2'$, полученную применением конструктора задачи 5.5 к игре $\mathcal{G}_2$: в ней к проигрышному графу G_2 добавлена новая вершина B, соединенная с A, при этом шляпность вершины A стала равна

$$2\left\lceil \frac{h(A)}{2} \right\rceil - 1 \leqslant h(A),$$

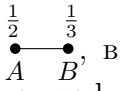
шляпность вершины B равна 2, а шляпности остальных вершин задаются функцией h. Применим теперь конструктор задачи 3.3 к играм $\mathcal{G}_1'$ и $\mathcal{G}_2'$ (считаем, что $s = 1$, $g_1 = g_2 = \star 1$). Мы получим проигрышную игру на графе G, в которой функция шляпности не превосходит h. Это невозможно.

5.9. Обозначим исходную игру через $\mathcal{G}_1 = (G_1, h_1, g_1)$, где $g_1 \equiv 1$. Подграф графа G_1, получающийся из G_1 удалением вершины A, обозначим через G_2, подграф графа G_2, получающийся из G_2 удалением вершины B, обозначим через G_3, а через G_4 обозначим граф, полученный из G_3

добавлением вершины C, которая всех видит и которую все видят, т. е. фактически G_4 получается из G_2 переименованием вершины B в C. Рассмотрим игры $\mathcal{G}_2 = (G_2, h_2, g_2)$, $\mathcal{G}_3 = (G_3, h_3, g_3)$, $\mathcal{G}_4 = (G_4, h_4, g_4)$, где

$$h_2(v) = \begin{cases} h_1(v) & v \in G_3, \\ 3 & v = B \end{cases}, \qquad h_3(v) = h_1\big|_{G_3}, \qquad h_4(v) = \begin{cases} h_1(v) & v \in G_3, \\ 6 & v = C \end{cases},$$

$$g_2 \equiv 2 \qquad g_3 \equiv 6 \qquad g_4(v) = \begin{cases} 1 & v \in G_3, \\ 5 & v = C \end{cases}.$$

Допустим, что игра $\mathcal{G}_1$ выигрышная. Удалим по задаче 3.4 все полуребра, ведущие в вершины A и B, мы получим выигрышную игру, в которой у остальных участников (мудрецов из G_3) число попыток стало равно 6, а стратегии не зависят от цветов шляп A и B. Если бы можно было выдать на G_3 расклад шляп, на котором никто из G_3 не угадывает, это фиксировало бы стратегии мудрецов A и B, играющих на ребре AB в игру 

, в результате все мудрецы проиграли бы, что невозможно. Следовательно, сужение игры на граф G_3, т. е. игра $\mathcal{G}_3$, является выигрышной. Сделаем по задаче 3.6 подстановку этой игры с сокращением в игру 

на место вершины v, получаем выигрышную игру $\mathcal{G}_4$.

Пусть теперь наоборот игра $\mathcal{G}_4$ выигрышная. Мы должны заменить игрока C на двух игроков A (шляпности 2) и B (шляпности 3). Предъявим выигрышную стратегию игроков в полученной игре. Все игроки из G_3 будут пользоваться стратегией игры $\mathcal{G}_4$, интерпретируя пару (цвет A, цвет B) как композитный цвет игрока C. Покажем, как можно «конвертировать» стратегию игрока C в пару стратегий A и B.

Цвет игрока C — это элемент множества $\mathcal{C} = \{0,1\} \times \{0,1,2\}$. Пусть при состоявшемся раскладе шляп соседей C должен назвать все цвета из множества $\mathcal{C}$, кроме $(1,2)$. Тогда действия игроков A и B состоят в том, что A называет цвет, совпадающий с четность цвета B, а B называет цвет 0 или 1, противоположной четности к цвету A. Игрок C угадывал по своей стратегии, если у него был один из цветов $(0,0)$, $(0,2)$, $(1,1)$ или $(0,1)$, $(1,0)$. По нашему правилу в первых трех случаях угадает A, в остальных двух B. Аналогично распределяются роли A и B для других пятерок ответов C.

5.10. Покажем, что игра $\big\langle G, \star\mathrm{HG}_{s'}(G[A])+1, \star s\big\rangle$, где $s' = s(\mathrm{HG}_s(G[B])+1)^d$, — проигрышная. Для этого построим расклад шляп, для которого мудрецы проиграют. Поскольку $\mathrm{HG}_{s'}(G[A]) \geqslant s' \geqslant \mathrm{HG}_s(G[B]) + 1$, т. е. шляпность в рассматриваемой игре больше, чем $\mathrm{HG}_s(G[B]) + 1$, достаточно рассмотреть случай, когда шляпность мудрецов из B равна $\mathrm{HG}_s(G[B]) + 1$. Используя задачу 3.4, удалим всё полурёбра из A в B, сделав множество B невидимым для множества A. Так как в результате этого действия мы у каждого мудреца из A стираем не более d полуребер, число попыток у мудреца вырастет, но не будет превосходить s'. При этом стратегии у мудрецов из A теперь не зависят от расклада шляп на B. Значит, мы можем считать, что на графе $G[A]$ происходит игра $\big\langle G[A], \star\mathrm{HG}_{s'}(G[A]) + 1, \star s'\big\rangle$. По определению s-шляпного числа эта игра проигрышная. Значит, существует расклад шляп на A, такой что никто из A не угадывает свой цвет. Выдадим мудрецам из A этот раклад, тогда у мудрецов из B будет детерминирована стратегия игры на $G[B]$. Поскольку шляпности мудрецов из B больше $\mathrm{HG}_s(G[B])$, мы можем каждому выдать цвет, который он не назвал. Мудрецы проиграли.

Paint my hat in 3.5 colors!

K. Kokhas, A. Latyshev

Project team: O. Bursian, D. Kokhas, K. Kokhas, V. Retinskiy

1 Let us introduce: the HATS game!

Let an undirected graph G be given, one sage and one chest with hats of different colors are located in each of its vertices. All the sages are acquainted with each other. Graph G, the location of the sages in the vertices of the graph and the colors of hats in all chests are fixed and known to everybody. In particular, each sage understands, in which vertex each of the others sages is located. The referee performs the following test with the sages. He puts a hat on the head of each sage, the hat is taken from the sage's chest. Each sage sees only the hats of the sages located in the neighbouring vertices of the graph, he does not see his own hat and does not know its color. The sages cannot communicate during the test. At the command of the referee each of the sages writes names of several colors on his paper simultaneously (how many colors the sages has to mention, is determined by the additional rule). We say that the sages have passed the test successfully = «have won», if at least one of them wrote the color of his hat in his paper.

The sages have been informed of the rules of the test before the testing and they have the possibility to hold a meeting, in which they must to define their public strategy. The publicity means that all the participants, including the referee, know this strategy. The strategy of the sages has to be deterministic, that is each sage has to write colors on his paper looking only the colors that he sees on his neighbours. We call the strategy *winning* if for any hats placement at least one sage will guess correctly the color of the hat on his head, i. e. mention this color in the his list of guesses. We say that the sages win, if they have a winning strategy, and that they lose, if they have not.

Therefore, the HATS game is not a game in a sense as it is ordinarily understood. This game lasts only one move.

1.1. The referee puts a hat of white, blue, red or green color on the head of each of two sages. Each of them sees the hat of the other, but does not see his own hat. Each of them writes on his own paper two colors simultaneously. They try to guess correctly the colors of their own hats. Prove that the sages can come to an agreement in the meeting before the test in such a way that at least one of them will guess correctly.

1.2. The referee puts a hat of five possible colors on the head of each of two sages. Each of them sees the hat of the other, but does not see his own hat. Each of them try to guess correctly the color of his own hat. The first sage writes on his own paper two colors and the second — three colors simultaneously. Prove that the sages can come to an agreement in the meeting before test in such a way that at least one of them will guess correctly.

1.3. Five sages stand around the non-transparent baobab. Shah has put red, blue, yellow or green hat the head of each of the sages. Sage does not know the color of his own hat and sees only the two neighbouring sages. As usual, without any communication each sages must makes one assumptions about the colors of his hat. But they fear be too lucky. How they should act to guarantee that for any placement of hats no more than two sages guess correctly the colors of their hats?

1.4. Sultan examines six court sages. By the rule of the examination the sultan locates 5 sages in 5 pits positioned around a circle, and locates the sixth sage in the tower in the center of the circle. The sultan writes one of the numbers 1, 2 or 3 on the forehead of each of the first five sages and writes a number from 1 to 243 on the forehead of the central sage. The sage in the tower sees the numbers of all the other sages, and these sages see his number (but do not see each other). All the sages must simultaneously try to guess correctly their numbers: the sages in the pits must say two numbers and the sage in the tower — one number. The sultan has explained to the sages the rules of the examination beforehand and has given time to communicate before the beginning of the examination. Can the sages act so that at least one of them certainly guess correctly his number?

We identify a vertex of graph G and the sage located in it. We assume that the colors are numbered by 0, 1, 2, 3, ... and that the chest of sage v contains hats of colors from 0 to some number $h(v) - 1$.

The HATS game is the triple $\langle G, h, g\rangle$, where $G = \langle V, E\rangle$ — a graph, $h\colon V \to \mathbb{N}$ — a function that for each vertex v equals the number of colors of hats keeping in the chest in this vertex, $g\colon V \to \mathbb{N}$ — a function equal to the number of guesses of each sage. We call function h a «hatness», and g — a function of guesses or the number of attempts. For each non negative integer h we denote by $\star h$ the function on V possessing the constant value h. Instead of the notation $\langle G, h, \star 1\rangle$ we will use shorter notation $\langle G, h\rangle$.

1.5. Prove that if the game $\langle G, h, g\rangle$ is winning, then for each non negative integer k the game $\langle G, k \cdot h, k \cdot g\rangle$ is winning, too.

1.6. Game $\langle G, h, g\rangle$ is given. Let $K \subset G$ is anticlique (a set of vertices such that there is no edge connected any pair of them) and for each $v \in K$ $h(v) > g(v)$. Prove that there exists a hats placement, for which none of the sages in K guesses correctly.

1.7. Let h and g be natural numbers, $G = \langle G, \star h, \star g\rangle$ be a winning game, $r' \leqslant \frac{h}{g}$ be a rational number. Prove that there exist natural numbers h' and g' such that $\frac{h'}{g'} = r'$ and game $\langle G, \star h', \star g'\rangle$ is winning.

1.8. Formulate and prove the analogue of the previous statement for non-constant functions of hatness and guessing.

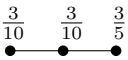
1.9. Denote by K_n a complete graph on n vertices. Prove that the game $\langle K_n, h, g\rangle$ is winning if and only if

$$\sum_{v \in K_n} \frac{g(v)}{h(v)} \geqslant 1.$$

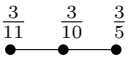
2 Paths and trees

The theory of HATS game on the complete graph K_3 is given by the problem statement 1.9. Now consider a path P_3 which is less complicated graph.

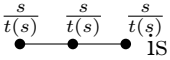
2.1. Prove that the sages lose in the game $\langle P_3, \star 3, \star 1\rangle$.

2.2. a) Prove that the game 

is winning (the numerator is the number of guesses, and the denominator is the hatness).

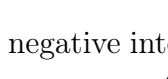
b) Prove that the game 

is losing.

c) Prove that the game 

is losing, where $t(s) = s^2 + s + 1$.

Let G be a graph and s be a non negative integer. Denote by $\mathrm{HG}_s(G)$ the s-hat number of G, i.e. the maximum number of hats h for which the game $\langle G, \star h, \star s\rangle$ is winning. For $s = 1$ this number is called hat number of G and is denoted by $\mathrm{HG}(G)$.

2.3. Prove that for any non negative integers n and s the game 

on path P_n is losing. Here all vertices except the leftmost vertex A have hatness $4s - 1$ and s guesses.

2.4. Prove that one can find n such that $\mathrm{HG}_2(P_n) = 6$, $\mathrm{HG}_3(P_n) = 10$, $\mathrm{HG}_4(P_n) = 14$.

2.5. Prove that for any non negative integer s the game $\langle P_n, \star(4s - 2), \star s\rangle$ is winning for $n \geqslant 2s$.

2.6. a) Let $t(s) = s^2 + s + 1$. Prove that for each tree T the game $\langle T, \star t(s), \star s\rangle$ is losing.

b) Len $K_{1,n}$ be "a star" graph (i.e. a tree consisting of a root and n leaves). Prove that for sufficiently large n the game $\langle K_{1,n}, \star(s^2 + s), \star s\rangle$ is winning.

c) Prove that for any non negative integer h there exists integer n such that the game on graph $K_{1,n}$ is winning if all the sages in pendant vertices have one guess and hatness 3, and the central sage has 2 guesses and hatness h.

3 Constructors

3.1. Let $\langle G, h, g\rangle$ be a winning game, A_1 and A_2 be vertices of G, not connected with an edge and such that $h(A_1) = h(A_2)$. We glue vertices A_1 and A_2 of G into one new vertex A, denote by $\widetilde{G}$ the obtained graph. Let functions $\widetilde{h}$ and $\widetilde{g}$ defined on the set of vertices of $\widetilde{G}$ coincide with h and g in all vertices except A_1 and A_2, and $\widetilde{h}(A) = h(A_1)$, $\widetilde{g}(A) = g(A_1) + g(A_2)$. Then the game $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ is also winning. (And then if the game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is losing, then the game $\langle G, h, g\rangle$ is losing too.)

Let $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$, $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be two games such that $V_1 \cap V_2 = \{v\}$. Let $G = G_1 +_v G_2$ be the union of graphs G_1 and G_2, in which both vertices v are glued into one new vertex. Define functions $h, g\colon V_1 \cup V_2 \to \mathbb{N}$:

$$h(u) = \begin{cases} h_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ h_1(v)h_2(v), & u = v, \end{cases} \qquad g(u) = \begin{cases} g_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ g_1(v)g_2(v), & u = v. \end{cases}$$

We say that the game $\mathcal{G} = \langle G, h, g\rangle$ is a product of games $\mathcal{G}_1$ and $\mathcal{G}_2$ and denote it by $\mathcal{G}_1 \times_v \mathcal{G}_2$ (fig. 1).

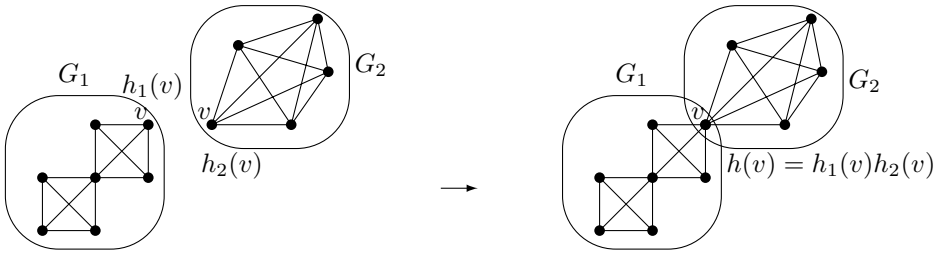


Рис. 1. The product $G_1 \times_v G_2$

3.2. The theorem about the product. If the sages win in games $\mathcal{G}_1$ and $\mathcal{G}_2$, then they also win in game $\mathcal{G}_1 \times_v \mathcal{G}_2$.

3.3. Let $G = G_1 +_A G_2$, where G_1 and G_2 are graphs, for which $V(G_1) \cap V(G_2) = \{A\}$. Let games $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ and $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be losing, and the following conditions hold:

$$g_1(A) = g_2(A) = s, \qquad h_1(A) \geqslant h_2(A) = s + 1.$$

Then game $\mathcal{G} = \langle G_1 +_A G_2, h\rangle$ is losing, where

$$h(x) = \begin{cases} h_i(x), & x \in V_i \setminus \{A\}\ (i = 1, 2),\\ h_1(A), & x = A, \end{cases} \qquad g(x) = \begin{cases} g_i(x), & x \in V_i \setminus \{A\}\ (i = 1, 2),\\ s, & x = A. \end{cases}$$

3.4. A half-edge removal. Let $\langle G, h, g\rangle$ be a winning game, AB be an edge of graph G, $\widetilde{G}$ be the graph obtained from G by replacing edge AB by directed edge $B \to A$ (i.e. sage A does not see sage B, but B sees A). Let function $\widetilde{g}$ on the vertices of graph G coincide with g in all vertices except A, and $\widetilde{g}(A) = h(B)g(A)$. Then game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is winning too. (And therefore, if game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is losing, then $\langle G, h, g\rangle$ is also losing.)

3.5. Substitution theorem. Let $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ be $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be winning games. Let A be an arbitrary vertex of graph G_2. Consider the new graph G obtained from G_2 by substitution of graph G_1 on the place of vertex v (each vertex G_1 is connected with former neighbours of vertex A by new edges, see fig. 2). Then game $\langle G, h, g\rangle$ is winning, where

$$h(u) = \begin{cases} h_2(u), & u \in V(G_2) \setminus \{A\},\\ h_1(u)h_2(A), & u \in V(G_1), \end{cases} \qquad g(u) = \begin{cases} g_2(u), & u \in V(G_2) \setminus \{A\},\\ g_1(u)g_2(A), & u \in V(G_1). \end{cases}$$

3.6. Substitution with reducing. Let $\mathcal{G} = \langle G, h, \star s\rangle$, $\mathcal{G}' = \langle G', h', g'\rangle$ be winning games. Let A be a vertex of graph G', and $h'(A) = s$. Let $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ be the winning game obtained by the substitution of

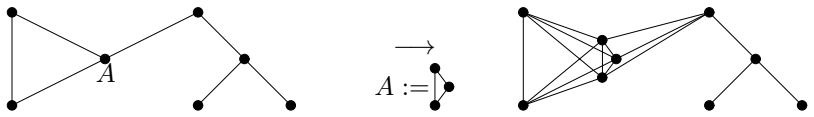


Рис. 2. Substitution of a graph on the place of vertex A.

game $\mathcal{G}$ on the place of vertex A to game $\mathcal{G}'$ (as in problem 3.5). By the rule of the substitution for all substituting vertices v

$$\widetilde{h}(v) = h(v)h'(A) = s \cdot h(v), \qquad \widetilde{g}(v) = g(v)g'(A) = s \cdot g'(A).$$

Consider new functions h^*, g^* on graph $\widetilde{G}$, which differ from $\widetilde{h}$, $\widetilde{g}$ only by the values in substituting vertices v, and this difference is the cancellation by s:

$$h^*(v) = h(v), \qquad g^*(v) = g'(A).$$

Then game $\langle \widetilde{G}, h^*, g^* \rangle$ is also winning.

3.7. Blowing up of a vertex. Let $\mathcal{G} = \langle G, h, g \rangle$ be winning game, $A \in V(G)$, $\widetilde{G}$ be the graph obtained from G by the substitution of clique B consisting of $g(A)$ vertices on the place of vertex A. Then game $\langle \widetilde{G}, \widetilde{h}, \widetilde{g} \rangle$ is also winning, where

$$\widetilde{h}(v) = \begin{cases} h(v), & v \in V(G) \setminus \{A\}, \\ h(A), & v \in B, \end{cases} \qquad \widetilde{g}(v) = \begin{cases} g(v), & v \in V(G) \setminus \{A\}, \\ 1, & v \in B. \end{cases}$$

4 "Petals" and "petunias"

We define a *petal graph* to be a graph G obtained from a path by adding a vertex v adjacent to every vertex of this path, see fig. 3, we say that v is the *stem* of G.

Then, we define a *petunia* to be a graph constructed in the following way. Take two petals L_1 and L_2, denote one vertex in each of them by v_1, and construct a graph $M_2 = L_1 +_{v_1} L_2$. After that consider graph M_2 and a new petal L_3 denote one vertex in each of them by v_2, and construct a graph $M_3 = M_2 +_{v_2} L_3$ and so on.

A *royal petunia* is a petunia (рис. 4), for which the vertex v_i in each step of its construction were chosen as the stem of petal L_{i+1}.

4.1. Let G be a petal of n vertices, see fig. 3, let the stem has hatness 2 and the other vertices have hatness 7. Prove that the sages lose in the game $\langle G, h \rangle$.

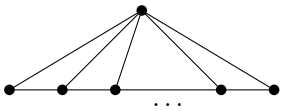


Рис. 3. A petal of n vertices

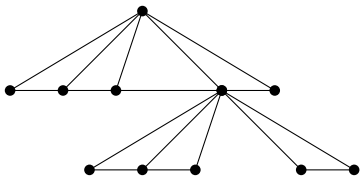


Рис. 4. A royal petunia

4.2. Let G be a petal of n vertices, $f(s) = s^2 + s$. Prove that $\mathrm{HG}_s(G) \leqslant f(f(s))$.

4.3. Let M be a petunia, h_s be maximum integer such that the game $\langle M, \star h_s, \star s \rangle$ is winning. Prove that $h_s \leqslant f(f(f(s)))$.

4.4. a) Prove that $\mathrm{HG}_s(G) = 4s(s+1) - 2$, where G is a petal of $n \geqslant 2s + 1$ vertices (fig. 3).

b) Prove the same equality if G is a royal petunia.

Paint my hat in 3.5 colors!

K. Kokhas, A. Latyshev

Project team: O. Bursian, D. Kokhas, K. Kokhas, V. Retinskiy

1 Let us introduce: the HATS game!

Let an undirected graph G be given, one sage and one chest with hats of different colors are located in each of its vertices. All the sages are acquainted with each other. Graph G, the location of the sages in the vertices of the graph and the colors of hats in all chests are fixed and known to everybody. In particular, each sage understands, in which vertex each of the others sages is located. The referee performs the following test with the sages. He puts a hat on the head of each sage, the hat is taken from the sage's chest. Each sage sees only the hats of the sages located in the neighbouring vertices of the graph, he does not see his own hat and does not know its color. The sages cannot communicate during the test. At the command of the referee each of the sages writes names of several colors on his paper simultaneously (how many colors the sages has to mention, is determined by the additional rule). We say that the sages have passed the test successfully = "have won", if at least one of them wrote the color of his hat in his paper.

The sages have been informed of the rules of the test before the testing and they have the possibility to hold a meeting, in which they must to define their public strategy. The publicity means that all the participants, including the referee, know this strategy. The strategy of the sages has to be deterministic, that is each sage has to write colors on his paper looking only the colors that he sees on his neighbours. We call the strategy *winning* if for any hats placement at least one sage will guess correctly the color of the hat on his head, i. e. mention this color in the his list of guesses. We say that the sages win, if they have a winning strategy, and that they lose, if they have not.

Therefore, the HATS game is not a game in a sense as it is ordinarily understood. This game lasts only one move.

1.1. The referee puts a hat of white, blue, red or green color on the head of each of two sages. Each of them sees the hat of the other, but does not see his own hat. Each of them writes on his own paper two colors simultaneously. They try to guess correctly the colors of their own hats. Prove that the sages can come to an agreement in the meeting before the test in such a way that at least one of them will guess correctly.

1.2. The referee puts a hat of five possible colors on the head of each of two sages. Each of them sees the hat of the other, but does not see his own hat. Each of them try to guess correctly the color of his own hat. The first sage writes on his own paper two colors and the second — three colors simultaneously. Prove that the sages can come to an agreement in the meeting before test in such a way that at least one of them will guess correctly.

1.3. Five sages stand around the non-transparent baobab. Shah has put red, blue, yellow or green hat the head of each of the sages. Sage does not know the color of his own hat and sees only the two neighbouring sages. As usual, without any communication each sages must makes one assumptions about the colors of his hat. But they fear be too lucky. How they should act to guarantee that for any placement of hats no more than two sages guess correctly the colors of their hats?

1.4. Sultan examines six court sages. By the rule of the examination the sultan locates 5 sages in 5 pits positioned around a circle, and locates the sixth sage in the tower in the center of the circle. The sultan writes one of the numbers 1, 2 or 3 on the forehead of each of the first five sages and writes a number from 1 to 243 on the forehead of the central sage. The sage in the tower sees the numbers of all the other sages, and these sages see his number (but do not see each other). All the sages must simultaneously try to guess correctly their numbers: the sages in the pits must say two numbers and the sage in the tower — one number. The sultan has explained to the sages the rules of the examination beforehand and has given time to communicate before the beginning of the examination. Can the sages act so that at least one of them certainly guess correctly his number?

We identify a vertex of graph G and the sage located in it. We assume that the colors are numbered by 0, 1, 2, 3, ... and that the chest of sage v contains hats of colors from 0 to some number $h(v) - 1$.

The HATS game is the triple $\langle G, h, g\rangle$, where $G = \langle V, E\rangle$ — a graph, $h\colon V \to \mathbb{N}$ — a function that for each vertex v equals the number of colors of hats keeping in the chest in this vertex, $g\colon V \to \mathbb{N}$ — a function equal to the number of guesses of each sage. We call function h a "hatness", and g — a function of guesses or the number of attempts. For each non negative integer h we denote by $\star h$ the function on V possessing the constant value h. Instead of the notation $\langle G, h, \star 1\rangle$ we will use shorter notation $\langle G, h\rangle$.

1.5. Prove that if the game $\langle G, h, g\rangle$ is winning, then for each non negative integer k the game $\langle G, k \cdot h, k \cdot g\rangle$ is winning, too.

1.6. Game $\langle G, h, g\rangle$ is given. Let $K \subset G$ is anticlique (a set of vertices such that there is no edge connected any pair of them) and for each $v \in K$ $h(v) > g(v)$. Prove that there exists a hats placement, for which none of the sages in K guesses correctly.

1.7. Let h and g be natural numbers, $G = \langle G, \star h, \star g\rangle$ be a winning game, $r' \leqslant \frac{h}{g}$ be a rational number. Prove that there exist natural numbers h' and g' such that $\frac{h'}{g'} = r'$ and game $\langle G, \star h', \star g'\rangle$ is winning.

1.8. Formulate and prove the analogue of the previous statement for non-constant functions of hatness and guessing.

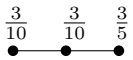
1.9. Denote by K_n a complete graph on n vertices. Prove that the game $\langle K_n, h, g\rangle$ is winning if and only if

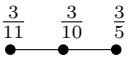
$$\sum_{v \in K_n} \frac{g(v)}{h(v)} \geqslant 1.$$

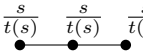
2 Paths and trees

The theory of HATS game on the complete graph K_3 is given by the problem statement 1.9. Now consider a path P_3 which is less complicated graph.

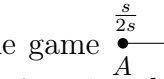
2.1. Prove that the sages lose in the game $\langle P_3, \star 3, \star 1\rangle$.

2.2. a) Prove that the game  is winning (the numerator is the number of guesses, and the denominator is the hatness).

b) Prove that the game  is losing.

c) Prove that the game  is losing, where $t(s) = s^2 + s + 1$.

Let G be a graph and s be a non negative integer. Denote by $\mathrm{HG}_s(G)$ the s-hat number of G, i.e. the maximum number of hats h for which the game $\langle G, \star h, \star s\rangle$ is winning. For $s = 1$ this number is called hat number of G and is denoted by $\mathrm{HG}(G)$.

2.3. Prove that for any non negative integers n and s the game  on path P_n is losing. Here all vertices except the leftmost vertex A have hatness $4s - 1$ and s guesses.

2.4. Prove that one can find n such that $\mathrm{HG}_2(P_n) = 6$, $\mathrm{HG}_3(P_n) = 10$, $\mathrm{HG}_4(P_n) = 14$.

2.5. Prove that for any non negative integer s the game $\langle P_n, \star(4s - 2), \star s\rangle$ is winning for $n \geqslant 2s$.

2.6. a) Let $t(s) = s^2 + s + 1$. Prove that for each tree T the game $\langle T, \star t(s), \star s\rangle$ is losing.

b) Len $K_{1,n}$ be "a star" graph (i.e. a tree consisting of a root and n leaves). Prove that for sufficiently large n the game $\langle K_{1,n}, \star(s^2 + s), \star s\rangle$ is winning.

c) Prove that for any non negative integer h there exists integer n such that the game on graph $K_{1,n}$ is winning if all the sages in pendant vertices have one guess and hatness 3, and the central sage has 2 guesses and hatness h.

3 Constructors

3.1. Let $\langle G, h, g\rangle$ be a winning game, A_1 and A_2 be vertices of G, not connected with an edge and such that $h(A_1) = h(A_2)$. We glue vertices A_1 and A_2 of G into one new vertex A, denote by $\widetilde{G}$ the obtained graph. Let functions $\widetilde{h}$ and $\widetilde{g}$ defined on the set of vertices of $\widetilde{G}$ coincide with h and g in all vertices except A_1 and A_2, and $\widetilde{h}(A) = h(A_1)$, $\widetilde{g}(A) = g(A_1) + g(A_2)$. Then the game $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ is also winning. (And then if the game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is losing, then the game $\langle G, h, g\rangle$ is losing too.)

Let $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$, $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be two games such that $V_1 \cap V_2 = \{v\}$. Let $G = G_1 +_v G_2$ be the union of graphs G_1 and G_2, in which both vertices v are glued into one new vertex. Define functions $h, g\colon V_1 \cup V_2 \to \mathbb{N}$:

$$h(u) = \begin{cases} h_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ h_1(v)h_2(v), & u = v,\end{cases} \qquad g(u) = \begin{cases} g_i(u), & u \in V_i \setminus \{v\},\ (i = 1, 2),\\ g_1(v)g_2(v), & u = v.\end{cases}$$

We say that the game $\mathcal{G} = \langle G, h, g\rangle$ is a product of games $\mathcal{G}_1$ and $\mathcal{G}_2$ and denote it by $\mathcal{G}_1 \times_v \mathcal{G}_2$ (fig. 1).

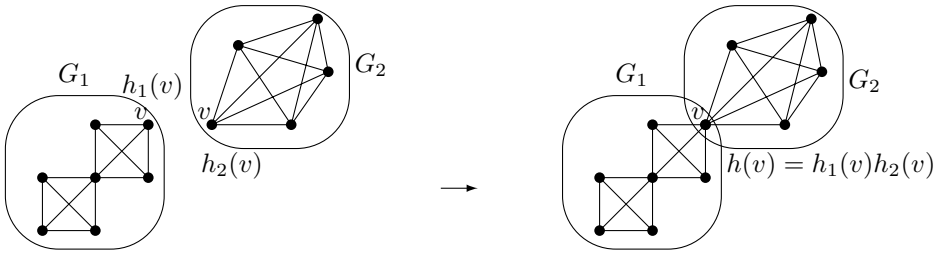


Figure 1. The product $G_1 \times_v G_2$

3.2. The theorem about the product. If the sages win in games $\mathcal{G}_1$ and $\mathcal{G}_2$, then they also win in game $\mathcal{G}_1 \times_v \mathcal{G}_2$.

3.3. Let $G = G_1 +_A G_2$, where G_1 and G_2 are graphs, for which $V(G_1) \cap V(G_2) = \{A\}$. Let games $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ and $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be losing, and the following conditions hold:

$$g_1(A) = g_2(A) = s, \qquad h_1(A) \geqslant h_2(A) = s + 1.$$

Then game $\mathcal{G} = \langle G_1 +_A G_2, h, g\rangle$ is losing, where

$$h(x) = \begin{cases} h_i(x), & x \in V_i \setminus \{A\}\ (i = 1, 2),\\ h_1(A), & x = A,\end{cases} \qquad g(x) = \begin{cases} g_i(x), & x \in V_i \setminus \{A\}\ (i = 1, 2),\\ s, & x = A.\end{cases}$$

3.4. A half-edge removal. Let $\langle G, h, g\rangle$ be a winning game, AB be an edge of graph G, $\widetilde{G}$ be the graph obtained from G by replacing edge AB by directed edge $B \to A$ (i e. sage A does not see sage B, but B sees A). Let function $\widetilde{g}$ on the vertices of graph G coincide with g in all vertices except A, and $\widetilde{g}(A) = h(B)g(A)$. Then game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is winning too. (And therefore, if game $\langle\widetilde{G}, h, \widetilde{g}\rangle$ is losing, then $\langle G, h, g\rangle$ is also losing.)

3.5. Substitution theorem. Let $\mathcal{G}_1 = \langle G_1, h_1, g_1\rangle$ be $\mathcal{G}_2 = \langle G_2, h_2, g_2\rangle$ be winning games. Let A be an arbitrary vertex of graph G_2. Consider the new graph G obtained from G_2 by substitution of graph G_1 on the place of vertex v (each vertex G_1 is connected with former neighbours of vertex A by new edges, see fig. 2). Then game $\langle G, h, g\rangle$ is winning, where

$$h(u) = \begin{cases} h_2(u), & u \in V(G_2) \setminus \{A\},\\ h_1(u)h_2(A), & u \in V(G_1),\end{cases} \qquad g(u) = \begin{cases} g_2(u), & u \in V(G_2) \setminus \{A\},\\ g_1(u)g_2(A), & u \in V(G_1).\end{cases}$$

3.6. Substitution with reducing. Let $\mathcal{G} = \langle G, h, \star s\rangle$, $\mathcal{G}' = \langle G', h', g'\rangle$ be winning games. Let A be a vertex of graph G', and $h'(A) = s$. Let $\langle\widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ be the winning game obtained by the substitution of

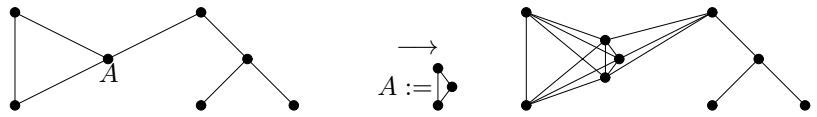


Figure 2. Substitution of a graph on the place of vertex A.

game $\mathcal{G}$ on the place of vertex A to game $\mathcal{G}'$ (as in problem 3.5). By the rule of the substitution for all substituting vertices v

$$\widetilde{h}(v) = h(v)h'(A) = s \cdot h(v), \qquad \widetilde{g}(v) = g(v)g'(A) = s \cdot g'(A).$$

Consider new functions h^*, g^* on graph $\widetilde{G}$, which differ from $\widetilde{h}$, $\widetilde{g}$ only by the values in substituting vertices v, and this difference is the cancellation by s:

$$h^*(v) = h(v), \qquad g^*(v) = g'(A).$$

Then game $\langle \widetilde{G}, h^*, g^* \rangle$ is also winning.

3.7. Blowing up of a vertex. Let $\mathcal{G} = \langle G, h, g \rangle$ be winning game, $A \in V(G)$, $\widetilde{G}$ be the graph obtained from G by the substitution of clique B consisting of $g(A)$ vertices on the place of vertex A. Then game $\langle \widetilde{G}, \widetilde{h}, \widetilde{g} \rangle$ is also winning, where

$$\widetilde{h}(v) = \begin{cases} h(v), & v \in V(G) \setminus \{A\}, \\ h(A), & v \in B, \end{cases} \qquad \widetilde{g}(v) = \begin{cases} g(v), & v \in V(G) \setminus \{A\}, \\ 1, & v \in B. \end{cases}$$

4 "Petals" and "petunias"

We define a *petal graph* to be a graph G obtained from a path by adding a vertex v adjacent to every vertex of this path, see fig. 3, we say that v is the *stem* of G.

Then, we define a *petunia* to be a graph constructed in the following way. Take two petals L_1 and L_2, denote one vertex in each of them by v_1, and construct a graph $M_2 = L_1 +_{v_1} L_2$. After that consider graph M_2 and a new petal L_3 denote one vertex in each of them by v_2, and construct a graph $M_3 = M_2 +_{v_2} L_3$ and so on.

A *royal petunia* is a petunia (рис. 4), for which the vertex v_i in each step of its construction were chosen as the stem of petal L_{i+1}.

4.1. Let G be a petal of n vertices, see fig. 3, let the stem has hatness 2 and the other vertices have hatness 7. Prove that the sages lose in the game $\langle G, h \rangle$.

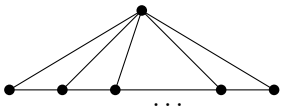


Figure 3. A petal of n vertices

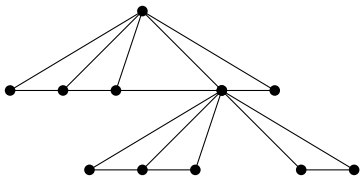


Figure 4. A royal petunia

4.2. Let G be a petal of n vertices, $f(s) = s^2 + s$. Prove that $\mathrm{HG}_s(G) \leqslant f(f(s))$.

4.3. Let M be a petunia, h_s be maximum integer such that the game $\langle M, \star h_s, \star s \rangle$ is winning. Prove that $h_s \leqslant f(f(f(s)))$.

4.4. a) Prove that $\mathrm{HG}_s(G) = 4s(s+1) - 2$, where G is a petal of n vertices for sufficiently large n (fig. 3).

b) Prove the same equality if G is a royal petunia that hat sufficiently big petals.

5 Problems after intermediate finish

To section 1

5.1. Let $K_{1,n}$ be a "star" graph, and $h = (h_0, \ldots, h_n)$, $g = (g_0, \ldots, g_n)$ be arbitrary functions of hatness and number of attempts, where $1 \leqslant g_i \leqslant h_i$ for all i, the zero index corresponds to the central vertex of the graph. Prove that the existence of k, for which $\langle K_{1,n}, k \cdot h, k \cdot g\rangle$ is winning, is equivalent to the inequality

$$\frac{g_0}{h_0} \geqslant \prod_{i=1}^{n} \left(1 - \frac{g_i}{h_i}\right).$$

To section 2

5.2. Let h and g be positive integers, and $g^2 - 3gh + h^2 < 0$. Prove that game $\langle P_3, \star h, \star g\rangle$ is winning.

Fractional hat guessing number of graph G we call the value $\hat{\mu}(G) = \sup\{\frac{h}{g} \colon \langle G, \star h, \star g\rangle \text{ is winning}\}$. As it follows from problem 1.9, $\mathrm{HG}(K_n) = \hat{\mu}(K_n) = n$, $\mathrm{HG}_s(K_n) = sn$. In the general case, $\hat{\mu}(K_n) \geqslant \frac{1}{s}\mathrm{HG}_s(G) \geqslant \mathrm{HG}(G)$.

5.3. Prove that $\hat{\mu}(K_3) = \frac{3+\sqrt{5}}{2}$.

To section 3

5.4. Let $\langle G_2, h_2\rangle$ be a losing game, $H_2 \subset G_2$ be a clique in G_2. Let G_1 be a complete graph. Define a hatness function h_1 on it in such a way that the relation

$$\left(\sum_{u \in G_1} \frac{1}{h_1(u)}\right)\left(\prod_{v \in H_2} h_2(v)\right) < 1$$

holds. Let G be the graph obtained by union of graphs G_1 and G_2 with adding all edges between vertices G_1 and H_2 (fig. 5). Prove that game $\langle G, h\rangle$ is losing if

$$h(v) = \begin{cases} h_1(v), & v \in G_1, \\ h_2(v), & v \in G_2. \end{cases}$$

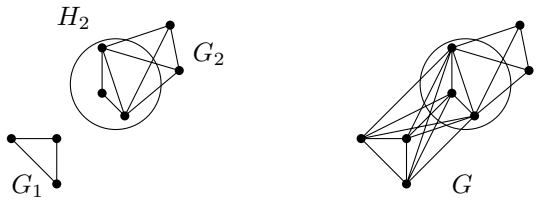


Figure 5. Example to problem 5.4. The number of vertices in G_1 and H_2 should not necessarily coincide

5.5. Let $\mathcal{G} = \langle G, h\rangle$ be a losing game, A be an arbitrary vertex of graph G. Consider graph $G' = (V', E')$ obtained by adding to graph G new pendant vertex B: $V' = V \cup \{B\}$, $E' = E \cup \{AB\}$. Then the sages lose in game $\langle G', h'\rangle$, where $h'(B) = 2$, $h'(A) = 2h(A) - 1$ and $h'(u) = h(u)$ for other vertices $u \in V$.

5.6. Let $\mathcal{G} = \langle G, h, g\rangle$ be a game, a vertex $A \in V(G)$ be connected with all other vertices of G, $h(A) = s + 1$, $g(A) = s$, and $\mathcal{G}' = \langle G \setminus \{A\}, h', (s+1) \cdot g'\rangle$, where $h' = h\Big|_{V(G)\setminus\{A\}}$, $g' = g\Big|_{V(G)\setminus\{A\}}$. Then the games $\mathcal{G}$ and $\mathcal{G}'$ are equivalent.

To section 5

5.7. a) A winning graph G contains a "long bridge" — two-link path ABC, such that after removing this path the graph falls into two components of connectivity: G_1 (containing vertex A) and G_2 (containing vertex C). Let hatness of vertex B equals 5. Prove that at least one of the games $\langle G_1, h\big|_{G_1}\rangle$, $\langle G_2, h\big|_{G_2}\rangle$ is winning.

b) Let graph $\widetilde{G}$ is obtained by subpartition of an arbitrary graph G (i. e. each edge of graph G has been replaced by two-link path). Prove that game $\langle \widetilde{G}, \star 5\rangle$ is losing.

5.8. Let $\mathcal{G} = \langle G, h\rangle$ be a winning game, and it is maximal in the following sense: when hatness function increase in any vertex, the sages lose and, besides that, there does not exist a subgraph of G, on which the sages can win with hatness function h. Suppose that graph G contains edge-bridge AB. Prove that game $\mathcal{G}$ can be represented as the product of games.

5.9. Sages A and B have 1 guess, see each other and all other sages in the graph (and the others see them), $h(A) = 2$, $h(B) = 3$. Prove that if to replace these two sages by one sage C that sees the others, and the others see him, and $h(C) = 6$, $g(C) = 5$, then the result of the game does not change.

5.10. Given natural numbers s and d. Let G be an arbitrary graph, the vertices of which are partitioned into two sets $V(G) = A \cup B$, and each vertex of A has no more than d neighbours from B. Prove that $\mathrm{HG}_s(G) \leqslant \mathrm{HG}_{s'}(G[A])$, where $s' = s(\mathrm{HG}_s(G[B]) + 1)^d$, $G[A]$ and $G[B]$ are induced subgraphs on sets A and B.

Solutions

1.1. Let us call white and red colors light, and blue and green colors dark. Then let the first sage write both dark colors, if he sees on the second a light color, and vice versa; and the second sage write both light colors, if he sees on the first a light color, and vice versa. It is not difficult to understand that at least one of the sages guesses correctly.

1.2. Renumber the hat colors from 1 to 5. Then let the first player write colors under the assumption that the sum of the numbers on the hats of the first and the second sages gives remainder 0 or 1 mod 5, and the second — under the assumption that the same sum gives remainder 2, 3 or 4 mod 5. Since the sum really gives some remainder, the sage with the correct assumption guesses correctly his color.

1.3. First remind how to play the game, when there are only two sages: the hats can be colored in only two colors (denote the colors by 0 and 1) and it is required that somebody necessarily guessed correctly. Here is a strategy: one sage (call him equalizer) checks hypothesis "the hat colors are identical", the other (distinguisher) — "the hat colors are different". Note that by this strategy for any hats placement one of the sages guesses correctly and the other does not.

Consider a visibility graph: the sages are vertices, the pairs of neighbouring sages are edges, then this graph is a cycle on five vertices. Denote its edges by a, b, c, d, e. We assume that the color of sage's hat is a two-digit binary number: 00, 01, 10 or 11; writing this number we will mark its bits by the labels of the edges incident to the vertex. For example, if there are two outgoing edges a and b from the vertex, then we subscribe one of the bits "a", and the other — "b" (the order of labels is not important, all the neighbours of the sage see this labelling).

Let the sages at the endpoints of each edge come to agreement, who on this edge is equalizer, and who is distinguisher. The guessing on each edge x happens as follows: each sage on this edge looks only at bit x of his neighbour's color and calculates the color of his own bit x in accordance with his role on this edge. Therefore, each sage casting a glance to the left and to the right, calculates both bits and names the obtained color as his answer.

It is evident that a sage guesses correctly the color of his hat only if he has guessed correctly both bits. Since the graph contains only 5 edges, only 5 bits have been guessed correctly, and hence, at most two sages have guessed correctly the colors of their hats.

1.4. Put into correspondence to each color of the central sage the sequence of 5 digits, each of which is 1, 2 or 3. The strategy of i-th sage in pit: look at i-th digit of the central sage and name the other two digits. The strategy of the central sage: name the color, i-th digit of which is equal to the digit of i-th sage from pit. If no sage from pit has guessed correctly, then the central guesses his color correctly.

1.5. For each sage v consider $k \cdot h(v)$ hat colors and split them into $h(v)$ groups containing k colors each, we call them megacolors. Then in game $\langle G, k \cdot h, k \cdot g\rangle$ each sage v can understand megacolors of all his neighbours, and, according to the strategy for game $\langle G, h, g\rangle$, name $g(v)$ of his own megacolors. But these $g(v)$ megacolors correspond to $k \cdot g(v)$ usual colors. It is not difficult to see that if the strategy for game $\langle G, h, g\rangle$ is winning, then the obtained strategy is winning too.

1.6. Give arbitrary hats to the sages that are not from K. Then all answers of the sages from K according the strategy are determined. It remains to give a hat to each of them such that he will not guess correctly.

1.7. Let $r' = \frac{p}{q}$. If $G = \langle G, \star h, \star g\rangle$ is winning, then game $\langle G, \star ph, \star pg\rangle$ is also winning. And since $\frac{p}{q} \leqslant \frac{h}{g}$, then $pg \leqslant qh$, whence game $\langle G, \star ph, \star qh\rangle$ is also winning, because the increasing of the number of attempts cannot destroy the working strategy.Then $h' = ph$, $q' = qh$ are the desired.

1.8. Let $G = \langle G, h, g\rangle$ be a winning game, $r' \colon V \to \mathbb{Q}$ be a function such that $0 < r'(v) \leqslant \frac{h(v)}{g(v)}$ for all v. Prove that there exist functions h' and g', for which $\frac{h'(v)}{g'(v)} = r'(v)$ for all v, and game $\langle G, h', g'\rangle$ is winning.

Proof. Let $r'(v) = \frac{p(v)}{q(v)}$. Denote $P = \prod_v p(v)$. Then game $\langle G, P \cdot h, P \cdot g\rangle$ is winning by problem 1.5. Since $\frac{p(v)}{q(v)} \leqslant \frac{h(v)}{g(v)}$, then by increasing the number of attempts in some vertices we obtain a winning game $\left\langle G, P \cdot h, \frac{P}{p} \cdot qh\right\rangle$. Therefore, $h' = P \cdot h$, $g'(v) = \frac{P}{p(v)} \cdot q(v)h(v)$ are the desired.

1.9. *"If" case.* Note that sage v guesses correctly in $\frac{g(v)}{h(v)}$ fraction of placements of all hats. And since in each placement at least one sage guesses correctly, the sum of these fractions is at least 1.

"Only if" case. We will show that if the inequality holds, then the sages have a winning strategy.

Let $H = \prod_v h(v)$. Code the hat colors by numbers from 0 to $H-1$: for each sage v let the possible color $i \in \{0, 1, \ldots, h(v)-1\}$ of his hat correspond to the remainder $\frac{iH}{h(v)}$ modulo H. In other words the set of reminders

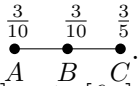
$$0, \quad \frac{H}{h(v)}, \quad \frac{2H}{h(v)}, \quad \ldots, \quad \frac{(h(v)-1)H}{h(v)} \pmod H. \qquad (*)$$

is a set of possible hats colors of sage v. When the hats placement is given, let S be the sum of numbers of all hats modulo H. The sages do not know the value of S, but each sage v can calculate value S_v that is the sum of the numbers of the hats, that the devilkin has given to the other sages, modulo H.

The strategy of the sages is the following: each sage v checks the hypothesis $S \in [a_v, b_v)$, where $[a_v, b_v)$ is an interval of length $\frac{Hg(v)}{h(v)}$, containing $\frac{Hg(v)}{h(v)}$ consecutive remainders modulo H, these intervals the sages choose in their meeting before the test. In order to check the hypothesis sage v has to solve the "inequality": he finds, for which reminder x the inclusion $S_v + x \in [a_v, b_v)$ is satisfied. After solving this problem he obtain a list $\frac{Hg(v)}{h(v)}$of possible values of x, but this list contains only $g(v)$ remainders of the form $(*)$. Then sage v will name $g(v)$ corresponding to them colors.

The given inequality in the problem statement is equivalent to the fact that the sum of lengths of all segments $[a_v, b_v)$ is at least H. If it holds, then, evidently, we can assign to each sage one segment in such a way that each remainder modulo H belongs to at least one of the segments. It guarantees the victory of the sages: whatever the sum of hats is equal, at least one of the sages will make right assumption and will guess correctly.

2.1. The sages cannot win even in game $\langle P_3, \star 3k, \star k\rangle$. It follows from the inequality of problem 5.1.

2.2. a) Denote the sages by A, B and C: 

. We will demonstrate the winning strategy for the sages. Let sage C name colors $[\frac{c_B}{2}]$, $[\frac{c_B}{2}]+1$, $[\frac{c_B}{2}]+2$ mod 5, and sage A name colors c_B, c_B+3, c_B+6 mod 10. Sage B, casting glances at the neighbours, suspects that they both do not guess correctly only if

$$c_B \notin S = \{c_A, c_A-3, c_A-6, 2c_c, 2c_C+1, 2c_C+2, 2c_C+3, 2c_C+4, 2c_C+5\}.$$

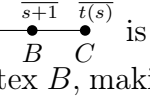
It remains to note that for the remainders modulo 10 the inclusion

$$\{c_A, c_A-3, c_A-6\} \subset \{2c_c, 2c_C+1, 2c_C+2, 2c_C+3, 2c_C+4, 2c_C+5\}$$

is impossible for any c_A and c_C. Therefore, set S contains at least 7 elements, and sage B can name in his answer the three (or less) remainders, not belonging to the set.

b) For every possible color c_B sage A makes three guesses, i. e. he names 30 answers of 11-element set of A's colors. Therefore, he names some color 1 or 2 times. Give the hat of this color to sage A. Then sage B will suspect, for which 8 colors of his hat sage A do not guess correctly. But the game 

is losing, and any strategy that is used by our sages in the above situation, is immediately reduced to the strategy in this losing game.

c) It is sufficient to verify that game 

is losing. Apply the statement of the constructor "removing a half-edge" (problem 3.4) for vertex B, making this vertex invisible for A and C. As a result

vertices A and C see nobody, have hatness s^2+s+1 and s^2+s guesses. Therefore, the referee can give them such hats that they will not guess correctly. After that the strategy of sage B is completely determined, he has hatness $s+1$ and s guesses, so he will not guess correctly too.

Another solution can be obtained by standard "probabilistic" observations: the number of hats placements, for which sage v guesses correctly, does not exceed fraction $g(v)/h(v)$ of the total number of placements. We need only note that for our graph $\frac{3s}{s^2+s+1} < 1$ for $s > 1$.

2.3. For each natural we s prove the statement by induction on n. Base case $n = 1$, i. e. the loss in game $\overset{\frac{s}{2s}}{\underset{A}{\bullet}}\!\!-\!\!\overset{\frac{s}{4s-1}}{\underset{B}{\bullet}}$ follows from the statement of problem 1.9.

Induction step. Consider three leftmost vertices A, B, C. Consider all possible hat color assignments to sage B. Sage A names $s(4s-1)$ colors from set $\{0, 1, 2, \ldots, 2s-1\}$ in total. Therefore some color c_A occurs in his answers at most $[\frac{s(4s-1)}{2s}] = 2s-1$ times. Give to sage A the hat of this color. Then sage B sees color c_A and knows, for which $2s-1$ colors of his hat sage A names color c_A. So sage B may assume that the color of his own hat is taken from set C_B consisting of $4s-1-(2s-1) = 2s$ colors. At that moment the devilkin (the other name of the referee) declares that in current hats placement the color of B's hat belongs to C_B and inform the other sages what is the set C_B. Then the game from induction step takes place on the remained graph and it is losing.

2.4. The inequality $\mathrm{HG}_2(P_4) \geqslant 6$ holds because the product of games $\overset{\frac{2}{6}}{\bullet}\!\!-\!\!\overset{\frac{2}{3}}{\underset{v_1}{\bullet}}$ $\times_{v_1}$ $\overset{\frac{1}{2}}{\underset{v_1}{\bullet}}\!\!-\!\!\overset{\frac{1}{2}}{\underset{v_2}{\bullet}}$ $\times_{v_2}$ $\overset{\frac{2}{3}}{\underset{v_2}{\bullet}}\!\!-\!\!\overset{\frac{2}{6}}{\bullet}$ is winning by theorem of product.

The inequality $\mathrm{HG}_3(P_6) \geqslant 10$ holds since the game $\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{5}}{\underset{v_1}{\bullet}}$ $\times_{v_1}$ $\overset{\frac{1}{2}}{\underset{v_1}{\bullet}}\!\!-\!\!\overset{\frac{1}{2}}{\underset{v_2}{\bullet}}$ $\times_{v_2}$ $\overset{\frac{3}{5}}{\underset{v_2}{\bullet}}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}\!\!-\!\!\overset{\frac{3}{10}}{\bullet}$ is winning (the leftmost and rightmost multipliers are winning by problem 2.2).

Finally, the inequality $\mathrm{HG}_4(P_{10}) \geqslant 14$ holds as a result of the fact that game $G(u) \times_u \overset{\frac{1}{2}}{\underset{u}{\bullet}}\!\!-\!\!\overset{\frac{1}{2}}{\underset{w}{\bullet}}$ $\times_w G(w)$ is winning, where $G(u) = \overset{\frac{4}{15}}{\bullet}\!\!-\!\!\overset{\frac{4}{5}}{\underset{v_1}{\bullet}}$ $\times_{v_1}$ $\overset{\frac{1}{3}}{\underset{v_1}{\bullet}}\!\!-\!\!\overset{\frac{2}{3}}{\underset{v_2}{\bullet}}$ $\times_{v_2}$ $\overset{\frac{2}{5}}{\underset{v_2}{\bullet}}\!\!-\!\!\overset{\frac{4}{14}}{\bullet}\!\!-\!\!\overset{\frac{4}{7}}{\underset{u}{\bullet}}$.

In view of the statement of problem 2.3 any game in the form $\overset{\frac{s}{4s-1}}{\underset{A}{\bullet}}\!\!-\!\!\overset{\frac{s}{4s-1}}{\bullet}\!\!-\!\!\overset{\frac{s}{4s-1}}{\bullet}\!\!-\!\!\cdots$ is losing (as compared to problem 2.3 here the hatness of vertex A has been increased). For $s = 2, 3, 4$ this gives, by the way, for all n the inequalities $\mathrm{HG}_2(P_n) \leqslant 6$, $\mathrm{HG}_3(P_n) \leqslant 10$, $\mathrm{HG}_4(P_n) \leqslant 14$.

2.5. Consider a hatness function h on graph P_s:

$$h(v_i) = \begin{cases} 4s-2 & \text{for } 1 \leqslant i < s, \\ 2s-1 & \text{for } i = s. \end{cases}$$

To prove the statement of the problem it is sufficient to verify that game $\langle P_s, h, \star s\rangle$ is winning. For construction of sages' strategy we need the following auxiliary statement — a theorem about game with hint.

Let game $\mathcal{G} = \langle G, h, g\rangle$ be winning under condition that the devilkin makes the following hint during the game. For one vertex $B \in V(G)$ a natural number $w_B \leqslant h(B)$ is fixed and it is known that the devilkin will come to sage B during the game and will tell him a set of w_B consecutive remainders (i. e. the set of remainders in the form x, $x+1$, …, $x+w_B \bmod h(B)$), containing the color of his hat; the other sages will not hear this hint. Vertex B, number w_B and the rule of proclaiming of the hint are known to the sages beforehand. Denote a game with hint by $\langle G, h, g, B, w_B\rangle$.

For example, game $\langle G, h, g, B, w_B\rangle$ is certainly winning in the case $w_B \leqslant g(B)$.

T h e o r e m. Let graph G contain vertex B, and graph $\tilde{G}$ be obtained from graph G by appending new vertex A and edge AB. Let hatness function $\tilde{h}$ and function of the number of guesses $\tilde{g}$ be given on graph $\tilde{G}$, and let $h = \tilde{h}\big|_{V(G)}$, $g = \tilde{g}\big|_{V(G)}$. Let for some natural numbers w_A, w_B such that $g(A) \leqslant w_A \leqslant h(A)$ and $g(B) \leqslant w_B \leqslant h(B)$, the conditions hold:

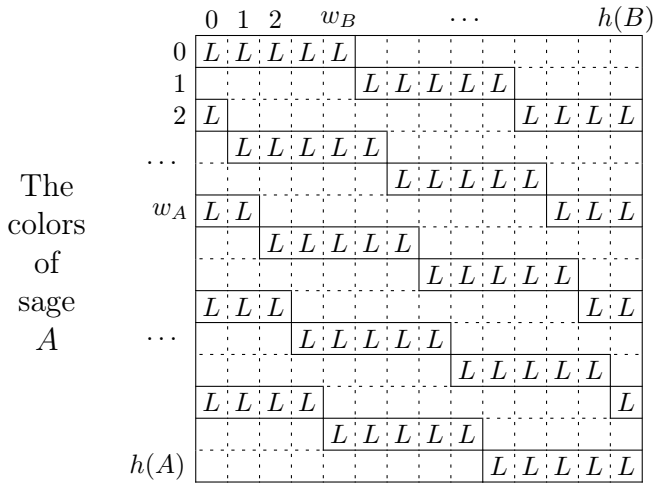


Figure 6. The strategy of sage A. Here $h(A) = 14$, $h(B) = 14$, $w_A = 6$, $w_B = 5$. In the construction of the table it is not required, but to complete the picture one can assume that $g(A) = 4$, $g(B) = 4$.

(i) game with hint $\langle G, h, g, B, w_B\rangle$ is winning,
(ii) $w_B \cdot h(A)$ is divisible by $h(B)$,
(iii) $w_A w_B \geqslant (w_A - g(A))h(B)$.
Then game with hint $\langle \tilde{G}, \tilde{h}, \tilde{g}, A, w_A\rangle$ is winning.

P r o o f. To describe the strategy of sage A, construct table $h(A) \times h(B)$, in which some squares are empty, and the others contain letters "L" by the following rule. Number the rows of the table by numbers from 0 to $h(A) - 1$, we identify the numbers of rows with possible colors of A's hat. Number the columns of the table by numbers from 0 to $h(B) - 1$, we identify the numbers of columns with possible colors of B's hat. For each i $(0 \leqslant i \leqslant h(A) - 1)$ we put letters "L" in the cells of i-th row in columns with numbers

$$iw_B, \quad iw_B + 1, \quad \ldots, \quad iw_B + w_B - 1 \pmod{h(B)} \tag{1}$$

(i. e. w_B letters "L" in total), see fig. 6. One may consider the obtained table as toroidal: calculations modulo $h(B)$ in rule (1) allow to identify $h(B)$-th column with zeroth column, and condition (ii) allows to identify $h(A)$-th row with zeroth row.

L e m m a. Consider arbitrary w_A consecutive rows of this table (taking into account its toroidal nature, i. e. one can take several lower rows and the corresponding number of upper rows). Then each column of the table contains at most $g(A)$ empty cells in these rows.

Proof. In view of toroidal nature of the table it is sufficient to verify this statement for the set of first w_A rows. Consider j-th column. It is evident that this column contains letter "L" in the entry at i-th row $(0 \leqslant i \leqslant w_A - 1)$ if and only if

$$0 \leqslant (j - iw_B) \bmod h(B) \leqslant w_B - 1. \tag{2}$$

In the integer sequence $d_i(j) = j - iw_B$ the distance between $d_0(j)$ and $d_{w_A-1}(j)$ is equal to

$$(w_A - 1)w_B.$$

By condition (iii) the inequality holds:

$$(w_A - 1)w_B \geqslant (w_A - g(A))h(B) - w_B,$$

which means that for each j inequality (2) has at least $w_A - g(A)$ solutions for variable i, i. e. each column of the table contains at least $w_A - g(A)$ letters "L" in the chosen w_A rows. Thus, it contains at most $g(A)$ empty squares. □

The hint that sage A receive from the devilkin is actually a set of w_A consecutive rows of the table. Then the strategy of sage A is to name the colors, corresponding to the numbers of the rows with empty cells in j-th column of the table, where j is the color of B's hat. Sage A can do it, because by lemma the rows indicated in the devilkin's hint contain at most $g(A)$ empty cells in j-th column.

Describe the strategy of sage B. He sees color i of the hat of sage A and concludes that A does not guess correctly only in the cases, when B's color corresponds to the columns containing letter "L" in i-th row. Therefore, B may think that his own color is given by the set of these w_B columns, and, receiving this hint, he plays with this hint by the strategy for graph G.

The theorem is proven.

Turn to the problem solution. We present the strategy for the sages.

For $k = 1, 3, \ldots, s-1$ denote by P_k a path on vertices $v_1, \ldots, v_k$ (it is a subgraph of P_s). Function h allows us to define the hatnesses of vertices $v_1, \ldots, v_k$. Check by induction on k ($1 \leqslant k \leqslant s$) that game with hint $\langle P_k, h, \star s, v_k, s+k-1\rangle$ is winning (remind that in this game the devilkin pointed to sage v_k the range of $s+k-1$ consecutive colors containing the color of his hat).

Base case $k = 1$: in game $\langle P_1, h, \star s, v_1, s\rangle$ the only player v_1 wins thanks to hint.

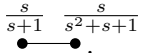
Inductive step $k \to k+1$, $k \leqslant s-2$. Let game with hint $\langle P_k, h, \star s, v_k, s+k-1\rangle$ be winning. Then by the proven theorem game $\langle P_{k+1}, h, \star s, v_{k+1}, s+k\rangle$ is winning too: here $B = v_k$, $w_B = s+k-1$, $G = \langle P_k, h, \star s, v_k, s+k-1\rangle$, $A = v_{k+1}$, $w_A = s+k$, $\tilde{G} = \langle P_{k+1}, h, \star s, v_{k+1}, s+k\rangle$. Condition ii) of theorem holds because $h(A) = h(B)$, and the condition iii) is provided by the inequality

$$w_A w_B = (s+k-1)(s+k) \underset{(*)}{\geqslant} k(4s-2) = (w_A - g(A))h(B),$$

where inequality $(*)$ is reduced to evident inequality $(s-k)^2 \geqslant s-k$.

The last step $k = s-1 \to s$ also holds by the proven theorem. It is verified similarly with the only difference that condition ii) holds due to the fact that number $w_B = 2s-2$ is even, and therefore $w_B \cdot h(A) = (2s-2)(2s-1)$ is divisible by $h(B) = 4s-2$.

Thus, we have proved that game with hint $\langle P_s, h, \star s, v_s, 2s-1\rangle$ is winning. But then game $\langle P_s, h, \star s\rangle$ is evidently winning too.

2.6. a) Solution 1. Induction by the number of vertices of the tree. Inductive step. The adding to the losing tree next pendant vertex can be interpreted as gluing of two losing games by constructor of problem 3.3, where one of the games is the game on tree $\langle T, \star t(s), \star s\rangle$, and another one is 

.

Solution 2. We prove the statement by induction on the number of tree vertices. Base case $n = 1$ is trivial. Prove the inductive step.

Let the sages choose some strategy f in game $\langle T, \star t(s), \star s\rangle$. The following two propositions hold.

P r o p o s i t i o n I. For each sage A at least $t(s) - s$ colors of his hat can be used for construction of "disproving" hats placements. By the other words, one can choose $t(s) - s$ colors and for each of them construct a hats placement, in which A's hat has the chosen color and none of the sages guesses.

P r o p o s i t i o n II. For any sage A and any set C of $s+1$ colors (of his hats) one can define the hat colors on set $N(A)$ (the set of neighbours of A) in such a way that after appending any hat $\alpha \in C$ for sage A to this placement one can supplement the obtained partial hats placement to the hats placement on the whole tree T so that none of the sages on $T \setminus \{A\}$ guesses correctly.

It is clear that proposition I follows from II. Besides that, from II the inductive step immediately follows: take any sage A and any set C of $s+1$ colors, then proposition II provides the hats placement on set $N(A)$, which uniquely determines what s colors are named by sage A in this game. Give to sage A a unnamed color from set C, then A will not guess correctly. By proposition II one can make so that the other sages will not guess correctly.

Proof of proposition II.

Take an arbitrary sage A and an arbitrary set C of $s+1$ colors (of his hats). Conduct an *experiment*: give any hat $\alpha \in C$ to sage A and remove him (in our mind) from tree T. The tree falls into connected components, for which the inductive step holds. It is evident that each component contains one sage

from $N(A)$. Let $B \in N(A)$ be one of these sages and T_B be his connectivity component. Since we have already defined the color of A's hat, strategy f determines the strategy of sage B for game on T_B, the other sages from T_B can use strategy f too. By proposition I this strategy can be disproved, when one gives to sage B a hat of some set containing $t(s) - s$ colors.

The above experiment can be conducted in $s + 1$ ways. The obtained games on T_B differ by the strategy of sage B and for each of these games we have a "disproving" set consisting of $t(s) - s$ colors of sage B. It remains to note that the intersection of these $s + 1$ sets contains at least $t(s) - (s + 1)s = 1$ elements, i. e. it is non empty. Assign the color from this intersection to sage B. Similarly, we will treat with the other connectivity components. As a result we have built a hats placement on set $N(A)$, for which proposition II holds.

b) This solution is reported to us by S. Berlov. We prove that for $n = (s^2 + s)!$ the sages win. Let A be the central sage. Consider an $(s+1) \times s$ table. Invite $(s^2 + s)!$ sages to play in our game and put into correspondence each arrangement of numbers from 0 to $s^2 + s - 1$ in this table to a separate sage. The strategy of the sages is the following. Each "peripheral" sage finds in his table the row containing number c_A, and names all the numbers of this row. Further on, sage A for each number i from 1 to $(s^2 + s)!$ checks whether somebody of the sages wins if $c_A = i$ (it can be easily checked, because A sees the colors of all hats and knows the sages' tables). Let i_1, i_2, ..., i_k be the list of "bad" values of c_A, for which none of "peripheral" sages wins. If $k \leqslant s$, then A just names these values, and the sages have won. Suppose that $k \geqslant s + 1$. Since all possible tables are occurred among the tables of sages, there exists sage B, for which the numbers i_1, i_2,..., i_{s+1} are placed in different rows of his table. But then one of the rows contains the number c_B, and if this row contains number i_ℓ, then sage B wins when $c_A = i_\ell$. Therefore color i_ℓ is not bad. A contradiction.

c) Similarly to p. b). By a "scrap-heap" we mean three heaps of stones containing h stones in total (the stones are numbered from 0 to $h - 1$, and the heaps are numbered by 0, 1, 2, i. e. by possible hat colors of peripheral sages, empty heaps are allowed). Let n be the number of all possible scrap-heaps. Define the strategy of the sages on graph $K_{1,n}$. Give a unique scrap-heap to each sage B_i. The strategy of B_i is to name the number of heap containing the stone c_A. The strategy of sage A is to enroll those colors of his own hat, for which none of B_i has guessed correctly, and to name all listed colors. This is possible because the list contains at most two colors. Indeed, if the list contains colors c_1, c_2, c_3, then consider any scrap-heap, in which stones c_1, c_2, c_3 lie in the first, second and third heap respectively. Without loss of generality one can assume that the owner of the scrap-heap has received a hat of the first color. But then he certainly guesses correctly his own color, if sage A has received hat of color c_1 that contradicts the definition of c_1.

3.1. It is evident: on graph $\widetilde{G}$ sage A at first has to name $g(A_1)$ colors by the strategy of vertex A_1 in graph G (taking into account the colors of the neighbours of A_1 only), and then $g(A_2)$ colors by the strategy of vertex A_2 (looking only at the neighbours of A_2). The sages, who see on graph G only one of A_i, play as if A is this A_i. As for those sages, who saw in graph G both sages A_1 and A_2 and now see only one sage A, they must play assuming that the hats of A_1 and A_2 have the same color.

3.2. The hatness of sage v is equal to $h_1(v)h_2(v)$. So one can assume that the hat of sage v has "composite color", i. e. its color is an ordered pair (c_1, c_2), where c_i is the color of v's hat in game $\mathcal{G}_i$. Fix winning strategies for games $\mathcal{G}_1$ and $\mathcal{G}_2$ and build strategy for game $\mathcal{G}_1 \times_v \mathcal{G}_2$. Let all the sages from graph $G_i \setminus \{v\}$ play by the winning strategy for game $\mathcal{G}_i$ (the neighbours of v from graph G_i look only at component c_i of the color of sage v). As for sage v, he plays by both strategies at once: looking only at his neighbours in graph G_1, sage v finds $g_1(v)$ first components of his color by the winning strategy for game $\mathcal{G}_1$, and by the winning strategy for game $\mathcal{G}_2$ he finds $g_2(v)$ second components. Taking all possible pairs of the founded colors, he makes $g_1(v)g_2(v) = g(v)$ guesses.

The constructed strategy is winning, because either somebody in $G_1 \setminus \{v\}$ or in $G_2 \setminus \{v\}$ guesses correctly, or v guesses correctly both components of his color.

3.3. Assuming the contrary let f be a winning strategy in game $\mathcal{G}$. Denote by N_1 the set of neighbours of vertex A in graph G_1. For any hats placement φ on the vertices of graph G_1 the answers of all

the sages from set $V(G_1) \setminus A$ are determined by strategy f. We will show that there exist $s+1$ hats placements φ_i $(i = 1, \ldots, s+1)$ on graph G_1, such that for $i \neq j$

$$\varphi_i\big|_{N_1} = \varphi_j\big|_{N_1}, \qquad \varphi_i(A) \neq \varphi_j(A),$$

and such that if the sages from G_1 play according strategy f, then for all these placements none of the sages from $V(G_1) \setminus A$ guesses correctly.

For each hats placement α on vertices of N_1 denote by $C(\alpha)$ the set of hat colors of sage A, such that for all placements β on G_1, for which

$$\beta\big|_{N_1} = \alpha, \qquad \beta(A) \in C(\alpha),$$

none of the sages from set $V(G_1) \setminus A$ guesses correctly by strategy f. Suppose that the statement from the previous paragraph does not hold. Then each set $C(\alpha)$ contains at most s colors. Consider then the following strategy for game $\mathcal{G}_1$: let all the sages from G_1, except A, play by strategy f, and sage A name the colors from set $C(\alpha)$ (supplementing them by arbitrary colors, if $C(\alpha)$ contains less than s elements). This strategy is winning, because if nobody in $V(G_1) \setminus A$ has guessed correctly, then a hat from $C(\alpha)$ is on the head of A, and he guesses correctly. Contradiction.

Consider these $s+1$ placements φ_i. Fix a hats placement $\alpha = \varphi_i\big|_{N_1}$ on N_1 and restrict ourselves to only those hats placements on G_2, where sage A receives a hat of one of $s+1$ colors $\varphi_i(A)$, $i = 1, \ldots, s+1$. Then strategy f defines the actions of the sages on graph G_2, i. e. in losing game $\mathcal{G}_2$ subject with the only restriction that in the case $h_1(A) > s+1$ sage A by this strategy can name more than $s+1$ colors, i. e. more than his hatness in game G_2. But in this case mention of "outsider" colors does help to win. Therefore there exists disproving placement ψ on G_2. If $\psi(A) = \varphi_j(A)$, then $\psi \cup \varphi_j\big|_{V(G_1)\setminus A}$ is a disproving hats placement for strategy f in game $\mathcal{G}$.

3.4. It is evident. At first, sage A on graph $\widetilde{G}$ has to name the $g(A)$ colors, which he names by the strategy for graph G, when B's hat is painted in the first color. After that sage A names the $g(A)$ colors, which he names when B's hat is painted in the second color and so on.

3.5. For each natural N denote the set $\{0, 1, \ldots, N-1\}$ by $[N]$ for short.

For each vertex u of substituted graph G_1 define its color in game $\langle G, h, g\rangle$ as a pair from set $[h_1(u)] \times [h_2(A)]$. Let sage u look for the first component of his color by the strategy of game $\mathcal{G}_1$, and the second component by the strategy of A in game $\mathcal{G}_2$. The neighbours of vertex A from graph G_2 in new graph G see the whole subgraph G_1, and therefore can determine, who has guessed correctly the first component. Let B be the first of these sages (in lexicographical order). Then the vertices of graph $G_2 \setminus \{A\}$ can play by the strategy of game $\mathcal{G}_2$, using the second component of color B as a color of A. Since $\mathcal{G}_2$ is a winning game, some of the vertices win. If it is vertex from $G_2 \setminus \{A\}$, then it guesses correctly its color in graph G too. And if the winner of $\mathcal{G}_2$ was vertex A, then B correctly found both components of its color.

3.6. For proof we modify the strategy from the previous solution. In view of this construction vertex v after substitution gets a composite color from set $[h(v)] \times [h'(A)]$, and the strategy of sage v consists in calculating both components of his color, i. e. he chooses $s = g(v)$ colors $c_1, \ldots, c_s \in [h(v)]$, calculates G'-component of his color, i. e. chooses $g'(A)$ colors $e_1, \ldots, e_{g'(A)} \in [h'(A)]$, and after that he names all the pairs of colors (c_i, e_j).

We will change the construction of substitution and describe how the sages play in changed situation. The change affects only the sages $v \in G$, we assign for these sages new hatness and number of guesses: $h^*(v) = h(v)$ and $g^*(v) = g'(A)$. Therefore now v's hat has a color from set $[h(v)]$ (instead of a composite color), that is interpreted by his neighbours from $N_G(v)$ and $N_{G'}(A)$ as G-component of his color as before.

The strategy of each sage $v \in G$ consists of two phases. The first phase: casting glances at the neighbours in G, sage v calculates "G-component" of his color, i. e. a set consisting of s colors $c_1, \ldots, c_s \in [h(v)]$. Further, sage v identifies the obtained set and $[h'(A)]$ (by the rule $c_i \mapsto i$; remind that

$h'(A) = s$). After that the second phase begins: he looks at his neighbours in graph G' and apply the strategy of sage A naming $g'(A)$ colors from his newfound set $[h'(A)]$.

It remains to describe strategy of the sages from $N_{G'}(A)$. They all see the whole graph G, so they know, what set of colors each sage v has identified with set $[h'(A)]$. Besides that, they all know, who from $V(G)$ has guessed correctly G-component of his color. Let w be the first of these sages in lexicographical order. Since sage w has guessed correctly G-component of his color, the color of his hat belongs to the set $[h'(A)]$, that he has constructed in the first phase. Then during the second phase the sages of graph $G' \setminus \{A\}$ simply play the winning strategy of game $\mathcal{G}'$, substituting w with its constructed set $[h'(A)]$ in the place of A, and sage w actually plays by this strategy too, as explained above. As a result, somebody of them will guess correctly.

3.7. Each neighbour of A in $V(G) \setminus \{A\}$ now sees the whole set B, computes a "virtual color of sage A"

$$c_A = \sum_{v \in B} c_v \pmod{h(A)}$$

and plays by the strategy from game $\mathcal{G}$. As for the sages from B, they take for themselves one answer a_i each from the strategy of sage A, and sage v_i names color

$$a_i - \sum_{v \in B, v \neq v_i} c_v \pmod{h(A)}$$

(therefore, i-th sage verifies hypothesis $c_A = a_i$).

4.1. Let B be the vertex of hatness 2. Apply for vertex B the statement of constructor "removing half-edge" (problem 3.4) making this vertex invisible for the other vertices. Then the other sages do not see B, have two attempts, and lose by the statement of problem 2.6 b). Giving them a disproving hats placement, the referee will make so that sage B will not guess correctly too.

4.2. Fix number s. Consider the case, when the upper vertex has hatness $s+1$, and the other vertices have hatness h. Acting as in the previous problem, we make the upper vertex invisible for the others, as a result, the number of guesses of the vertices on path P_{n-1} becomes equal to $s(s+1) = f(s)$. By the statement of problem 2.6 b) the sages lose for $h > f(f(s))$. Thus $t_s \leqslant f(f(s))$.

4.3. We will prove by induction on the number of petals that for $h > f(f(f(s)))$ the game is losing. The base case, one petal G, follows from the previous problem: game $\langle G, \star h, \star s\rangle$ is already losing for $h > f(f(s))$.

But we need one more relative statement – a "modified base of the induction": game $\langle G, \star\bar{h}, \star s\rangle$ is losing for $h > f(f(f(s)))$, where $\star\bar{h}$ denotes the hatness function that is equal to h in all the vertices of petal G, except one vertex B for which $\bar{h}(B) = s+1$.

Proof of the statement. If B is the upper vertex of petal G, then this is again the statement of the base. Let B be an arbitrary vertex of petal on path P_{n-1} (fig. 7, left). Using constructor "removal of half-edge" (problem 3.4), make vertex B invisible for the other vertices. As a result the number of guesses of its neighbours becomes equal to $f(s)$. Now vertex B can be deleted from G, because nobody sees it, it has hatness $s+1$ and s guesses, so it is fated to fail in guessing. It can be easily seen that the remained graph is a union of two petals with common upper vertex (or one petal, but this case is trivial) and its vertices have s or $f(s)$ guesses (fig. 7, center). Add to graph horizontal edge between former neighbours of B (fig. 7, right), this edge can help to the sages to win. As a result, we have obtained a petal, which vertices have hatnesses at least $f(f(f(s)))$ and at most $f(s)$ guesses. By the statement of the base the sages nevertheless lose.

Now prove the inductive step. Consider petunia $M_n = M_{n-1} +_{v_n} L_n$. In view of modified statement of the base game $\langle L_n, \star\bar{h}, \star s\rangle$ is losing for $h > f(f(f(s)))$, where we denote by $\star\bar{h}$ the hatness function that is equal to h in all the vertices of petal G, except v_n, and hatness of v_n is equal to $s+1$. Game $\langle M_{n-1}, \star h, \star s\rangle$ is losing by the induction hypothesis. It remains to note that game $\langle M_n, \star h, \star s\rangle$ can be obtained by constructor of problem 3.3 from losing games $\langle M_{n-1}, \star h, \star s\rangle$ and $\langle L_n, \star\bar{h}, \star s\rangle$ and therefore is losing too.

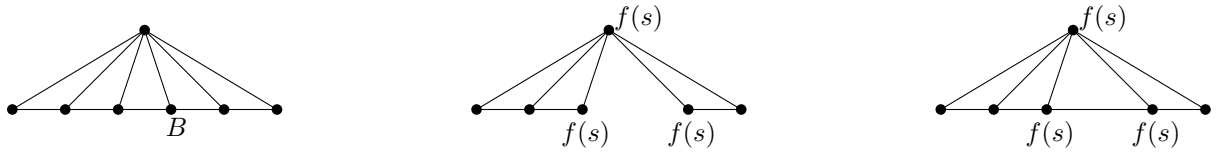


Figure 7. Removing of vertex B from petal G

4.4. a) Estimation $\mathrm{HG}_s(G) < 4s(s+1)-1$. Let A be the stem of the petal, $h(A) = s+1$, and the other vertices v have hatness $h(v) = 4s(s+1)-1$. It is sufficient to verify that game $\langle G, h, \star s\rangle$ is losing. By the statement of problem 5.6, this game is equivalent to the game on path P_n, where all vertices have hatness equal to $4s(s+1)-1$ and $s(s+1)$ guesses. But this game is losing by problem 2.3.

Now we will prove that game $\langle G, \star 4s(s+1)-2, \star s\rangle$ is winning for sufficiently large n.

Let $\mathcal{G}_0 = \langle P_k, \star 4s(s+1)-2, \star s(s+1)\rangle$. For sufficiently large k this game is winning by problem 2.5.

Similarly to the problem 2.6 c), one can prove that for any natural h there exists such natural n, that game on graph $K_{1,n}$ is winning, if the hatnesses of all peripheral sages are equal to $s+1$ and they all have one attempt for guessing, and the hatness of the central sage is equal to h and he has s attempts. Set $h = 4s(s+1)-2$ and choose suitable n. Substitute with reducing game $\mathcal{G}_0$ in the place of each peripheral sage[1]. We obtain a winning game, where the hatnesses of all vertices are equal to $4s(s+1)-2$, the numbers of attempts are equal to s, and the graph is a subraph of a large petal.

b) As we have checked in p. a), game $\langle G, h, \star s\rangle$ is losing, where G is a petal with large number of vertices, and h is the function defining hatness of the stem by $s+1$, and the hatnesses of the other vertices by $4s(s+1)-1$. By the statement of problem 3.3 gluing of stem of such petal to a vertex of another losing game with s guesses gives again a losing game. But royal petunia by definition is constructed by consecutive stem's glueings of petals! Therefore a game on a royal petunia with large petals, where all the vertices have hatness $4s(s+1)-1$ and s guesses, except the first (rooted) stem with hatness $s+1$ and s guesses, is losing. It gives the estimation $\mathrm{HG}_s(G) < 4s(s+1)-1$.

Then $\mathrm{HG}_s(G) = 4s(s+1)-2$, since this hatness is realized already on petals that are royal petunias too though not very branchy.

5.1. *"If" case.* Fix one of h_0 colors of the central sage's hat. Then the strategies of the other vertices are determined, and in $\prod_{i=1}^{n}(h_i - g_i)$ cases none of pendant vertices guesses correctly. Therefore the central sage must guess. But the central sage can do this only in $g_0\prod_{i=1}^{n} h_i$ cases in total. We obtain an inequality that is equivalent to the inequality from the condition.

"Only if" case. We will show that for $N = \prod_{i=1}^{n} h_i$ game $\langle K_{1,n}, (N\cdot h_0; h_1, \ldots, h_n), (N\cdot g_0; g_1, \ldots, g_n)\rangle$ is winning.

Encode $h_0\cdot h_1\cdot \ldots \cdot h_n$ colors of the central sage by sets $(c_0; c_1, \ldots, c_n)$, where $0 \leqslant c_i < h_i$. Let i-th sage, when he sees color $(c_0; c_1, \ldots, c_n)$, name colors $c_i, c_i+1, \ldots c_i+g_i-1 \pmod{h_i}$. And let the central sage look at the others and name all variants, in which none of them guesses correctly. How many are there such variants? There are h_0 variants for zeroth component and $h_i - g_i$ variants for each of the others. But the inequality from the condition is equivalent to the inequality $h_0\prod_{i=1}^{n}(h_i - g_i) \leqslant N\cdot g_0$,

[1]We need here the following more general version of the constructor than that in problem 3.6.

Let $\mathcal{G} = \langle G, h, \star s g_0\rangle$, $\mathcal{G}' = \langle G', h', g'\rangle$ be winning games. Let A be a vertex of graph G', and $h'(A) = s$. Let $\langle \widetilde{G}, \widetilde{h}, \widetilde{g}\rangle$ be the winning game obtained by the substitution of game $\mathcal{G}$ on the place of vertex A to game $\mathcal{G}'$ (as in problem 3.5). By the rule of the substitution for all substituting vertices v

$$\widetilde{h}(v) = h(v)h'(A) = s\cdot h(v), \qquad \widetilde{g}(v) = g(v)g'(A) = sg_0\cdot g'(A).$$

Consider new functions h^*, g^* on graph $\widetilde{G}$, which differ from $\widetilde{h}$, $\widetilde{g}$ only by the values in substituting vertices v, and this difference is the cancellation by s:

$$h^*(v) = h(v), \qquad g^*(v) = g_0\cdot g'(A).$$

Then game $\langle \widetilde{G}, h^*, g^*\rangle$ is also winning.

thus the central sage has enough attempts.

5.2. Denote the sages by A, B and C: 

. We present a winning strategy for the sages. Let sage A name colors c_B, $c_B{+}1$, …, $c_B{+}(g{-}1)$ mod h, and sage C c_B, $c_B{+}[\frac{h}{g}]$, …, $c_B{+}[(g{-}1)\frac{h}{g}]$ mod h, where $[x]$ denotes the rounding to the nearest integer. Therefore, if B's hat is from the set

$$I_A = \big(c_A, c_A - 1, \ldots, c_A - (g-1)\big) \bmod h,$$

then sage A will guess correctly, and if B's hat is from the set

$$I_C = \Big(c_C, c_C - \Big[\frac{h}{g}\Big], \ldots, c_C - \Big[(g-1)\cdot\frac{h}{g}\Big]\Big) \bmod h,$$

then sage C will guess correctly. It remains to prove that for sage B there are at most g colors not covered by set $I_A \cup I_C$ or, equivalently, that

$$h - |I_A| - |I_C| + |I_A \cap I_C| \leqslant g.$$

Since $|I_A| = |I_C| = g$, it is equivalent to the inequality $|I_A \cap I_C| \leqslant 3g - h$.

Suppose that this statement is wrong and $|I_A \cap I_C| > 3g - h$. Then there exists k such that both numbers $c_C - [k\cdot\frac{h}{g}]$ and $c_C - [(k+3g-h)\cdot\frac{h}{g}]$ belong to $I_A \cap I_C$ (the elements of $I_A \cap I_C$ can be written in two forms: $c_A - i = c_C - \big[\ell\cdot\frac{h}{g}\big]$; the number ℓ that corresponds to the minimal possible i, can be taken as k). Since both numbers belong to set I_A, consisting of consecutive remainders, the distance between them does not exceed $g-1$:

$$\Big(c_C - \Big[k\cdot\frac{h}{g}\Big]\Big) - \Big(c_C - \Big[(k+3g-h)\cdot\frac{h}{g}\Big]\Big) \leqslant g-1,$$

that is equivalent

$$\Big[(k+3g-h)\cdot\frac{h}{g}\Big] - \Big[k\cdot\frac{h}{g}\Big] \leqslant g-1.$$

Getting rid of rounding, we obtain the corollary:

$$(k+3g-h)\cdot\frac{h}{g} - 0.5 - k\cdot\frac{h}{g} - 0.5 \leqslant g-1.$$

The last is equivalent to the inequality $(3g-h)\cdot\frac{h}{g} \leqslant g$, i. e. $0 \leqslant g^2 - 3gh + h^2$, that contradicts the condition.

5.3. By the statement of problem 5.1 the existence of k, for which game $\langle P_3, \star kh, \star kg\rangle = \langle K_{1,2}, \star kh, \star kg\rangle$ is winning, is equivalent to the condition

$$\Big(1 - \frac{g}{h}\Big)\Big(1 - \frac{g}{h}\Big) \leqslant \frac{g}{h}.$$

For non-negative h it is equivalent to the inequality $g^2 - 3gh + h^2 \leqslant 0$, that for $1 \leqslant g \leqslant h$ is equivalent to the inequality

$$\frac{h}{g} \leqslant \frac{3+\sqrt{5}}{2}.$$

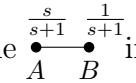
Now the problem statement is evident.

5.4. Consider an arbitrary strategy of the sages in game $\langle G, h\rangle$. The product $\prod\limits_{v\in H_2} h_2(v)$ enumerates hats placements on H_2. When we choose each of these hats placements, we fix strategy of the sages on G_1. For the fixed hats placement on H_2 consider hats placements on G_1. The sum $\sum\limits_{u\in G_1} \frac{1}{h_1(u)}$ estimates from above the fraction of those placements on G_1, where at least one sage from G_1 guesses

correctly. Then the product $\left(\sum\limits_{u\in G_1}\frac{1}{h_1(u)}\right)\prod\limits_{v\in H_2}h_2(v)$ estimates from above the maximum fraction of those placements on G_1, where at least one sage from G_1 guesses correctly provided that each sage makes $\prod\limits_{v\in H_2}h_2(v)$ guesses. Therefore the inequality from the problem condition means that there exists hats placement α on G_1, for which none of sages from G_1 guesses correctly, whatever hats were given to the sages from H_2. Therefore after assigning hats placement α to sages from G_1, none of them guesses correctly and the strategies of the other sages on graph G_2 are completely determined and now are suitable for game $\langle G_2, h_2\rangle$. Since this game is losing, hats placement α can be enlarged to hats placement on G_2, for which nobody from G_2 guesses correctly too.

5.5. Let the sages have fixed a strategy on graph G'. We will construct a disproving hats placement for this strategy. The strategy of sage A for each of $2h(B)-1$ possible colors of hat of B prescribes to name one of two colors. Some of these two colors is named at most $h(B)-1$ times. Give to sage A the hat of this color, this will fix the strategy of sage B on the remained graph G. Now, to prevent correct guessing of A, we give to B a hat of one of at least $h(B)$ remained colors. Since game $\mathcal{G}$ is losing, we can construct hats placement on graph G so that nobody on G will guess correctly.

5.6. If $\mathcal{G}$ is a winning game, we remove by problem 3.4 all half-edges $\overrightarrow{vA}$ and obtain the winning game. In this game A has s guesses, $s+1$ colors and no information, therefore we can assign A's color such that A does not guess. But now the remaining sages play the game $\mathcal{G}'$. Hence $\mathcal{G}'$ is winning.

If the game $\mathcal{G}'$ is winning, substitute $\mathcal{G}'$ in the winning game 

in place of vertex B by problem 3.6. We obtain a winning game $\mathcal{G}$.

5.7. a) Let $\mathcal{G}$ be a losing game on path ABC where $h(A)=h(C)=2$, $h(B)=5$. If both games were losing, then the initial game would be obtained from these games and game $\mathcal{G}$ by constructor of problem 3.3 (where $s=1$, $g_1=g_2=\star 1$) and were losing too.

b) Set $V(\widetilde{G})$ consists of the vertices of graph G and the set of new vertices V_1 (that are situated in the middles of two-link paths). Define a function on $V(\widetilde{G})$:

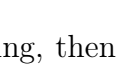
$$h(v)=\begin{cases}2, & v\in V(G),\\ 5, & v\in V_1.\end{cases}$$

It is sufficient to verify that game $\langle\widetilde{G},h\rangle$ is losing. It is evident. Indeed, each sage from V_1 has two neighbours in $\widetilde{G}$ with hatness 2, so he names by his strategy at most four colors. Then we give him a hat of the color, that he does not name, and he will not guess correctly. Now all the answers of the sages from $V(G)$ are determined, and we give to each sage a hat of the color that he does not name, too.

5.8. Let after deletion of the bridge graph G fall into components G_1 (containing vertex B) and G_2 (containing vertex A). Define hatness functions h_1 and h_2 on these graphs by the rule

$$h_1(x)=\begin{cases}h(x), & x\in V(G_1)\setminus\{B\},\\ \lceil\frac{h(B)}{2}\rceil, & x=B.\end{cases}\qquad h_2(x)=\begin{cases}h(x), & x\in V(G_2)\setminus\{A\},\\ \lceil\frac{h(A)}{2}\rceil, & x=A.\end{cases}$$

Let $\mathcal{G}_1'=\langle G_1, h\big|_{G_1}\rangle$, it is a losing game due to properties of function h.

If games $\mathcal{G}_1=\langle G_1,h_1\rangle$ and $\mathcal{G}_2=\langle G_2,h_2\rangle$ are both winning, then game $\mathcal{G}_1\times_B$ 

$\times_A\mathcal{G}_2$ is also winning. If the values $h(A)$ and $h(B)$ are even, we obtain the desired decomposition in the product of games. But if at least one of the numbers $h(A)$, $h(B)$ is odd, then the hatness function of the obtained game majorizes h and by properties of function h such game cannot be winning, a contradiction.

It remains to consider the case, when at least one of games game $\mathcal{G}_1=\langle G_1,h_1\rangle$ or $\mathcal{G}_2=\langle G_2,h_2\rangle$ is losing, let it be game $\mathcal{G}_2$. Let us apply constructor of problem 5.5 to loosing game $\mathcal{G}_2$: take a new

vertex B of hatness 2 connected with A, let the hatness of vertex A become equal to

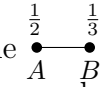
$$2\left\lceil\frac{h(A)}{2}\right\rceil - 1 \leqslant h(A)$$

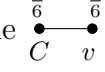
and the hatnesses of other vertices be defined by function h. Denote the obtained game by $\mathcal{G}_2'$. Apply now constructor of problem 3.3 to games $\mathcal{G}_1'$ and $\mathcal{G}_2'$ (we assume that $s = 1$, $g_1 = g_2 = \star 1$). We will obtain a losing game on graph G, in which hatness function does not exceed h. It is impossible.

5.9. Denote the initial game by $\mathcal{G}_1 = (G_1, h_1, g_1)$, where $g_1 \equiv 1$. Denote by G_2 the subgraph of graph G_1 obtained from G_1 by removing vertex A, denote by G_3 the subgraph of G_2 obtained from G_2 by removing vertex B, and denote by G_4 the graph obtained from G_3 by adding vertex C, which is connected to all other vertices, i. e. in fact G_4 is obtained from G_2 by renaming vertex B to C. Consider games $\mathcal{G}_2 = (G_2, h_2, g_2)$, $\mathcal{G}_3 = (G_3, h_3, g_3)$, $\mathcal{G}_4 = (G_4, h_4, g_4)$, where

$$h_2(v) = \begin{cases} h_1(v) & v \in G_3, \\ 3 & v = B \end{cases}, \qquad h_3(v) = h_1\big|_{G_3}, \qquad h_4(v) = \begin{cases} h_1(v) & v \in G_3, \\ 6 & v = C \end{cases},$$

$$g_2 \equiv 2 \qquad g_3 \equiv 6 \qquad g_4(v) = \begin{cases} 1 & v \in G_3, \\ 5 & v = C \end{cases}.$$

Suppose that game $\mathcal{G}_1$ is winning. When we remove by problem 3.4 all the half-edges leading from vertices A and B, we obtain a winning game, in which the number of guesses of all other sages (i. e. the sages from G_3) become equal to 6, and the strategies do not depend of colors of A's and B's hats. Assume that there exists a hats placement on G_3, for which nobody from G_3 guesses correctly. This hats placement determines the strategies of sages A and B, playing on edge AB in game 

, and as a result all the sages lose. That is impossible. Therefore the restriction of the game to graph G_3, i.e. game $\mathcal{G}_3$, is winning. Making by problem 3.6 substitution of this game with reducing in game 

in the place of vertex v, we obtain winning game $\mathcal{G}_4$.

Conversely, let game $\mathcal{G}_4$ be winning. We wish to replace player C by two players A (with hatness 2) and B (with hatness 3). Let us demonstrate the winning strategy of the players in the obtained game. All players from G_3 will use the strategy of game $\mathcal{G}_4$, interpreting pair (color A, color B) as composite color of player C. Show how one can "convert" the strategy of player C to a pair of strategies of A and B.

The color of player C is an element of the set $\mathcal{C} = \{0,1\} \times \{0,1,2\}$. Let for the current hats placement of his neighbours C must name all the colors from set $\mathcal{C}$, except $(1,2)$. Then the actions of players A and B consist in that A names the color with the same parity as B's color and B names color 0 or 1 of opposite parity to A's color. Player C has guessed correctly, if one of colors $(0,0)$, $(0,2)$, $(1,1)$ or $(0,1)$, $(1,0)$ was on his head. By our rule in the first three cases A guesses correctly, in the other two B guesses correctly.

The roles of A and B are assigned similarly for the other sets of five guesses of C.

5.10. Show that game $\big\langle G, \star\mathrm{HG}_{s'}(G[A]) + 1, \star s\big\rangle$, where $s' = s(\mathrm{HG}_s(G[B]) + 1)^d$, is losing. For this we construct hats placement such that the sages will lose. Since $\mathrm{HG}_{s'}(G[A]) \geqslant s' \geqslant \mathrm{HG}_s(G[B]) + 1$, i. e. the hatness in the game under consideration is larger than $\mathrm{HG}_s(G[B]) + 1$, it is sufficient to consider the case, when the hatness of the sages from B is equal to $\mathrm{HG}_s(G[B]) + 1$. Applying problem 3.4, remove all half-edges from A in B, making set B invisible for set A. Since during this action we erase at most d half-edges for each sage from A, the number of sages' guesses will increase, but will not exceed s'. And the strategy of the sages from A now does not depend on the hats placement on B. Therefore we can assume that they play a game $\big\langle G[A], \star\mathrm{HG}_{s'}(G[A]) + 1, \star s'\big\rangle$ on graph $G[A]$. By the definition of s-hat number this game is losing. Thus, there exists a hats placement on A, such that nobody from A guesses correctly. Give to the sages from A this placement, then the strategy of the sages from B of game on $G[B]$ is determined. Since the hatnesses of the sages from B are greater than $\mathrm{HG}_s(G[B])$, we can assign colors on B so that the sages will lose.

Многочлены в теории чисел

Проект подготовили и представляют:
Павел Козлов, Илья Богданов, Павел Кожевников, Андрей Рябичев, Борис Френкин, Navid Safaei

Аннотация

В этом проекте мы собираемся познакомить участников с несколькими замечательными задачами и идеями, возникающими на стыке теории чисел и теории многочленов. Этот проект будет состоять из нескольких разделов, каждый из них будет по-своему интересен.

В разделе 0 собраны вспомогательные факты, которые будет полезно знать для решения задач.

Во разделе 1 речь пойдет о делителях (и простых делителей) значений различных многочленов с целыми коэффициентами. Здесь удается поработать с некоторыми конкретными многочленами, а также установить некоторые общие, причем весьма красивые и удивительные, результаты. Например, оказывается, для любого непостоянного многочлена с целыми коэффициентами существует бесконечно много простых чисел вида $4k+1$, на которые делятся его значения в целых точках. А если потребовать от многочлена дополнительно наличие вещественного корня, то это же можно сказать о простых числах вида $4k+3$.

Раздел 2 посвящён в основном одной сложной теоретико-числовой задаче, в которой описываются все ситуации, когда произведения n последовательных чисел, увеличенные на константу, являются точными степенями. По ходу решения этой задачи участники ознакомятся с аналитическими и числовыми методами, полезными и для решения других задач.

В разделе 3 собраны разные задачи, представляющие самостоятельный интерес и в некотором смысле родственные другим задачам проекта.

0 Вспомогательные факты

0.1 Основы теории чисел

Перечислим некоторые теоретико-числовые сведения, которые могут потребоваться при решении задач.

- Деление с остатком и алгоритм Евклида.
- Линейное представление НОД.
- Основная теорема арифметики (о существовании и единственности разложения натурального числа на простые сомножители).

Следствие основной теоремы арифметики — наличие для любого натурального числа $n > 1$ *канонического разложения* $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, где $p_1, \dots, p_k$ — различные простые числа, $\alpha_1, \dots, \alpha_k$ — степени их вхождения в разложение.

Степень вхождения простого числа p в разложение целого n ниже будем обозначать $v_p(n)$.

• Китайская теорема об остатках.

Одна из ее переформулировок такова: Пусть даны n бесконечных в обе стороны арифметических прогрессий, состоящих из целых чисел, причем разности прогрессий $d_1, \ldots, d_n$ попарно взаимно просты. Тогда пересечение этих прогрессий — прогрессия с разностью $d_1 \ldots d_n$.

• Сравнения по модулю и вычеты.

Запись $a \equiv b \pmod{n}$ (a и b сравнимы по модулю n) для целых a, b и натурального n означает, что a и b имеют равные остатки при делении на n, или что $n \mid (a - b)$.

Вычетом по модулю n называют класс эквивалентности относительно отношения равенства по модулю n (каждый такой класс представляет собой арифметическую прогрессию с разностью n); впрочем, вычетом иногда называют и любого представителя класса. Все n вычетов образуют *полную систему вычетов*, которую обозначаем $\mathbb{Z}_n$. Можно считать, что $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, если для каждого вычета выбрать соответствующего представителя. На множестве вычетов естественно вводятся операции сложения и умножения. Обратным к вычету a называется вычет a^{-1} такой, что aa^{-1} равно 1 в $\mathbb{Z}_n$, т.е. $aa^{-1} \equiv 1 \pmod{n}$. Вычет a обратим (т.е. имеет обратный) тогда и только тогда, когда $\text{НОД}(a, n) = 1$.

• Теоремы Эйлера и Ферма.

Теорема Эйлера гласит, что для взаимно простых $a \in \mathbb{Z}$ и $n \in \mathbb{N}$ выполнено $a^{\varphi(n)} \equiv 1 \pmod{n}$, где $\varphi(n)$ — функция Эйлера числа n, т.е. количество чисел из множества $\{1, \ldots, n\}$, взаимно простых с n.

Теорема Ферма — частный случай теоремы Эйлера для простого $n = p$.

• *Показателем* целого числа a по модулю натурального n называется наименьшее натуральное k такое, что $a^k \equiv 1 \pmod{n}$. (Ясно, что показатель определен только в случае $\text{НОД}(a, n) = 1$.) Показатель обозначаем $ord_n(a)$.

Отметим следующее свойство показателя: $a^m \equiv 1 \pmod{n}$ тогда и только тогда, когда $ord_n(a) \mid m$. В силу теоремы Эйлера отсюда, в частности, следует, что $ord_n(a) \mid \varphi(n)$.

Если $ord_n(a) = \varphi(n)$, то степени $1, a, a^2, \ldots, a^{\varphi(n)-1}$ пробегают все вычеты, взаимно-простые с n. В таком случае a называют *первообразным корнем* по модулю n. Первообразный корень существует тогда и только тогда, когда n равно 2, 4, p^α или $2p^\alpha$ для простого p и натурального α.

• Напомним *LTE-лемму* (Lifting the Exponent Lemma).

Пусть p — нечётное простое число, a, b — различные целые. Тогда если $p \mid a - b$, то

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n),$$

Если же $p = 2$, то это верно при условии $4 \mid a - b$.

• Ненулевой вычет a по простому нечетному модулю p называется *квадратичным*, если сравнение $x^2 \equiv a \pmod{p}$ имеет непустое множество решений. Количество (ненулевых) квадратичных вычетов $\frac{p-1}{2}$ — столько же, сколько невычетов.

Справедлив критерий Эйлера: ненулевой вычет a является квадратичным тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

0.2 Теория делимости в $\mathbb{Q}[x]$

Множество многочленов с рациональными коэффициентами обозначим $\mathbb{Q}[x]$, а множество многочленов с целыми коэффициентами — $\mathbb{Z}[x]$. Многочлены степени не меньше 1 назовём *непостоянными*, так что постоянные многочлены — это многочлены, тождественно равные некоторому числу. Непостоянный многочлен $f \in \mathbb{Q}[x]$ степени d называется *приводимым* над $\mathbb{Q}$ (или приводимым в $\mathbb{Q}[x]$), если он может быть представлен в виде произведения двух многочленов степени меньшей чем d с рациональными же коэффициентами. Каждый непостоянный многочлен из $\mathbb{Q}[x]$ является либо приводимым, либо *неприводимым* над $\mathbb{Q}$. Так же, как и целые числа, многочлены из $\mathbb{Q}[x]$ можно делить с остатком (например, "уголком"). В $\mathbb{Q}[x]$ определяется НОД многочленов $f_1, f_2, \ldots, f_k$ как многочлен наибольшей степени, на который делится каждый из многочленов $f_1, f_2, \ldots, f_k$. НОД многочленов единственен с точностью до умножения на ненулевое число, НОД двух многочленов можно находить с помощью алгоритма Евклида. Многочлены, НОД которых равен 1, называются *взаимно простыми*. Аналогами теорем о линейном представлении НОД и основной теоремы арифметики для целых чисел являются следующие теоремы:

Факт 0.1 (Теорема о линейном представлении НОД). Для любых многочленов $f_1, f_2, \ldots, f_k \in \mathbb{Q}[x]$ найдутся такие многочлены $u_1, u_2, \ldots, u_k \in \mathbb{Q}[x]$, что

$$\text{НОД}(f_1, f_2, \ldots, f_k) = u_1 f_1 + u_2 f_2 + \ldots u_k f_k.$$

Факт 0.2 (Основная теорема арифметики). Непостоянный многочлен $f \in \mathbb{Q}[x]$ представим в виде $f = h_1 \cdot h_2 \cdot \ldots \cdot h_r$, где h_i — неприводимые над $\mathbb{Q}$ многочлены, причем если $f = h'_1 \cdot h'_2 \cdot \ldots \cdot h'_s$ — другое такое разложение, то $s = r$ и для некоторой перенумерации $h'_1, h'_2 \ldots h'_r$ будет выполнено

$$h'_1 = u_1 h_1, \quad h'_2 = u_2 h_2, \quad \ldots, \quad h'_r = u_r h_r,$$

где $u_1, u_2 \ldots u_r$ — ненулевые рациональные числа.

Группируя в разложении на неприводимые многочлены одинаковые сомножители, можно получить *каноническое разложение*, подобно каноническому разложению натурального числа на простые сомножители.

0.3 Лемма Гаусса

Назовем *содержанием* многочлена с целыми коэффициентами НОД всех его коэффициентов. Далее содержание многочлена f обозначим $d(f)$. Если $d(f) = 1$, то многочлен f называют *примитивным*.

Факт 0.3. Пусть $f, g \in \mathbb{Z}[x]$. Тогда $d(fg) = d(f) \cdot d(g)$. В частности, произведение двух примитивных многочленов снова будет примитивным многочленом.

Доказательство. Начнем с последнего утверждения. Пусть $f(x) = a_0 + a_1 x + \ldots a_n x^n$ и $g(x) = b_0 + b_1 x + \ldots b_m x^m$ — примитивные многочлены из $\mathbb{Z}[x]$, произведение которых не является примитивным, то есть для некоторого простого числа p верна делимость $p \mid d(fg)$.

Выберем наименьшие индексы s, t, для которых $p \nmid a_s, p \nmid b_t$. Такие индексы найдутся в силу примитивности f и g. Коэффициент при x^{s+t} в многочлене fg будет равен

$$c_{s+t} = a_s b_t + (a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \ldots) + (a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \ldots).$$

Так как a_{s-i} и b_{t-i} при $i > 0$ делятся на p по условию и $p \mid c_{s+t}$ по предположению, то $p \mid a_s b_t$, а это противоречит выбору индексов s и t.

Переходя к общему случаю, запишем произвольные многочлены $f, g \in \mathbb{Z}[x]$ в виде

$$f = d(f) f_0, \qquad g = d(g) g_0,$$

где f_0, g_0 — примитивные многочлены. Так как $fg = d(f)d(g) \cdot f_0 \cdot g_0$ и по доказанному $d(f_0 \cdot g_0) = 1$, то $d(fg) = d(f)d(g)$, что и требовалось доказать.

Факт 0.4 (Лемма Гаусса). Многочлен из $\mathbb{Z}$, неприводимый над $\mathbb{Z}$, также неприводим над $\mathbb{Q}$.

Доказательство. Предположим, что для некоторых многочленов $h \in \mathbb{Z}[x]$ и $f, g \in \mathbb{Q}[x]$ выполняется равенство $h = fg$. После умножения обеих частей этого равенства на НОК знаменателей и вынесения НОК числителей всех коэффициентов у f и g, оно переписывается в виде:

$$ah = bf_0 g_0,$$

где $a, b \in \mathbb{Z}$, а f_0 и g_0 — примитивные многочлены над $\mathbb{Z}$. По предыдущему пункту, $a \cdot d(h) = b$, так что после сокращения получается разложение

$$h = d(h) f_0 g_0,$$

поэтому многочлен h приводим также и в $\mathbb{Z}[x]$.

С помощью леммы Гаусса и основной теоремы арифметики для $\mathbb{Q}[x]$ можно получить следующий

Факт 0.5 (Основная теорема арифметики в $\mathbb{Z}[x]$). Непостоянный многочлен $f \in \mathbb{Z}[x]$ представим в виде $f = h_1 \cdot h_2 \cdot \ldots \cdot h_r$, где $h_i \in \mathbb{Z}[x]$ — неприводимые над $\mathbb{Q}$ (непостоянные) многочлены.

Если в последнем разложении $f = h_1 h_2 \ldots h_r$ сгруппировать пропорциональные сомножители и вынести из каждого сомножителя НОД его коэффициентов, то мы придем к *каноническому* разложению многочлена с целыми коэффициентами

$$f = u \cdot g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_k^{\alpha_k},$$

где $g_i \in \mathbb{Z}[x]$ — попарно взаимно простые примитивные неприводимые над $\mathbb{Q}$ (непостоянные) многочлены, $u \in \mathbb{Z}$, $u \neq 0$, $k \geqslant 1$, $\alpha_i \geqslant 1$.

Каноническое разложение единственно с точностью до домножения сомножителей на ± 1.

0.4 Лемма Гензеля

В этой параграфе опишем очень важный результат, который не один раз пригодится в дальнейшем. Для начала заметим, что для любого постоянного многочлена f верно следующее тождество:

$$f(x+y) = f(x).$$

Дальше, для любого линейного многочлена f верно соотношение:

$$f(x+y) = f(x) + cy,$$

где константа c равна коэффициенту при x или, другими словами, первой производной многочлена f.

Вышенаписанное несложно обобщить на случай произвольного многочлена (например, с помощью индукции по степени многочлена). Верен следующий факт: если f — многочлен степени d с целыми коэффициентами, то справедливо равенство:

$$f(x+y) = f(x) + f_1(x)y + f_2(x)y^2 + \ldots + f_d(x)y^d,$$

где f_i, $i = 1, 2, \ldots, d$ — многочлены с целыми коэффициентами степени не выше $d-1$; f_i явно выражаются как $f_i = \frac{f^{(i)}}{i!}$.

Непосредственным следствием этого утверждения является следующая очень полезная лемма:

Факт 0.6 (Лемма Гензеля). Пусть $f \in \mathbb{Z}$ — многочлен с целыми коэффициентами. Тогда для любого простого q, натурального s и целых r, n верно следующее сравнение

$$f(n + rq^s) \equiv f(n) + rq^s f'(n) \pmod{q^{2s}}.$$

1 Делители значений многочлена и приложения

Введем следующие обозначения. Для многочлена $f \in \mathbb{Z}[x]$ через $D(f)$ обозначим множество натуральных чисел m, для которых $f(n)$ делится на m при некотором целом n. Иначе говоря, $m \in D(f)$ тогда и только тогда, когда сравнение $f(x) \equiv 0 \pmod{m}$ имеет целочисленное решение.

Более общо, для многочленов $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$ через $D(f_1, f_2, \ldots, f_k)$ обозначим множество натуральных чисел m таких, что система сравнений

$$f_i(x) \equiv 0 \pmod{m}, \;\; i = 1, 2, \ldots, k, \tag{1}$$

имеет целочисленное решение. Через $P(f_1, f_2, \ldots, f_k)$ будем обозначать множество всех простых чисел, принадлежащих $D(f_1, f_2, \ldots, f_k)$.

Ясно, что если $f(n)$ делится на m, то и $f(n+mt)$ делится на m для любого целого t. Таких образом, множество целых чисел x, удовлетворяющих системе (1), либо пустое, либо является объединением бесконечных в обе стороны арифметических прогрессий с разностью m.

Очевидно, вместе с каждым $m \in D(f)$ в множество $D(f)$ входят и все натуральные делители m. Для постоянного многочлена $f = u \in \mathbb{Z}$ множество $D(u)$ совпадает с множеством (натуральных) делителей числа u. Легко видеть, что для непостоянного многочлена $f \in \mathbb{Z}[x]$ множество $D(f)$ бесконечно.

Задача 1.1. а) Докажите, что для любых заданных натуральных $m_1, \ldots, m_n$ существует многочлен $f \in \mathbb{Z}[x]$, для которого $m_1, \ldots, m_n$ не принадлежат $D(f)$.

б) Докажите, что $D(fg) \supset D(f)$ для любых двух многочленов $f, g \in \mathbb{Z}[x]$.

в) Докажите, что $D(f(g)) \subset D(f)$ для любых двух многочленов $f, g \in \mathbb{Z}[x]$.

Задача 1.2. Для любого непостоянного многочлена $f \in \mathbb{Z}[x]$ множество $P(f)$ бесконечно.

Задача 1.3. Если $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$, $k \geqslant 2$ — взаимно простые в совокупности многочлены, то множество $D(f_1, f_2, \ldots, f_k)$ конечно. (И, следовательно, множество $P(f_1, f_2, \ldots, f_k)$ конечно.)

Задача 1.4. Пусть $f \in \mathbb{Z}[x]$. Докажите, что если $m_1, m_2 \in D(f)$, и НОД$(m_1, m_2) = 1$, то $m_1 m_2 \in D(f)$.

Задача 1.5. Найдите $P(f)$, если
а) $f(x) = x^2 + 1$;
б) $f(x) = x^2 + x + 1$;
в) $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$, где $p > 2$ — простое число.

Задача 1.6. а) Ясно, что если многочлен $f \in \mathbb{Z}[x]$ имеет целый корень, то $P(f)$ совпадает с множеством всех простых чисел. Докажите, что обратное утверждение неверно.

б) Пусть $P(f)$ совпадает с множеством всех простых чисел. Следует ли отсюда, что у f есть рациональный корень?

Для многочлена $f \in \mathbb{Z}[x]$ через $P_\alpha(f)$ обозначим множество простых чисел p таких, что $v_p(f(n)) = \alpha$ для некоторого целого n.

Ясно, что если $v_p(f(n)) = \alpha$, то и $v_p(f(n + p^{\alpha+1}k)) = \alpha$ при любом целом k. Таких образом, множество целых чисел x таких, что $v_p(f(x)) = \alpha$, либо пустое, либо является объединением бесконечных в обе стороны арифметических прогрессий с разностью $p^{\alpha+1}$.

Легко видеть, что $P_\alpha(f) \subset P(f)$, причем для $f \in \mathbb{Z}[x]$, не равного тождественно нулю, $P(f) = \bigcup\limits_{\alpha=1}^{\infty} P_\alpha(f)$. Отметим также, что для $f \in \mathbb{Z}[x]$ и $k \in \mathbb{N}$ выполнено $P_\alpha(f) = P_{k\alpha}(f^k)$.

Задача 1.7. Пусть $f \in \mathbb{Z}[x]$.

а) Если $p \in P(f) \setminus P(f, f')$, то $p \in P_\alpha(f)$ для сколь угодно больших α.

б) Докажите, что множества $P_\alpha(f) \setminus P(f, f')$ совпадают с $P(f) \setminus P(f, f')$ при $\alpha = 1, 2, 3, \ldots$.

Задача 1.8. Ясно, что если многочлен $f \in \mathbb{Z}[x]$ имеет целый корень, то $D(f) = \mathbb{N}$. Верно ли обратное утверждение?

Задача 1.9. Пусть $f \in \mathbb{Z}[x]$ таков, что при каждом натуральном n значение многочлена $f(n)$ является нетривиальной точной степенью некоторого натурального числа, т.е. $f(n) = m(n)^{s(n)}$, где $m(n)$ и $s(n) > 1$ — натуральные числа.

а) Докажите, что f приводим над $\mathbb{Q}$.

б) Докажите, что существуют натуральное $s > 1$ и многочлен $q \in \mathbb{Z}[x]$ такие, что $f = q^s$.

Задача 1.10. Докажите, что Для любого непостоянного многочлена $f \in \mathbb{Z}[x]$ множество $P(f)$ содержит бесконечно много простых чисел вида $4k + 1$.

2 Об одной задаче Сендерова

Задача 2.1. Многочлен $Q(x)$ с вещественными коэффициентами таков, что его старший коэффициент рациональный, и для некоторого натурального $k > 1$ выполняется $Q(x)^k \in \mathbb{Z}[x]$. Докажите, что $Q(x) \in \mathbb{Z}[x]$.

Задача 2.2. Про многочлен $P(x)$ чётной степени с целыми коэффициентами известно, что его значения при любых достаточно больших натуральных n и старший коэффициент являются квадратами целых чисел. Докажите, что существует многочлен $Q(x)$ с целыми коэффициентами такой, что $P(x) = Q(x)^2$.

Задача 2.3. Про многочлен $P(x)$ с целыми коэффициентами известно только то, что его значения при любых достаточно больших натуральных n являются квадратами целых чисел. Докажите, что существует многочлен $Q(x)$ с целыми коэффициентами такой, что $P(x) = Q(x)^2$.

Здесь и далее используется следующее обозначение:

$$P_k(x) = x(x+1)\dots(x+k-1),$$

где k — некоторое натуральное число.

Задача 2.4. Пусть приведённый многочлен $Q(x)$ степени $l > 2$ с действительными коэффициентами таков, что для некоторого положительного b каждый из многочленов $R(x) = Q(x) - b$ и $S(x) = Q(x) + b$ имеет ровно l различных действительных корней. Пусть $r_1 < r_2 < \dots < r_l$ и $s_1 < s_2 < \dots < s_l$ их корни соответственно. Упорядочьте элементы множества $\{r_1, r_2, \dots, r_l, s_1, s_2, \dots, s_l\}$.

Задача 2.5. Докажите, что многочлен $P_k(x) + c$ ни при каких натуральных $k > 4$ и c не является квадратом другого многочлена с целыми коэффициентами.

Задача 2.6. Докажите, что для каждого комплексного a степень НОД многочленов $P_k(x) - a$ и $P_k'(x)$ не превосходит 2, более того, если k нечётно, то она не превосходит 1.

Задача 2.7. Предположим, что существуют многочлены $Q(x), R(x)$ степени, не меньшей 2, с рациональными коэффициентами такие, что $P_k(x) = R(Q(x))$. Докажите, что тогда k чётно, и степень многочлена $Q(x)$ равна ровно 2.

Задача 2.8 (В. А. Сендеров). Найдите все натуральные числа k, c такие, что выражение $P_k(n) + c$ является точной степенью для всех натуральных чисел n.

3 Разное

Задача 3.1. Даны многочлены $f, g \in \mathbb{Z}[x]$. Известно, что для бесконечно многих натуральных n число $f(n)$ делится на $g(n)$.

а) Докажите, если если старший коэффициент g равен 1, то $g \mid f$ (в $\mathbb{Z}[x]$).

б) Докажите, что всегда найдется бесконечная арифметическая прогрессия A натуральных чисел такая, что $g(n) \mid f(n)$ для любого $n \in A$.

Задача 3.2. Дан многочлен $f \in \mathbb{Z}[x]$ и натуральные числа a_1, a_2,..., a_m. Известно, что для любого целого n число $f(n)$ делится хотя бы на одно из чисел a_1, a_2,..., a_m. Докажите, что существует такое натуральное k, что $k \leq m$ и $f(n)$ делится на a_k для любого целого n.

Каждый многочлен $f \in \mathbb{Z}[x]$ определяет функцию $\mathbb{Z}_n \to \mathbb{Z}_n$, поскольку вычет $f(m)$ по модулю n зависит только от вычета m по модулю n.

Задача 3.3. а) Докажите, что если функция $\mathbb{Z}_n \to \mathbb{Z}_n$ реализуется многочленом из $\mathbb{Z}[x]$, то она реализуется и многочленом из $\mathbb{Z}[x]$, степень которого не превышает $n-1$.

б) Для каких n любая функция $\mathbb{Z}_n \to \mathbb{Z}_n$ реализуется многочленом из $\mathbb{Z}[x]$?

в) Найдите все натуральные $n > 1$, для которых верно следующее утверждение: если $f \in \mathbb{Z}$, $\deg f \leqslant n-1$ таков, что $f(m)$ делится на n при всех целых m, то все коэффициенты f делятся на m.

г) Для каких n любая функция $\mathbb{Z}_n \to \mathbb{Z}_n$, удовлетворяющая условию

$$\text{НОД}(a-b,n) \mid \text{НОД}(f(a)-f(b),n), \qquad a,b \in \mathbb{Z}_n,$$

реализуется многочленом из $\mathbb{Z}[x]$?

Задача 3.4. Пусть $f \in \mathbb{Z}[x]$ задает биекцию по любому простому модулю. Докажите, что f линейный.

Задача 3.5. Про многочлены f и g с целыми коэффициентами известно, что при любом целом x число $f(g(x))-x$ делится на данное целое n. Докажите, что число $g(f(x))-x$ тоже делится на n при любом целом x.

Многочлены в теории чисел

(Продолжение)

0 Вспомогательные факты

0.5 Алгебраические числа и минимальные многочлены

Комплексное число α называется *алгебраическим*, если существует ненулевой многочлен $f \in \mathbb{Q}[x]$ такой, что $f(\alpha) = 0$. Например, $\sqrt{2} + \sqrt{3}$ — алгебраическое число, поскольку $f(\sqrt{2} + \sqrt{3}) = 0$, где $f(x) = x^4 - 10x^2 + 1$. Очевидно, множество алгебраических чисел содержит $\mathbb{Q}$.

Ненулевой многочлен $f \in \mathbb{Q}[x]$ минимальной степени, для которого $f(\alpha) = 0$, называется *минимальным многочленом* алгебраического числа α. Степень этого многочлена называется *степенью* числа α.

Несложно понять, что минимальный многочлен любого алгебраического числа всегда неприводим в $\mathbb{Q}[x]$. Кроме того, любой многочлен $h \in \mathbb{Q}[x]$, имеющий α своим корнем, делится на минимальный многочлен. Действительно, разделим многочлен h на минимальный многочлен f с остатком:

$$h = fq + r,$$

где $q, r \in \mathbb{Q}[x]$ и $\deg r < \deg f$. Подставив $x = \alpha$ в уравнение выше, найдём, что $r(\alpha) = 0$. Следовательно, из условия минимальности f получаем, что r тождественно равен 0, то есть h делится на f.

Из доказанного немедленно следует

Факт 0.7. Каждый неприводимый многочлен $f \in \mathbb{Q}[x]$ является минимальным многочленом для каждого из своих корней.

Задача 0.8. а) Пусть f — неприводимый многочлен с рациональными коэффициентами. Докажите, что f и f' взаимно просты.

б) Пусть f — многочлен в $\mathbb{Q}[x]$. Докажите, что многочлены f и f' **не** взаимно просты тогда и только тогда, когда существует непостоянный многочлен g такой, что $g^2 \mid f$.

в) Докажите, что у неприводимого (в $\mathbb{Q}[x]$) многочлена нет кратных комплексных корней (и, следовательно, количество его комплексных корней совпадает с его степенью).

Непустое множество комплексных чисел $\mathbb{F}$ называется *числовым полем*, если оно состоит не только из нуля, и вместе с любыми числами $a, b \in \mathbb{F}$ оно содержит также числа $a + b$, ab, $-a$ и a^{-1} (последнее — в случае $a \neq 0$). Иначе говоря, в поле можно совершать все обычные арифметические операции (сложение, умножение, вычитание и деление на ненулевое число), получая числа, также принадлежащие этому полю. (В этом проекте под полями понимаются именно числовые поля.)

Поскольку большинство алгебраических выкладок использует ровно эти операции, многие факты, доказательства которых использует лишь эти действия, продолжают оставаться верными над любым полем. Так, обозначая через $\mathbb{F}[x]$ множество многочленов с коэффициентами из $\mathbb{F}$, нетрудно показать, что в $\mathbb{F}[x]$ верны теоремы о линейном представлении НОД и основная теорема арифметики (факты 0.1 и 0.2).

Здесь полезно заметить, что поиск НОД двух многочленов (алгоритмом Евклида) не зависит от того, над каким полем это происходит. Значит, и полученный НОД не зависит от поля (лишь бы все коэффициенты многочленов лежали в этом поле).

Аналогично определению выше, комплексное число α называется *алгебраическим над полем* $\mathbb{F}$, если α является корнем ненулевого многочлена из $\mathbb{F}[x]$. Такой многочлен минимальной степени называется *минимальным многочленом числа* α *над полем* $\mathbb{F}$. Сформулированные выше факты об алгебраических числах также переносятся на случай произвольного поля.

Важные базовые примеры полей получаются из следующего факта.

Факт 0.9. а) Пусть α — алгебраическое число. Тогда множество

$$\mathbb{Q}[\alpha] = \{f(\alpha)\colon f \in \mathbb{Q}[x]\}$$

является полем.

б) Аналогично, если α — алгебраическое число над полем $\mathbb{F}$, то множество

$$\mathbb{F}[\alpha] = \{f(\alpha)\colon f \in \mathbb{F}[x]\}$$

является полем.

Поле $\mathbb{F}[\alpha]$ называется *расширением поля* $\mathbb{F}$ *алгебраическим числом* α.

Доказательство. Мы докажем сразу пункт б).

Для элементов $g(\alpha), h(\alpha) \in \mathbb{F}[\alpha]$ очевидно, что $g(\alpha)+h(\alpha)$, $-g(\alpha)$ и $g(\alpha)h(\alpha)$ лежат в $\mathbb{F}[\alpha]$. Осталось доказать, что $g(\alpha)^{-1} \in \mathbb{F}[\alpha]$, если, конечно, $g(\alpha) \neq 0$,

Пусть $f \in \mathbb{F}[x]$ — минимальный многочлен числа α над $\mathbb{F}$; тогда g не делится на f. поскольку $g(\alpha) \neq 0$. Из неприводимости f теперь вытекает, что НОД$(f, g) = 1$, и по теореме о линейном представлении НОД существуют такие многочлены $a, b \in \mathbb{F}[x]$, что $1 = af + bg$. Подставляя в это равенство α, получаем

$$1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = b(\alpha)g(\alpha),$$

то есть число $g(\alpha)^{-1} = b(\alpha)$ лежит в $\mathbb{F}[x]$.

Замечание. Применяя деление на f с остатком, несложно получить, что каждый элемент в $\mathbb{F}[\alpha]$ представляется как $g(\alpha)$, где $g \in \mathbb{F}[x]$ и $\deg g < \deg f$ (проведите эту выкладку!).

Следующую задачу можно решать по-разному; один из возможных путей решения опирается на такую известную лемму.

Факт 0.10. Пусть задана система однородных линейных уравнений, то есть система вида

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0,\\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0,\\ &\vdots\\ a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kn}x_n &= 0, \end{aligned}$$

где a_{ij} — фиксированные (скажем, рациональные) коэффициенты, а x_i — неизвестные. Тогда, если количество уравнений k меньше количества неизвестных n, то у системы есть (рациональное) решение, в котором не все значения переменных нулевые.

Эту лемму можно доказать, например, последовательным исключением неизвестных. Лемма верна и над любым полем: если коэффициенты принадлежат полю $\mathbb{F}$, то можно найти и решение, в котором все значения неизвестных лежат в $\mathbb{F}$.

Следующая задача также допускает обобщение над любым полем, но для простоты восприятия мы формулируем её над полем $\mathbb{Q}$.

Задача 0.11. а) Пусть α — алгебраическое число, и $\mathbb{F} = \mathbb{Q}[\alpha]$. Тогда любое число в $\mathbb{F}$ алгебраично.

б) Пусть число α алгебраично, а число β алгебраично над $\mathbb{F} = \mathbb{Q}[\alpha]$. Тогда β алгебраично.

в) Множество $\overline{\mathbb{Q}}$ всех алгебраических чисел является полем.

г) Более того, любое число, алгебраическое над $\overline{\mathbb{Q}}$, лежит в $\overline{\mathbb{Q}}$. (Такие поля называются *алгебраически замкнутыми*.

Пусть α и β — алгебраические числа; положим $\mathbb{F} = \mathbb{Q}[\alpha]$. Тогда поле $\mathbb{F}[\beta]$ обозначается также как $\mathbb{Q}[\alpha, \beta]$. Нетрудно проверить, что $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\beta, \alpha]$.

Аналогично можно определить поле $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ при $\alpha_i \in \overline{\mathbb{Q}}$.

Задача 0.12 (Теорема о примитивном элементе). а) Пусть α и β — два алгебраических числа. Докажите, что существует алгебраическое число γ такое, что $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$. Более того, это число можно искать в виде $\gamma = \alpha + t\beta$ при $t \in \mathbb{Q}$.

б) Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — алгебраические числа. Докажите, что существует алгебраическое число γ такое, что $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{Q}[\gamma]$. В каком виде можно искать γ в этом случае?

0.6 Круговые многочлены

Комплексное число z называется *примитивным корнем степени n из* 1, если $z^n = 1$, но $z^k \neq 1$ при $1 \leqslant k < n$. Следующие свойства несложно вытекают из определений.

Факт 0.13. а) Любой корень степени n из 1 является степенью (любого) примитивного корня.

б) Число $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ — примитивный корень степени n из 1.

в) Все примитивные корни степени n из 1 имеют вид $\varepsilon_d = \cos\frac{2\pi d}{n} + i\sin\frac{2\pi d}{n}$, где $\text{НОД}(d, n) = 1$.

г) Если ε — примитивный корень степени n из 1, то все примитивные корни степени n из 1 имеют вид ε^d, где $\text{НОД}(d, n) = 1$.

(n-й) круговой многочлен (или *(n-й) многочлен деления круга*) — это многочлен

$$\Phi_n(x) = \prod_{\varepsilon}(x - \varepsilon),$$

где ε пробегает множество всех примитивных корней степени n из 1. Из предыдущего факта следует, что

$$\Phi_n(x) = \prod_{d \leqslant n,\ (d,n)=1} (x - \varepsilon^d),$$

где ε — любой примитивный корень степени n из 1.

Приведём несколько примеров круговых многочленов:

$$\Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$

Отметим несколько полезных фактов о круговых многочленах:

• Степень $\Phi_n(x)$ из определения кругового многочлена равна количеству чисел, взаимно простых с n и не превосходящих n, то есть $\varphi(n)$.

• Так как каждый корень степени n из 1 является примитивным корнем некоторой степени d из 1, где $d \mid n$, и наоборот, то верна следующая формула

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

• $\Phi_n(x) \in \mathbb{Z}[x]$. Это доказывается по индукции из предыдущей формулы: $\Phi_n(x)$ получается делением $x^n - 1$ на многочлен с целыми коэффициентами и старшим коэффициентом 1.

Задача 0.14. а) Пусть p — простое число. Докажите, что: Если $p \mid n$, то $\Phi_n(x^p) = \Phi_{np}(x)$;

б) Если $p \nmid n$, то $\Phi_n(x^p) = \Phi_{np}(x)\Phi_n(x)$;

в) Если $\text{НОД}(n, a) = 1$, то $\Phi_n(x^a) = \prod_{d|a} \Phi_{nd}(x)$;

г) Если n нечётно, то $\Phi_n(-x) = \Phi_{2n}(x)$.

Задача 0.15. Докажите, что $x^n - 1 = \Phi_n(x)q(x)$, где $q(x) \vdots x^d - 1$ для всех $d \mid n$, $d < n$.

Задача 0.16. Чему равно а) $\Phi_n(0)$? б) $\Phi_n(1)$?

В дальнейшем нам понадобится умение обращаться с многочленами в $\mathbb{Z}_p[x]$. Поскольку их можно так же, как и многочлены в $\mathbb{Q}[x]$, складывать, вычитать, умножать и делить с остатком, то в $\mathbb{Z}_p[x]$ можно определить:

• наибольший общий делителей нескольких многочленов, а также его линейное представление;

• взаимную простоту нескольких многочленов;

• неприводимость и каноническое разложение на неприводимые множители.

Однако в $\mathbb{Z}_p[x]$ не все факты формулируются и доказываются точно так же, как и в $\mathbb{Q}[x]$. В этом можно убедиться на примере следующей задачи.

Задача 0.17. а) Докажите аналог задачи 0.8б для многочлена $f(x)$ в $\mathbb{Z}_p[x]$.

б) Дано простое p и различные натуральные m, n, не делящиеся на p. Докажите, что многочлены $\Phi_m(x)$ и $\Phi_n(x)$ взаимно просты в $\mathbb{Z}_p[x]$.

1 Делители значений многочлена и приложения

Задача 1.11. Даны непостоянные многочлены $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$. Докажите, что

а) пересечение множеств $P(f_1) \cap P(f_2)$ бесконечно;

б) пересечение множеств $P(f_1) \cap P(f_2) \cap \ldots \cap P(f_k)$ бесконечно.

Задача 1.12. Доажите, что для любого многочлена $f \in \mathbb{Z}[x]$,

а) нечетной степени;

б) имеющего хотя бы один вещественный корень,

множество $P(f)$ содержит бесконечно много простых чисел вида $4k + 3$.

Напомним, что через Φ_n обозначается n-й круговой многочлен.

Задача 1.13. Пусть m и n — различные натуральные числа, не делящиеся на простое число p. Докажите, что $p \notin P(\Phi_m, \Phi_n)$.

Задача 1.14. Докажите, что $2 \in P(\Phi_n)$ тогда и только тогда, когда $n = 2^k$.

Задача 1.15. а) Пусть $p \in P(\Phi_n)$. Докажите, либо p — делитель n, либо $p \equiv 1 \pmod{n}$.

б) Докажите частный случай *теоремы Дирихле*: для заданного натурального k в арифметической прогрессии вида $kn+1$ содержится бесконечно много простых чисел.

Задача 1.16. а) Пусть m — целое число, не делящееся на нечётное простое p, и пусть $d = \mathrm{ord}_p(m)$. Докажите, что при любом $i = 0, 1, 2, \ldots$ число p делит $\Phi_{n_i}(m)$, где $n_i = dp^i$.

б) Найдите $P(\Phi_n)$ для любого натурального n.

2 Об одной задаче Сендерова

Задача 2.9. Найдите все натуральные числа n такие, что существуют многочлены $g(x)$ и $h(x)$ с комплексными коэффициентами каждый степени, не меньшей 2, такие, что многочлен

$$f(x) = x^n + \ldots + x^2 + x + 1$$

можно представить в виде $g(h(x))$.

3 Разное

Задача 3.6. Найдите все натуральные n такие, что для любого целого k существует целое a, при котором число $a^3 + a - k$ делится на n.

Задача 3.7. $f = x^d + a_1 x^{d-1} + \ldots + a_d$, где $d > 1$, a_i — целые, p — простое. Докажите, что f задает функцию $\mathbb{Z}_p \to \mathbb{Z}_p$, не являющую биекцией, если

а) $d = p - 1$;

б) d — делитель $p - 1$.

Задача 3.8. Пусть $f \in \mathbb{Z}[x]$ задает биекцию по модулю n. Докажите, что существует такой $g \in \mathbb{Z}[x]$, что $f(g(x)) - x$ делится на n при любом целом x.

Многочлены в теории чисел

Решения

0.5 Алгебраические числа и минимальные многочлены

0.8. а) Предположим противное, существует непостоянный многочлен d с рациональными коэффициентами, который делит как f, так и f'. Поскольку f неприводим, то $d = c\cdot f$, следовательно, f должен делить f', что невозможно, поскольку $\deg f' < \deg f$.

б) Пусть описанный многочлен g существует, $f = g^2h$. Тогда

$$f' = g^2h' + 2gg'h = g\cdot(gh' + 2g'h),$$

и потому $g \mid \text{НОД}(f, f')$. Значит, f и f' не взаимно просты.

Наоборот, если многочлена g не существует, то в каноническом разложении

$$f = h_1h_2\dots h_k$$

на неприводимые сомножители все многочлены $h_1, \dots, h_k$ различны (более точно, среди них нет пропорциональных). Если бы f и f' не были взаимно простыми, то их НОД был бы произведением некоторых из h_i; пусть для определённости он делится на h_1, то есть $h_1 \mid f'$. Но

$$f' = h_1'h_2\dots h_k + h_1h_2'h_3\dots h_k + h_1h_2h_3'\dots h_k + \dots + h_1h_2\dots h_k',$$

где все слагаемые, кроме, возможно, первого, делятся на h_1. Значит, и первое слагаемое тоже должно на этот многочлен делиться. Поскольку h_1 неприводим, делиться на него должен один из сомножителей. Это невозможно, ибо $h_1 \nmid h_i$ при $i \geqslant 2$ по нашему предположению, и $h_1 \nmid h_1'$ по пункту а)

в) Пусть многочлен f неприводим. По пункту а), многочлены f и f' взаимно просты. По пункту б), это значит, что квадрат непостоянного многочлена не может делить f; в частности, f не может делиться на многочлен вида $(x-\alpha)^2$ при $\alpha \in \mathbb{C}$. Это и значит, что у f нет кранных корней.

0.11. а) Пусть $\gamma \in \mathbb{F}[\alpha]$, и пусть n — степень числа α. Тогда при каждом $i = 0, 1, \dots, n$ имеем $\gamma^i = g_i(\alpha)$, где $g_i \in \mathbb{F}[x]$ и $\deg g_i < n$.

Покажем, что существуют числа $\mu_0, \dots, \mu_n \in \mathbb{Q}$, не равные одновременно нулю, для которых

$$\mu_n\gamma^n + \mu_{n-1}\gamma^{n-1} + \dots + \mu_0 = 0;$$

из этого будет следовать даже, что γ — алгебраическое число степени не более n. Равенство выше переписывается как

$$\mu_n g_n(\alpha) + \mu_{n-1}g_{n-1}(\alpha) + \dots + \mu_0 g_0(\alpha) = 0.$$

Значит, достаточно найти (не равные одновременно нулю) числа $\mu_0, \mu_1, \dots, \mu_n \in \mathbb{Q}$ такие, что

$$\mu_n g_n(x) + \mu_{n-1}g_{n-1}(x) + \dots + \mu_0 g_0(x) = 0.$$

Это равенство задаёт систему из n уравнений на переменные $\mu_0, \ldots, \mu_n$ (здесь i-е уравнение — равенство нулю коэффициента при x^{i-1}, при $i = 1, 2, \ldots, n$). По лемме 0.10 эта система имеет требуемое решение.

Замечание. Другое решение этого (и следующего) пунктов можно получить из основной теоремы о симметрических многочленах. Так, например, можно показать, что если $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ — все корни минимального многочлена для α, а $\beta = \beta_1, \ldots, \beta_k$ — аналогичные корни для β, то многочлен с корнями вида $\alpha_i + \beta_j$ имеет рациональные коэффициенты, и поэтому все эти числа алгебраичны.

б) Пусть степень α равна n, а степень β над $\mathbb{F}$ равна k. Как и в прошлом пункте, любой элемент поля $\mathbb{F}$ выражается как сумма чисел $1, \alpha, \ldots, \alpha^{n-1}$, домноженных на рациональные коэффициенты (такая сумма называется *линейной комбинацией*). Тогда каждый элемент из $\mathbb{F}[\beta]$ есть линейная комбинация чисел $1, \beta, \ldots, \beta^{k-1}$ с коэффициентами из $\mathbb{F}$; иначе говоря, он есть линейная комбинация чисел вида $\alpha^i \beta^j$, где $0 \leqslant i < n$ и $0 \leqslant j < k$, уже с рациональными коэффициентами.

Представляя в таком виде каждое из чисел $1, \beta, \ldots, \beta^{nk}$, можно теперь дословно повторить рассуждения из предыдущего пункта, получив, что β алгебраично степени не выше nk.

в) Решение предыдущего пункта показывает, что не только β, но и любой элемент из $\mathbb{Q}[\alpha, \beta]$ алгебраичен (степени не выше nk). Значит, если $0 \neq \alpha, \beta \in \overline{\mathbb{Q}}$, то и $\alpha + \beta, \alpha\beta, \alpha^{-1}, -\alpha \in \mathbb{Q}[\alpha, \beta] \subset \overline{\mathbb{Q}}$. Это и доказывает требуемое.

г) Пусть α является корнем многочлена $p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 \in \overline{\mathbb{Q}}[x]$. Тогда α алгебраично над полем $\mathbb{Q}[p_0, p_1, \ldots, p_n]$. Повторяя рассуждения пункта б) для этого случая, получаем, что α алгебраично.

0.12. а) Пусть f и g — минимальные многочлены чисел α и β соответственно.

Выберем какое-то $t \in \mathbb{Q}$ и рассмотрим число $\gamma = \gamma(t) = \alpha + t\beta$. Положим $\mathbb{F} = \mathbb{Q}[\gamma]$.

Ясно, что $\mathbb{F} \subseteq \mathbb{Q}[\alpha, \beta]$. Если $\beta \in \mathbb{F}$, то и $\alpha = \gamma - t\beta \in \mathbb{F}$, а потому и $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{F}$, то есть $\mathbb{F} = \mathbb{Q}[\alpha, \beta]$. Таким образом, нам надо разобраться, при каких условиях $\beta \notin \mathbb{F}$.

Число β является корнем двух многочленов; $g(x)$ и $f_1(x) = f(\gamma - tx)$ (второго — поскольку $f(\gamma - t\beta) = f(\alpha) = 0$). Коэффициенты обоих многочленов лежат в $\mathbb{Q}[\gamma] = \mathbb{F}$. Значит, и многочлен $h = \text{НОД}(f_1, g)$ также имеет коэффициенты в $\mathbb{F}$. Если h линеен, то получаем, что $\beta \in \mathbb{F}$, чего мы и добиваемся.

В противном случае у многочлена h есть хотя бы два комплексных корня — совпадающих или различных (это — общие корни многочленов f_1 и g). По задаче 0.8в многочлен $g(x)$ не имеет кратных корней, так что и корни h также различны. Один из них — β, обозначим другой через $\beta' \neq \beta$. Тогда β' — корень g, а число $\alpha' = \gamma - t\beta'$ — корень f. Таким образом, $\gamma = \alpha' + t\beta' = \alpha + t\beta$, откуда

$$t = \frac{\alpha - \alpha'}{\beta' - \beta}.$$

Однако выражение в правой части может принимать лишь конечное число значений, ибо у каждого из многочленов f и g по конечному количеству корней. Значит, если выбрать $t \in \mathbb{Q}$, не совпадающее ни с одним из них, мы добьёмся требуемого.

б) Следует из а) непосредственной индукцией. Для шага индукции достаточно заметить, что $\mathbb{Q}[\alpha_{n-1}, \alpha_n] = \mathbb{Q}[\gamma]$ для некоторого γ; а тогда

$$\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_{n-2}, \gamma] = \mathbb{Q}[\gamma']$$

для некоторого γ' по предположению индукции.

Число γ находится в виде $\alpha_1 + t_2\alpha_2 + t_3\alpha_3 + \ldots + t_n\alpha_n$.

0.6 Круговые многочлены

0.14. Во всех пунктах, пользуясь сведениями о степенях круговых многочленов, несложно получить, что многочлены слева и справа имеют одинаковую степень и не имеют кратных корней. Так как старший коэффициент обоих многочленов равен 1, остаётся лишь показать, что каждый корень многочлена слева является также корнем многочлена справа.

0.15. Оба многочлена Φ_n и $x^d - 1$ делят $x^n - 1$ и взаимно просты, так как не имеют общих корней. Поэтому $x^n - 1$ делится на их произведение.

0.16. а) Для начала заметим, что $\Phi_1(0) = -1, \Phi_2(0) = 1$. Если же $n > 2$, то среди корней $\Phi_n(x)$ нет действительных, и эти корни разбиваются на пары комплексно сопряженных чисел модуля 1. Следовательно $\Phi_n(x)$ представляется в виде произведения многочленов вида $x^2 + ax + 1$, поэтому $\Phi_n(0) = 1$.

б) Заметим, что $\Phi_1(1) = 0$, а также 1 не является корнем никакого другого кругового многочлена. Если же n делится на некоторое простое p, то по задаче 0.14а $\Phi_n(1) = \Phi_{np}(1)$. Таким образом, достаточно вычислить $\Phi_n(1)$ для бесквадратных n.

Если n — простое, то $\Phi_n(1) = n$. Если же n делится по крайней мере на два простых числа, одно из которых равно p, то n/p — это натуральное число, большее 1 и по задаче 0.14б

$$\Phi_n(1) = \frac{\Phi_{n/p}(1)}{\Phi_{n/p}(1)} = 1.$$

Суммируя вышенаписанное, получаем, что при $n > 1$

$$\Phi_n(1) = \begin{cases} p & \text{, если } n = p^k \\ 1 & \text{, если } n \neq p^k \end{cases}$$

Замечание. Оба пункта также можно решить по индукции, используя разложение $x^n - 1$ в произведение круговых многочленов.

0.17. а) Решение задачи 0.8б проходит дословно, за одним исключением — именно, надо по-другому обосновать, что $h_1 \nmid h_1'$. Дело в том, что степень h_1', конечно, меньше степени h_1, однако производная многочлена из $\mathbb{Z}_p[x]$ может оказаться нулевой, даже если его степень больше нуля (пример: $(x^p - 1)' = px^{p-1} = 0$). Так что нам надо показать, что $h_1' \neq 0$, если $h_1 \in \mathbb{Z}_p[x]$ — неприводимый многочлен.

Это делается так. Из бинома Ньютона следует, что для многочленов $a, b \in \mathbb{Z}_p[x]$ выполнено равенство $(a + b)^p = a^p + b^p$ (то же равенство, естественно, верно для элементов самого $\mathbb{Z}_p$). Применяя это свойство несколько раз, получаем, что

$$(a_0 + a_1x + a_2x^2 + \ldots + a_kx^k)^p = a_0 + a_1x^p + a_2x^{2p} + \ldots + a_kx^{pk}.$$

Таким образом, если $h_1' = 0$ (что означает, что степени всех мономов в h_1 кратны p), то h_1 является p-й степенью другого многочлена и потому не может быть неприводимым. Это завершает решение.

б) Предположим, что многочлены $\Phi_m(x)$ и $\Phi_n(x)$ делятся на некоторый непостоянный многочлен $g(x)$ в $\mathbb{Z}_p[x]$. Тогда из разложения $x^{mn} - 1$ в произведение круговых многочленов следует, что $g(x)^2 \mid x^{mn} - 1$ (в $\mathbb{Z}_p[x]$, естественно). Следовательно, по пункту а) многочлен $x^{mn} - 1$ и его производная mnx^{mn-1} не взаимно просты в $\mathbb{Z}_p[x]$, что, очевидно, неверно, ибо $p \nmid mn$ и $x \nmid x^{mn} - 1$.

1 Делители значений многочлена и приложения

1.1. а) Достаточно, чтобы все коэффициенты, кроме свободного члена, делились на $m_1m_2 \ldots m_n$.

б) Следует из того, что $f(n) \mid f(n)g(n)$.

в) Следует из того, что множество значений $f(g)$ в целых точках является подмножеством множества значений f в целых точках.

1.2. Предположим противное: пусть $P(f)$ состоит из k простых чисел, то есть $P(f) = \{p_1, p_2, \ldots, p_k\}$. Возьмем $a \in \mathbb{Z}$, для которого $f(a) = b \neq 0$. Зададим многочлен g равенством $g(x) = \frac{f(a+bpx)}{b}$, где $p = p_1p_2 \ldots p_k$. Как нетрудно видеть, g — непостоянный многочлен с целыми коэффициентами, причем $P(g) \subset P(f)$. Свободный член $g(0) = 1$, а все остальные коэффициенты многочлена g делятся на p, следовательно в множестве $P(g)$ не может лежать ни одно из чисел $p_1, p_2, \ldots, p_k$. Но тогда множество $P(g)$ пусто — противоречие. (Заметим, что проведенное рассуждение обобщает доказательство Евклида бесконечности множества простых чисел.)

1.3. По теореме о линейном представлении НОД найдутся такие многочлены $u_1, u_2, \ldots, u_k \in \mathbb{Q}[x]$, что

$$u_1f_1 + u_2f_2 + \ldots + u_kf_k = 1.$$

Если домножить многочлены $u_1, \ldots, u_k$ на натуральное число m, равное НОК знаменателей всех ненулевых коэффициентов $u_1, \ldots, u_k$, получим многочлены

$v_1, v_2, \ldots, v_k \in \mathbb{Z}[x]$. Домножая равенство $u_1 f_1 + u_2 f_2 + \ldots + u_k f_k = 1$ на m, получим $v_1 f_1 + v_2 f_2 + \ldots + v_k f_k = m$. Видим, что если при некотором n числа $f_1(n)$, $f_2(n)$, $\ldots$, $f_k(n)$ делятся на s, то m также делится на s. Отсюда следует, что множество $D(f_1, f_2, \ldots, f_k)$ может содержать лишь делители числа m, и значит оно конечно.

1.4. $f(n)$ делится на m_i для всех n из некоторой арифметической прогрессии с разностью m_i. Так как НОД$(m_1, m_2) = 1$, согласно КТО, прогрессии с разностями m_1 и m_2 пересекаются. Тогда n из их пересечения таково, что $m_1 m_2 \mid f(n)$.

1.5. а) -1 — квадратичный вычет по модулю p вида $4k+1$ и невычет по модулю $4k+3$ (это следует, например, из критерия Эйлера). Это означает, что простые вида $4k+1$ входят в $P(f)$, а простые вида $4k+3$ — нет. Кроме того, очевидно, $2 \in P(f)$.

в) $f(1) = p$, поэтому $p \in P(f)$.

Пусть $f(n)$ делится на простое $q \neq p$. Так как многочлен $x^p - 1$ делится на f (в $\mathbb{Z}[x]$), то $n^p \equiv 1 \pmod q$, откуда $\mathrm{ord}_p(n)$ равен 1 или p, поскольку он делит p.

В первом случае $n \equiv 1 \pmod q$, откуда $f(n) = n^{p-1} + n^{p-2} + \ldots + n + 1 \equiv p \pmod q$. Имеем $p \equiv 0 \pmod q$, откуда $p = q$ — противоречие.

Во втором случае $q - 1$ должно делиться на $\mathrm{ord}_p(n) = p$, т.е. $q \equiv 1 \pmod p$.

Наоборот, пусть простое $q \equiv 1 \pmod p$. Пусть a — первообразный корень по модулю q, и пусть $n = a^{\frac{q-1}{p}}$. Тогда $n \not\equiv 1 \pmod q$, но $n^p \equiv 1 \pmod q$, следовательно $f(n) = \dfrac{n^p - 1}{n - 1}$ делится на q.

Таким образом, в $P(f)$ входят все простые вида $pk + 1$ и p.

1.6. а) Если $f_k(x) = kx - 1$ для некоторого натурального k, то $P(f_k)$ совпадает с множеством всех простых чисел, за исключением делителей k. Тогда ясно, что для $f(x) = (2x-1)(3x-1)$ множество $P(f)$ совпадает с множеством всех простых чисел.

б) Не следует. Для каждого простого p и целых t, s хотя бы одно из чисел t, s, ts является квадратичным вычетом или нулевым вычетом по модулю p. Значит, для многочлена

$$f_{t,s}(x) = (x^2 - t)(x^2 - s)(x^2 - ts)$$

выполнено $p \in P(f_{t,s})$. Достаточно взять t, s такие, что t, s, ts отличны от точных квадратов.

1.7. а) Покажем индукцией по α, что найдется целое n_α такое, что $p^\alpha \mid f(n_\alpha)$.

Для $\alpha = 1$ утверждение следует из включения $p \in P(f)$. Пусть утверждение доказано для некоторого $\alpha \in \mathbb{N}$, и $f(n_\alpha) = p^\alpha m$ для некоторого $m \in \mathbb{Z}$. По лемме Гензеля

$$f(n_\alpha + p^\alpha z) \equiv p^\alpha (m + z f'(n_\alpha)) \pmod{p^{\alpha+1}}.$$

Но так как $p \notin P(f, f')$, то $f'(n_\alpha)$ не делится на p, поэтому достаточно выбрать $z = z_0$ так, чтобы $m + z_0 f'(n_\alpha)$ делилось на p, и положить $n_{\alpha+1} = n_\alpha + p^\alpha z_0$.

б) Возьмём n_α из пункта а). Тогда $f(n_\alpha + p^\alpha)$ делится на p^α, а $f'(n_\alpha)$ не делится на p, и из леммы Гензеля следует, что $v_p(f(n_\alpha + p^\alpha) - f(n_\alpha)) = \alpha$. Значит, либо $v_p(f(n_\alpha))$, либо $v_p(f(n_\alpha + p^\alpha))$ равен в точности α.

1.8. Обратное неверно. Покажем, что существует такой многочлен даже без рациональных корней. Возьмем $f_{t,s}$ из решения задачи 1.6, где t, s и ts — не точные квадраты. Пусть нечетное простое p не является делителем t и s. Тогда $p \notin P(h, h')$ для каждого из многочленов $h(x) = x^2 - a$, где a равно t, s или ts. Тогда, согласно задаче 1.7, $p^\alpha \in D(f_{t,s})$ для сколь угодно больших α.

Для конечного множества простых делителей q чисел t и s возьмем t', s', не делящихся ни на одно из таких простых q и такие, что t', s', $t's'$ — не точные квадраты. Тогда $q^\alpha \in D(f_{t',s'})$ для сколь угодно больших α.

Наконец, для $g(x) = x^2 + x + 2$, согласно задаче 1.7, $2^\alpha \in D(g)$ для сколь угодно больших α.

Согласно задаче 1.4, $f = f_{t,s} f_{t',s'} g$ — искомый многочлен — такой, что $D(f) = \mathbb{N}$.

Замечание. На самом деле искомый многочлен можно найти просто в виде $f_{t,s}$ для подходящих t и s.

1.9. б) Пусть $f = a h_1^{\alpha_1} \dots h_t^{\alpha_t}$, где $a \in \mathbb{Z}$, а $h_1, \dots h_t$ — попарно не пропорциональные примитивные неприводимые многочлены с целыми коэффициентами.

Так как НОД$(h_1, h_1') = 1$, согласно задачам 1.2, 1.3 множество

$$P_1(h_1) \setminus (P(h_1, h_1') \cup P(h_1, a) \cup P(h_1, h_2) \cup \dots \cup P(h_1, h_t))$$

бесконечно; выберем в нем p_1 и, в согласии с задачей 1.7, найдем n_1 такое, что $v_{p_1}(h_1(n_1)) = 1$. Согласно определению p_1, для всех m из прогрессии $n_1 + kp_1^2$ выполнено $v_{p_1}(h_1(m)) = 1$, в то время как $a, h_2(m), \dots, h_t(m)$ не делятся на p_1. Значит, для всех m из прогрессии $n_1 + kp_1^2$ выполнено $v_{p_1}(f(m)) = \alpha_1$.

Аналогично определим p_i, $i = 2, \dots, t$ и соответствующие прогрессии. По КТО, все t прогрессий пересекаются. Пусть m принадлежит всем прогрессиям. Тогда с одной стороны, по условию, $f(m) = u^s$, для некоторых целых u и $s > 1$. С другой стороны, $v_{p_i}(f(m)) = \alpha_i$, $i = 1, \dots, t$, поэтому все α_i кратны s, тем самым, $f = ar^s$, где $r \in \mathbb{Z}[x]$. Так как $f(m) = u^s = ar(m)^s$, константа a является точной s-й степенью. Окончательно, f представим в искомом виде $f = q^s$.

Замечание. Условие задачи можно ослабить, потребовав, чтобы точными степенями были значения f лишь на некоторой бесконечной арифметической прогрессии A. В решении при выборе p_i тогда требуем еще, чтобы p_i не было делителем разности этой прогрессии. Тогда наши прогрессии с разностями p_i^2 пересекутся с прогрессией A.

1.10. Задача непосредственно следует из следующей (при помощи 1.5а). Но мы приведём и непосредственное решение.

Мы докажем существование *одного* простого $p = 4k + 1 \in P(f)$; доказательство того, что таких простых бесконечно много, можно теперь получить так же, как и в задаче 1.2.

Пусть $\deg f = n$. Рассмотрим на минутку многочлен $f(x+i)$, где i — мнимая единица. Он представляется в виде $f(x+i) = P_1(x) + iP_2(x)$, где $P_1(x), P_2(x) \in \mathbb{Z}[x]$, причём $\deg P_1 = n$, $\deg P_2 = n-1 \geqslant 0$. Значит, существует такое $k \in \mathbb{Z}$, что числа $a = P_1(k)$ и $b = P_2(k)$ ненулевые, причём $|P_1(k)| > |P_2(k)|$. Заменив $P(x)$ на $P(x+k)$, мы можем считать, что $f(i) = a + bi$, где $|a| > |b| > 0$; тогда $f(-i) = a - bi$.

Пусть теперь $d = \text{НОД}(a, b)$, $a = a'd$, $b = b'd$; тогда $|a'| \geqslant |a|/|b| > 1$. Число $a'^2 + b'^2$ больше 2 и не может делиться на 4; значит, оно имеет нечётный простой делитель p. Поскольку числа a' и b' взаимно просты, они не могут делиться на p, и оно имеет вид $p = 4k+1$.

Положим $Q(x) = f(x) - a - bx$. Значения $Q(x)$ в точках $\pm i$ равны нулю, поэтому он делится на $(x-i)(x+i) = x^2+1$. Поскольку x^2+1 приведённый, получаем, что $f(x) = a + bx + (x^2+1)R(x)$ для некоторого $R(x) \in \mathbb{Z}[x]$.

Пусть теперь n — такое число, что $nb' \equiv -a' \pmod{p}$. Тогда $a + bn = d(a' + b'n)$ делится на p и $b'^2(n^2+1) = (b'n)^2 + b'^2 \equiv a'^2 + b'^2 \equiv 0 \pmod{p}$; поскольку b' не делится на p, получаем, что $p \mid n^2+1$. Значит, и число $f(n) = (a+bn) + (n^2+1)R(n)$ делится на p.

1.11. Мы докажем сразу пункт б).

Ясно, что достаточно ограничиться случаем, когда все многочлены f_i неприводимы над $\mathbb{Z}$ (если они приводимы, достаточно применить факт для некоторых их неприводимых делителей).

Пусть α_i — корень многочлена f_i, при $i = 1, 2, \ldots, k$. По теореме о примитивном элементе, существует алгебраическое число γ такое, что $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_k] = \mathbb{Q}[\gamma]$. В частности, это означает, что существуют такие многочлены $A_i \in \mathbb{Q}[x]$, что $\alpha_i = A_i(\gamma)$.

Пусть g — минимальный многочлен числа γ. Заметим, что $f_i(A_i(\gamma)) = 0$, так что многочлены $f_i(A_i(x))$ делятся на g при всех $i = 1, 2, \ldots, k$, то есть

$$f_i(A_i(x)) = g(x)h_i(x).$$

Коэффициенты многочленов из равенств выше могут быть нецелыми (но они рациональны); пусть N — наибольшее простое число, на которое делится какой-нибудь из знаменателей этих коэффициентов.

По задаче 1.2, существует бесконечно много простых чисел, делящих значения g в целых точках. Пусть $p > N$ — такое простое число, и пусть $g(n)$ — соответствующее значение. Тогда числители рациональных чисел $f_i(A_i(n)) = g(n)h_i(n)$ делятся на p, поскольку знаменатели чисел $P_i(n)$ и $Q_i(n)$ на него не делятся.

Единственная оставшаяся проблема заключается в том, что числа $A_i(n)$— рациональные, а не целые. Однако их знаменатели также не делятся на p. Значит, если $A_i(n) = k_i/\ell_i$ для взаимно простых целых k_i и ℓ_i, то можно выбрать такое целое m_i, что $k_i \equiv \ell_i m_i \pmod{p}$. Тогда $f_i(m_i) \equiv f_i(k_i/\ell_i) \equiv 0 \pmod{p}$. Значит, $p \in P(f_i)$ при всех $i = 1, 2, \ldots, k$.

1.12. Если $x \mid f$, то $D(f) = \mathbb{N}$, и утверждение очевидно. В противном случае пусть $b \neq 0$ — свободный член; заменяя f на $f(bx)/b \in \mathbb{Z}[x]$, можем считать, что $b = 1$. Без ограничения общности f считаем неприводимым, а его старший коэффициент положительным. Как и в задаче 1.10, достаточно показать, что найдется хотя бы одно простое $p \equiv 3 \pmod 4$, такое что $p \in P(f)$.

а) Предположим, что $\deg f$ нечетна. Рассмотрим большое *отрицательно* целое число $-n$, делящееся на 4. Тогда $f(-n) < 0$ и $f(-n) \equiv f(0) \equiv 1 \pmod 4$, поэтому $f(-n) = -(4k+3)$ для некоторого натурального k. Тогда в разложении $4k+3$ на простые множители должно содержаться искомое простое $p \equiv 3 \pmod 4$.

б) Если $D(f)$ содержит натуральное число, сравнимое с 3 по модулю 4, можно применить те же рассуждения, что и выше. В противном случае, поскольку f — неприводимый, у него нет кратных корней. Так как он имеет вещественный корень, найдется интервал (α, β), на котором f принимает только отрицательные значения.

Теперь выберем рациональное число $\frac{a}{b} \in (\alpha, \beta)$ (где a и b взаимно простые), такое что b не имеет простых делителей вида $4k+3$, а $4 \mid a$ (можно положить, например, $b = 5^N$ для подходящего N). Вспомним, что $f(a) \equiv 1 \pmod 4$. Более того, $f(a) > 0$, иначе $-f(a)$ — натуральное число вида $4k+3$, и работает рассуждение из пункта а). Тогда $f\left(\frac{a}{b}\right) = -\frac{c}{d}$, где $d = b^n \equiv 1 \pmod 4$, и натуральное c удовлетворяет условию

$$c = -b^n f\left(\frac{a}{b}\right) \equiv -f(a) \equiv 3 \pmod 4.$$

Поэтому найдется простое $p \mid c$, такое что $p \equiv 3 \pmod 4$. По нашему предположению $p \nmid b$; значит, найдется $a' \in \mathbb{Z}$, такое что $a \equiv ba' \pmod p$. Тогда имеем $b^n f(a') \equiv b^n f\left(\frac{a}{b}\right) = -c \equiv 0 \pmod p$, и искомое p найдено.

1.13. Решение 1. Предположим, противное, тогда для некоторого целого a многочлены $\Phi_m(x)$ и $\Phi_n(x)$ делятся на $x - a$ в $\mathbb{Z}_p[x]$, что противоречит задаче 0.17б.

1.13. Решение 2. Предположим, что $\Phi_m(k)$ и $\Phi_n(k)$ делятся на p. Тогда $k^m - 1$ и $k^n - 1$ тоже делятся на p. Пусть $m < n$. Тогда $x^{mn} - 1$ представляется в виде $(x^m - 1)\Phi_n(x)h(x)$, где $h \in \mathbb{Z}$. Подставляя k, получаем, что $v_p(k^{mn} - 1) > v_p(k^m - 1)$. Но так как n не делится на p, это противоречит LTE-лемме для $a = k^m$ и $b = 1$.

1.14. Следует напрямую из задачи 0.14, поскольку $2 \in P(f)$ если и только если хотя бы одно из чисел $f(0)$, $f(1)$ четно.

1.15. а) Пусть $\Phi_n(m)$ делится на простое число p. Тогда $m^n \equiv 1 \pmod p$. Пусть $d = \mathrm{ord}_p(m)$, тогда $d \mid n$ и $d \mid p - 1$.

Если $d = n$, то $n \mid p - 1$ и $p \equiv 1 \pmod n$.

Иначе $d < n$ и в $\mathbb{Z}[x]$ выполнено равенство $x^n - 1 = (x^d - 1) \cdot \Phi_n \cdot f$ для некоторого $f \in \mathbb{Z}[x]$. Отсюда $m^n - 1 = (m^d - 1) \cdot \Phi_n(m) \cdot f(m)$, где $p \mid m^d - 1$ и $p \mid \Phi_n(m)$. Следовательно,

$$v_p(m^n - 1) > v_p(m^d - 1).$$

С другой стороны, применив LTE-лемму для $a = m^d$ и $b = 1$, имеем

$$v_p(m^n - 1) - v_p(m^d - 1) = v_p(n/d).$$

Значит, $p \mid (n/d)$, откуда $p \mid n$.

б) Следует из а) и задачи 1.2.

1.16. а) Пусть $k = v_p(m^d - 1)$. Тогда для любого целого a имеем:

- если $d \nmid a$, то $p \nmid m^a - 1$ (вытекает из свойств порядка по модулю p);
- если $d \mid a$, то $v_p(m^a - 1) = k + v_p(a/d)$ (из LTE-леммы).

Значит, $n_i = dp^i$ — это наименьшее число n, для которого $p^{k+i} \mid m^n - 1$.

Выведем из разложения $x^n - 1$ на круговые многочлены формулу

$$\Phi_n = \frac{x^n - 1}{\text{НОК}\{x^d - 1 \colon d \mid n,\ d < n\}}.$$

Действительно, в знаменателе стоит произведение некоторых различных многочленов вида Φ_k при $k \mid n$, так что частное в правой части — многочлен. Более того, многочлен Φ_n делит числитель, но не знаменатель, а любой многочлен Φ_d при $d \mid n$, $d < n$, делит знаменатель, ибо $\Phi_d \mid x^d - 1$. Поэтому после сокращения остаётся лишь Φ_n.

Подставляя в эту формулу $x = m$ и $n = n_i$, получаем, что числитель делится на p^{k+i}, а знаменатель — на меньшую степень p. Отсюда $p \mid \Phi_{n_i}(m)$.

Замечание. На самом деле, в условии приведён список *всех* круговых многочленов, значения которых в точке m делятся на p. Это несложно получить из решения следующего пункта.

б) Согласно задаче 1.15а, в $P(\Phi_n)$ могут лежать лишь (1) простые вида $p = an + 1$ и (2) простые делители числа n.

Все простые вида (1) действительно лежат в $P(\Phi_n)$. Действительно, пусть $p = an+1$; выберем первообразный корень ξ по модулю p. Тогда $\text{ord}_p(\xi^a) = n$, поэтому при $m = \xi^a$ имеем $p \mid m^n - 1$, но $p \nmid m^d - 1$ при всех $d < n$; в частности, $p \nmid \Phi_d(m)$ при $d \mid n$. Значит, $p \mid \Phi_n(m)$ и, следовательно, $p \in P(\Phi_n)$.

С простыми вида (2) ситуация другая. Предположим, что $p \mid n$ и $p \in P(\Phi_n)$: пусть $p \mid \Phi_n(m)$. Пусть $d = \text{ord}_p(m)$; поскольку $p \mid \Phi_n(m) \mid m^n - 1$, имеем $d \mid n$. С другой стороны, $d \mid p - 1$, так что $d \mid \text{НОД}(n, p - 1)$.

Пусть $j = v_p(n)$. Тогда многочлен $\Phi_d \cdot \Phi_{dp} \cdot \ldots \cdot \Phi_{dp^j}$ делит Φ_n, то есть

$$x^n - 1 = \Phi_d \cdot \Phi_{dp} \cdot \ldots \cdot \Phi_{dp^j} \cdot f,$$

где $f \in \mathbb{Z}[x]$. Напомним, что $p^k \mid \Phi_d(m)$ и $p \mid \Phi_{dp^i}(m)$ при всех $i = 1, 2, \ldots, j$ (как и в пункте а), $k = v_p(m^d - 1)$). Значит,

$$v_p(m^n - 1) \geqslant k + j + v_p(f(m)).$$

С другой стороны, $v_p(m^n - 1) = k + j$ по LTE-лемме. Значит, $p \nmid f(m)$.

Пусть $k = n/p^j$. Если $k \nmid p-1$, то $k \neq d$ (и $d \mid k$). В этом случае имеем $\Phi_n \mid f$, и потому $p \nmid \Phi_n(m)$, ибо $p \nmid f(m)$. Это невозможно.

Пусть, наоборот, $k \mid p-1$. Тогда, как уже было сказано выше, существует число $m \in \mathbb{Z}$ такое, что $p \nmid m$ и $\mathrm{ord}_p(m) = k$. Тогда по пункту а) имеем $p \mid \Phi_n(m)$, то есть действительно $p \in P(\Phi_n)$.

Итак, $p \in P(\Phi_n)$ тогда и только тогда, когда $n/p^j \mid p-1$. Заметим, что в этом случае p обязано быть наибольшим простым делителем числа n.

Итого, ответ в задаче такой. $P(\Phi_n)$ состоит из всех простых p таких, что
- либо $p \equiv 1 \pmod{n}$;
- либо p — наибольший простой делитель n, и при этом $n/p^{v_p(n)} \mid p-1$.

2 Об одной задаче Сендерова

2.1. Пусть $Q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$, тогда $Q(x)^k$ можно записать в виде $b_{kn}x^{kn} + b_{kn-1}x^{kn-1} + \ldots + b_0$. Докажем по индукции (по $n-i$), что все коэффициенты a_i являются рациональными. Старший коэффициент a_n рационален по условию; предположим, что $a_n, a_{n-1}, \ldots, a_{n-s}$ рациональны и докажем, что $a_{n-s-1} \in \mathbb{Q}$. Для этого в равенстве $b_{kn}x^{kn} + b_{kn-1}x^{kn-1} + \ldots + b_0 = (a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0)^k$ сравним коэффициенты при x^{kn-s-1}: $b_{kn-s-1} = a_{n-s-1}a_n^{k-1} + S$, где $S = S(a_n, a_{n-1}, \ldots, a_{n-s})$ — значение рациональной функции в рациональных точках $a_n, a_{n-1}, \ldots, a_{n-s}$ и, следовательно, рациональное число. Отсюда, следует, что коэффициент $a_{n-s-1} = \frac{b_{n-s-1}-S}{a_n^{k-1}}$ также является рациональным, что и требовалось доказать. Итак, все коэффициенты Q рациональны.

Представим многочлен Q в виде $\dfrac{a}{b}R$, где a и b — взаимно простые натуральные числа, а R — примитивный многочлен с целыми коэффициентами. Тогда $Q^k = \dfrac{a^k}{b^k}R^k$. По лемме Гаусса, многочлен R^k примитивный, поэтому если $b \neq 1$, то все коэффициенты у Q^k не могут быть целыми.

Другой вариант завершения решения после доказательства рациональности коэффициентов Q такой. Представим теперь многочлен $Q(x)^k$ с целыми коэффициентами в виде произведения двух многочленов $Q(x)$ и $Q(x)^{k-1}$ с рациональными коэффициентами. По лемме Гаусса существует такое рациональное число q, что многочлены $qQ(x)$ и $q^{-1}Q(x)^{k-1}$ имеют целые коэффициенты. Предположим, что $q = a/b$, где a, b — целые взаимно простые числа, тогда многочлены $aQ(x), bQ(x)^{k-1}$ также имеют целые коэффициенты. Следовательно, многочлен $a^{k-1}Q(x)^{k-1} \in \mathbb{Z}[x]$. По алгориту Евклида для нахождения наибольшего общего делителя существуют целые числа s, t такие, что $a^{k-1}s + bt = (a, b) = 1$. Таким образом, многочлен $a^{k-1}sQ(x)^{k-1} + bsQ(x)^{k-1} = Q(x)^{k-1}$ имеет целые коэффициенты.

Продолжая этот процесс, легко придём к тому, что $Q(x)$ будет иметь целые коэффициенты.

2.2. Пусть данный в условии задачи многочлен имеет вид

$$P(x) = b_k^2 x^{2k} + a_{2k-1}x^{2k-1} + \ldots + a_0, \qquad b_k > 0.$$

Перепишем его в виде

$$P(x) = Q(x)^2 + r(x) = (b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0)^2 + r(x),$$

где $\deg r(x) \leqslant k-1$. Чтобы понять, что это возможно, сравним коэффициенты при x^{t+k} для $t = 0, 1, \ldots, k-1$ у двух разных форм записи: $a_{k+t} = 2b_k b_t + \sum_{i=1}^{k-1-t} b_{t+i}b_{k-1}$. Легко видеть, что по этим соотношениям последовательно и однозначно восстанавливаются $b_{k-1}, b_{k-2}, \ldots, b_1, b_0$. Также видно, что все b_i являются рациональными числами; обозначим через M НОК их знаменателей.

По условию, для всех достаточно больших натуральных n мы имеем $P(n) = y_n^2$, где $y_n \in \mathbb{Z}$. После домножения на M^2 мы получим соотношение $(My_n)^2 = Q_1(n)^2 + M^2 r(n)$, где $Q_1(x) = MQ(x) \in \mathbb{Z}[x]$. Если у $r(x)$ положительный старший коэффициент, то при достаточно больших натуральных n верно неравенство $(My_n)^2 > Q_1(n)^2$ и, следовательно, $(My_n)^2 \geqslant (1 + Q_1(n))^2$. Аналогично, если старший коэффициент многочлена $r(x)$ отрицательный, то $(My_n)^2 \leqslant (-1 + Q_1(n))^2$. В обоих случаях выполняется соотношение $2|Q_1(n)| \leqslant |M^2 r(n) - 1|$ при всех достаточно больших натуральных n, что, очевидно, неверно, так как $\deg Q_1 > \deg r$.

Следовательно, многочлен $r(x)$ тождественно равен нулю, и $P(x) = Q(x)^2$. Осталось доказать, что многочлен $Q(x)$ имеет целые коэффициенты, а это следует из задачи 2.1.

2.3. В условии этой задачи у нас нет дополнительных ограничений, как в задаче 2.2, но мы применим следующий красивый трюк. Очевидно, что существует целое ℓ такое, что многочлены $P(x)$ и $P(x+\ell)$ не имеют общих комплексных корней (и потому взаимно просты). Многочлен $H(x) = P(x) \cdot P(x+\ell)$ гарантированно имеет чётную степень и старший коэффициент, являющийся точным квадратом, а также точными квадратами являются и его значения во всех достаточно больших целых точках.

По задаче 2.2 существует многочлен $P_1(x) \in \mathbb{Z}[x]$ такой, что $P(x) \cdot P(x+\ell) = P_1(x)^2$. Рассмотрим его каноническое разложение в $\mathbb{Z}[x]$:

$$P_1 = u h_1 h_2 \ldots h_k,$$

где $u \in \mathbb{Z}$, а h_i — примитивные неприводимые многочлены. Из взаимной простоты многочленов $P(x)$ и $P(x+\ell)$ с учётом леммы Гаусса вытекает, что, скажем, $P(x)$ есть произведение некоторого целого u_1 и квадратов некоторых из многочленов h_i. При этом, поскольку у $P(x)$ есть ненулевые значения в целых точках, являющиеся квадратами, число u_1 — тоже квадрат. Следовательно, $P(x)$ является квадратом многочлена с целыми коэффициентами, что и требовалось доказать.

Отметим, что эту задачу можно решить и по-другому, повторяя решение задачи 1.9.

2.4. Заметим, что каждый интервал (r_i, r_{i+1}) содержит хотя бы один корень производной $R'(x) = Q'(x)$; мы получили $l-1$ различных корней, так что мы перечислили все корни этой производной, и на каждом интервале такой корень единственен. Аналогичное утверждение верно для многочлена $S(x)$. Тогда для любого $i < l$ отрезки $[r_i, r_{i+1}]$ и $[s_i, s_{i+1}]$ имеют общую точку, так как на каждом из них лежит i-ый по порядку корень $Q'(x)$.

Также понятно, что если между двумя последовательными корнями многочлена $R(x)$ лежит $a \geqslant 1$ корней $S(x)$, то $a \geqslant 2$, иначе бы график $y = S(x)$ касался прямой $y = 0$, и у многочлена $S(x)$ был бы кратный корень, что неверно. Аналогично устанавливается факт про последовательные корни многочлена $S(x)$. Таким образом, если, скажем, $[r_i, r_{i+1}]$ содержит s_i, то он содержит и s_{i+1} (отрезок $[r_i, r_{i+1}]$ не может содержать s_{i-1}, иначе бы $[r_{i-1}, r_i]$ и $[s_{i-1}, s_i]$ не имели общих точек). Значит, в любом случае отрезки $[r_i, r_{i+1}]$ и $[s_i, s_{i+1}]$ не просто пересекаются, а один из них лежит внутри другого.

Пусть l чётно. Тогда наименьшим среди всех корней многочленов $R(x)$ и $S(x)$ будет r_1, а наибольшим будет r_l, поэтому верна следующая цепочка неравенств:

$$r_1 < s_1 < s_2 < r_2 < r_3 < s_3 < \ldots < r_{l-1} < s_{l-1} < s_l < r_l.$$

Если l нечётно, аналогичные соображения приводят к ответу

$$s_1 < r_1 < r_2 < s_2 < s_3 < r_3 < \ldots < r_{l-1} < s_{l-1} < s_l < r_l.$$

2.5. Мы найдём даже все пары из натурального k и целого c, для которых

$$P_k(x) + c = Q(x)^2.$$

Заметим, что c является квадратом натурального $b = \pm Q(0)$. Перепишем наше равенство в виде:

$$x(x+1)\ldots(x+k-1) = Q(x)^2 - b^2 = (Q(x) - b)(Q(x) + b).$$

Не умаляя общности, можем считать, что многочлен $Q(x)$ является приведённым. Заметим, что тогда число k равняется удвоенной степени многочлена $Q(x)$, следовательно, должно быть чётно, а также чётен должен быть коэффициент при x^{k-1} у многочлена $Q(x)^2 - b^2$. Поэтому число $0 + 1 + \ldots + (k-1) = k(k-1)/2$, являющееся коэффициентом при x^{k-1} у многочлена $x(x+1)\ldots(x+k-1)$, также является чётным, а так как k чётно, то такое возможно только если $4 \mid k$.

Легко понять, что многочлены $Q(x) - b$ и $Q(x) + b$ имеют ровно по $l = k/2$ различных действительных корней, которые в объединении составляют множество $\{0, -1, \ldots, -k+1\}$. По задаче 2.4 корнями многочлена $Q(x) - b$ являются числа $1-k$, $4-k$, $\ldots$, -3, 0, а корнями многочлена $Q(x) + b$ являются числа $2-k$, $3-k$, $\ldots$, -2, -1. Если $k > 4$, то степень многочленов $Q(x) \pm b$ больше 2, и по теореме Виета у

этих многочленов одинакова сумма корней и одинакова сумма попарных произведений корней. Значит, совпадают и суммы их квадратов, а именно:

$$0^2 + 3^2 + \ldots + (k-4)^2 + (k-1)^2 = 1^2 + 2^2 + \ldots + (k-3)^2 + (k-2)^2,$$

но это равенство не может выполняться, так как для любого t

$$(t-4)^2 + (t-1)^2 = 2t^2 - 10t + 17 > 2t^2 - 10t + 13 = (t-3)^2 + (t-2)^2.$$

Следовательно, $k = 4$, при этом $Q(x) - b = x(x+3), Q(x) + b = (x+1)(x+2)$. Значит, $b = 1$ и $c = b^2 = 1$. Пара чисел $(k, c) = (4, 1)$ является единственным решением задачи.

2.6. Структура многочлена $P_k(x)$ такова, что его производная $P_k'(x)$ имеет ровно $k-1$ корень $r_1, \ldots, r_{k-1}$, причём эти корни можно упорядочить так, чтобы выполнялось неравенство

$$-(k-1) < r_{k-1} < -(k-2) < r_{k-2)} < \ldots < -1 < r_1 < 0.$$

Также график функции $y = |P_k(x)|$ симметричен относительно оси $x = -\frac{k-1}{2}$, поэтому $|P_k(r_i)| = |P_k(r_{k-i})|$ при $1 \leqslant i < k$. Из свойств производной следует, что $|P_k(x)|$ достигает своего максимума на каждом отрезке вида $[-i, -i+1]$ в точке r_i. Следовательно,

$$\frac{|P_k(r_{i-1})|}{|P_k(r_i)|} \geqslant \frac{|P_k(r_i+1)|}{|P_k(r_i)|} = \frac{|r_i+1| \cdot |r_i+2| \ldots |r_i+k|}{|r_i| \cdot |r_i+1| \ldots |r_i+k-1|} = \frac{|r_i+k|}{|r_i|},$$

и при $i \leqslant \frac{k}{2}$ выполняется неравенство $|P_k(r_{i-1})| > |P_k(r_i)|$. По симметрии для $i \geqslant \frac{k+2}{2}$ выполняется обратное неравенство $|P_k(r_{i-1})| < |P_k(r_i)|$.

Таким образом, для каждого комплексного a уравнение $P_k(x) = a$ имеет не более двух корней из множества $\{r_1, \ldots, r_{m-1}\}$ корней $P_k'(x)$. Дальше, если k нечётно, то $P_k(r_i) = -P_k(r_{k-i})$, следовательно количество этих корней в этом случае не больше одного. Из этого и следует требуемое, поскольку все корни P_k' простые (т.е. некратные).

2.7. Заметим, что $P_k'(x) = R'(Q(x)) \cdot Q'(x)$.

Пусть r — некий комплексный корень многочлена R'. Тогда r — общий корень многочленов $R'(x)$ и $R(x) - R(r)$, то есть $x - r \mid \text{НОД}(R'(x), R(x) - R(r))$. Подставляя $Q(x)$ вместо x, получаем $Q(x) - r \mid \text{НОД}(R'(Q(x)), R(Q(x)) - R(r))$. Наконец, поскольку $R'(Q(x)) \mid P_k'(x)$, отсюда вытекает, что $Q(x) - r \mid \text{НОД}(P_k'(x), P_k(x) - R(r))$.

Теперь из задачи 2.6 следует, что степень многочлена $Q(x) - r$, как и многочлена $Q(x)$ должна быть ровно 2, причём k должно быть чётно, что и требовалось доказать.

2.8. Решение 1. По задаче 1.9

$$P_k(x) + c = x(x+1)\ldots(x+k-1) + c = Q(x)^s \qquad (*)$$

для некоторого натурального числа $s \geqslant 2$ и некоторого многочлена $Q(x)$ с комплексными коэффициентами. Пусть старший коэффициент $Q(x)$ равен a, тогда, поскольку

$a^s = 1$, то можно заменить $Q(x)$ на $\frac{1}{a}Q(x)$, поэтому можно считать, что многочлен $Q(x)$ является приведённым, а тогда по задаче 2.1 многочлен Q имеет целые коэффициенты. Не умаляя общности, можно считать, что $Q(x)$ не является степенью другого многочлена, в противном случае мы можем заменить s на другое подходящее натуральное число.

Заметим, что

$$P_k'(x) = (P_k(x) + c)' = (Q(x)^s)' = Q'(x) \cdot Q(x)^{s-1}.$$

Значит, Q^{s-1} делит НОД$(P_k + c, P_k')$. Но по задаче 2.7, степень этого НОД не превосходит 2. Поэтому возможны лишь следующие случаи: (1) $s = 3$, $\deg Q = 1$; (2) $s = 2$, $\deg Q = 1$; и (3) $s = 2$, $\deg Q = 2$.

В случае (1) получаем, что $k = 3$ нечётно, но тогда степень НОД даже не больше 1, так что этот случай невозможен.

В случае (2) имеем $x(x + 1) + c = (x + a)^2$, откуда $a = 1/2$, то есть $Q \notin \mathbb{Z}[x]$.

В случае (3) имеем $x(x+1)(x+2)(x+3)+c = (x^2+ax+b)^2$; сравнивая коэффициенты при x^3 и x^2 в левой и правой частях, получаем $a = 3$, $b = 1$, а тогда $c = 1$, и мы приходим к единственному ответу $(k, c) = (4, 1)$.

2.8. Решение 2. Как мы уже отметили в первом решении, существуют натуральное $s > 1$ и многочлен $Q(x) \in \mathbb{Z}[x]$ такие, что

$$x(x + 1) \dots (x + k - 1) + c = Q(x)^s.$$

Полагая $x = 0$ мы находим, что $c = Q(0)^s = b^s$. Таким образом, верно равенство

$$x(x + 1) \dots (x + k - 1) = Q(x)^s - b^s.$$

Следовательно, $Q(-j)^s = b^s$ для всех $j = 0, 1, \dots, k - 1$. Если s нечётно, то многочлен $Q(x) - b$ имеет минимум k различных корней $0, -1, \dots, -k + 1$ и имеет степень не меньше k. Но тогда степень многочлена $Q(x)^s$ не меньше sk, что больше степени многочлена $P_k(x) = x(x + 1) \dots (x + k - 1)$, а это невозможно.

Предположим, что s чётно, в таком случае достаточно рассмотреть случай $s = 2$, а он разобран в задаче 2.5.

2.9. Заметим сразу, что

$$f(x) = \frac{x^{n+1} - 1}{x - 1}.$$

Пусть α — произвольный комплексный корень многочлена $g'(x)$. Как и в решении задачи 2.7, получаем, что $h(x) - \alpha \mid$ НОД$(f'(x), f(x) - g(\alpha))$. Значит,

$$\deg \text{НОД}(f'(x), f(x) - g(\alpha)) \geqslant 2.$$

Следовательно, существует как минимум два (возможно, совпадающие) корня r, s многочлена

$$f'(x) = \frac{nx^{n+1} - (n + 1)x^n + 1}{(x - 1)^2},$$

такие, что $f(r) = f(s)$. Легко заметить, что 1 не является корнем f', и что у f' нет кратных корней, так что $r \neq s$.

Из формулы для f' следует, что

$$n(s^{n+1} - 1) = (n+1)(s^n - 1) \quad \text{и} \quad n(r^{n+1} - 1) = (n+1)(r^n - 1).$$

Далее, из равенства $f(r) = f(s)$ следует, что

$$\frac{s^{n+1} - 1}{s - 1} = \frac{r^{n+1} - 1}{r - 1}.$$

Из соотношений выше следует тогда, что и

$$\frac{s^n - 1}{s - 1} = \frac{r^n - 1}{r - 1}.$$

Вычитая это равенство из предыдущего, получаем $s^n = r^n$, а тогда и $s - 1 = r - 1$, то есть $s = r$, что невозможно. Поэтому натуральных n, удовлетворяющих условию задачи, не существует.

3 Разное

3.1. а) Разделим f на g с остатком: $f = qg + r$, где $q, r \in \mathbb{Z}[x]$, $\deg r < \deg g$. Тогда найдется N такое, что для всех $n > N$ выполнено $|r(n)| < |g(n)|$, и если $n > N$ таково, что $g(n) \mid f(n)$, то $r(n) = 0$. Получаем, что $r(n) = 0$ для бесконечно многих значений n, поэтому r — нулевой многочлен.

б) После деления f на g с остатком в $\mathbb{Q}[x]$ представим неполное частное в виде q/m, где $m \in \mathbb{N}$ и $g \in \mathbb{Z}[x]$, то есть $f = \frac{qg}{m} + r$, где $r \in \mathbb{Q}[x]$, $\deg r < \deg g$. Тогда найдется N такое, что для всех $n > N$ выполнено $|r(n)| < |g(n)|/m$, и если $n > N$ таково, что $g(n) \mid f(n)$, то $r(n) = 0$. Получаем, что $r(n) = 0$ для бесконечно многих значений n, поэтому r — нулевой многочлен.

Далее, пусть для некоторого $n \in \mathbb{N}$ $g(n) \mid f(n)$, т.е. $m \mid q(n)$. Но тогда $m \mid q(n + mt)$ для любого целого t, и значит, $g(n + mt) \mid f(n + mt)$.

3.2. Предположим противное, тогда для каждого $i = 1, 2, \ldots, m$ найдется целое k_i такое, что $f(k_i)$ не делится на $p_i^{\alpha_i}$, где p_i — простое, а $p_i^{\alpha_i}$ — делитель a_i. Если $p_i = p_j$ и $\alpha_i \leqslant \alpha_j$, то для индекса j можно переопределить $\alpha_j = \alpha_i$ и $k_j = k_i$. После таких переопределений считаем, что равным p_i соответствуют одни и те же α_i и k_i. Согласно КТО, найдется k в пересечении прогрессий вида $k_i + p_i^{\alpha_i} t$. Тогда $f(k)$ не делится ни на одно из $p_i^{\alpha_i}$, и следовательно, ни на одно из a_i. Противоречие.

Каждый многочлен $f \in \mathbb{Z}[x]$ определяет функцию $\mathbb{Z}_n \to \mathbb{Z}_n$, поскольку вычет $f(m)$ по модулю n зависит только от вычета m по модулю n.

3.3. а) Разделим данный многочлен f на $x(x-1)\dots(x-(n-1))$ с остатком: $f = x(x-1)\dots(x-(n-1))g + r$, где где $q, r \in \mathbb{Z}[x]$, $\deg r < n$. Тогда f и r задают одну и ту же функцию $\mathbb{Z}_n \to \mathbb{Z}_n$.

б) Ответ: для простых n.

Для простого $n = p$ для любого набора $f(0), f(1), \dots, f(p-1)$ запишем формулу интерполяционного многочлена Лагранжа. Это многочлен из $\mathbb{Q}[x]$ такой, что знаменатели всех его коэффициентов не делятся на p, т.е. соответствующие им вычеты по модулю p обратимы. Чтобы получить нужный многочлен из $\mathbb{Z}[x]$, достаточно заменить каждый коэффициент на соответствующий вычет из $\{0, 1, \dots, p-1\}$.

Пусть теперь n — составное, и p — некоторый простой делитель n. Тогда функция $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, для которой $f(0)$ и $f(p)$ дают разные остатки при делении на p, очевидно, не реализуется многочленом $f \in \mathbb{Z}[x]$.

в) Ответ: для простых n (и $n = 1$).

Достаточно рассматривать многочлены степени $\leqslant n-1$ с коэффициентами из $\{0, 1, \dots, n-1\}$ (замена каждого коэффициента на коэффициент, дающий тот же остаток при делении на n, не меняет соответствующей функции $\mathbb{Z}_n \to \mathbb{Z}_n$). Размер множества рассматриваемых многочленов равен n^n, что совпадает с размером множества функций $\mathbb{Z}_n \to \mathbb{Z}_n$.

В случае простого $n = p$, поскольку любая функция реализуется многочленом, получаем, что тождественно нулевая функция реализуется только нулевым многочленом.

В случае составного n, как мы знаем из б), имеются функции, не реализуемые многочленом, поэтому найдется функция, реализуемая двумя разными многочленами f и g. Тогда разность $f - g$ — многочлен, не все коэффициенты которого делятся на n, но который задает нулевую функцию $\mathbb{Z}_n \to \mathbb{Z}_n$.

г) Ответ: для n, не делящихся на 8 и на p^2 для нечетного простого p.

Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Функцию, $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, удовлетворяющую условию

$$\text{НОД}(a-b, n) \mid \text{НОД}(f(a) - f(b), n), \qquad a, b \in \mathbb{Z}_n,$$

будем называть *хорошей*. Хорошая функция $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ естественно определяет функции $f_i : \mathbb{Z}_{p_i^{\alpha_i}} \to \mathbb{Z}_{p_i^{\alpha_i}}$, которые, как легко видеть, тоже являются хорошими. Если f задается многочленом из $\mathbb{Z}[x]$, то каждая f_i — тоже (тем же многочленом). Наоборот, если каждая f_i задается многочленом $g_i \in \mathbb{Z}[x]$, то и f задается многочленом $g \in \mathbb{Z}[x]$, в котором каждый коэффициент сравним с соответствующим коэффициентом многочлена g_i по модулю $p_i^{\alpha_i}$ (такие коэффициенты найдутся, по КТО).

Таким образом, вопрос о задании хорошей функции многочленом сводится с этому же вопросу для n, равных степени простого, $n = p^\alpha$.

Для $n = p$, как мы знаем, любая функция $Z_p \to \mathbb{Z}_p$ задается многочленом.

Пусть теперь $\alpha \geqslant 2$. Рассмотрим функцию $h : \mathbb{Z}_{p^\alpha} \to \mathbb{Z}_{p^\alpha}$ такую, что $h(n) = p$, если $n \equiv p \pmod{p^2}$, и $h(n) = 0$ для остальных p. Легко проверить, что эта функция хорошая.

С другой стороны, при нечетном простом p и $\alpha \geqslant 2$, а также при $p = 2$ и $\alpha \geqslant 3$ такая функция не задается многочленом с целыми коэффициентами. Действительно, пусть такой многочлен g существует. Мы знаем, что $g(0) \equiv g(2p) \equiv 0 \pmod{p^2}$ и $g(p) \equiv p \pmod{p^2}$. Тогда $g(p) \equiv g(0) + g'(0)p \pmod{p^2}$, откуда $g'(0)$ не делится на p. Но, если p нечётно, то $g(2p) \equiv g(0) + 2g'(0)p \pmod{p}^2$, поэтому $g'(0)$ делится на p — противоречие. Для $p = 2$ имеем $g(4) \equiv g(0) + 4g'(0) \pmod 8$, и также получаем, что $g'(0)$ делится на p — противоречие.

Остается разобрать случай $n = 4$. Рассмотрим функцию g, такую, что $g(0) = 2$, $g(1) = g(2) = g(3) = 0$. Эта функция задается многочленом $(x-1)(x-2)(x-3)$. Но легко видеть, что каждая хорошая функция является суммой константы и нескольких из функций x, $g(x)$, $g(x-1)$, $g(x-2)$, $g(x-3)$, а значит, задается многочленом.

3.4. Предположим противное, и рассмотрим многочлен $g(x) = f(x+1) - f(x)$. Степень g не меньше 1, и нам достаточно взять $p \in P(g)$: тогда значения f в двух соседних точках будут сравнимы по модулю p.

3.5. Каждое из условий означает, что многочлены f и g задают взаимно обратные биекции $\mathbb{Z}_n \to \mathbb{Z}_n$.

3.6. (Это — задача с APMO2014.)

Ответ: все числа вида $n = 3^l$, где l — целое неотрицательное число.

Фактически мы ищем натуральные n, удовлетворяющие следующему условию $(*)$: *множество* $A = \{a^3 + a \mid a = 0, 1, \ldots, n-1\}$ *— полная система вычетов по модулю* n, или, эквивалентно, *если целые* a, b *таковы, что* $n \mid a^3 + a - b^3 - b = (a-b)(a^2+ab+b^2+1)$, *то* $n \mid a - b$.

Очевидно, $n = 1$ удовлетворяет $(*)$, а $n = 2$ — нет.

Докажем сначала, что $n = 3^l$ удовлетворяет $(*)$ для всех $l \geqslant 1$. Действительно, легко проверить, что a^2+ab+b^2+1 не делится на 3 ни при каких целых a и b (например, перебором остатков по модулю 3, или замечанием, что $a^2+ab+b^2+1 = (a-b)^2+1+3ab$). Значит, если $3^l \mid (a-b)(a^2+ab+b^2+1)$, то $3^l \mid a - b$.

Далее заметим, что если A — не полная система вычетов по некоторому модулю r, то она — не полная система вычетов также и по модулю любого кратного r. Значит, остается доказать, что любое простое $p > 3$ не удовлетворяет $(*)$.

Если $p \equiv 1 \pmod 4$, возьмем $a = 0$ и b такое, что $b^2 \equiv -1 \pmod p$. Тогда $a^2 + ab + b^2 + 1$ делится на p, а $a - b$ не делится.

Теперь пусть $p \equiv 3 \pmod 4$, так что -1 — не квадратичный вычет по модулю n. Достаточно найти такой вычет x, что $x^2 + x + 1$ — квадратичный невычет. Действительно, для такого x, вычет $-(x^2 + x + 1)^{-1} \mod p$ будет квадратичным, поэтому найдется ненулевой вычет a, такой что

$$-1 \equiv a^2(x^2 + x + 1) = (ax)^2 + a \cdot ax + a^2 \pmod p;$$

тогда $(ax)^2+a\cdot ax+a^2+1$ делится на p, в то время как $ax-a$ не делится, за исключением случая $x \equiv 1 \pmod p$. Но если $x \equiv 1 \pmod p$, то заменим его на $x \equiv -2 \pmod p$, не изменив вычет x^2+x+1.

Предположим, что напротив, все вычеты вида x^2+x+1 — квадратичные или нулевые, тогда то же верно для $4(x^2+x+1) = 4(2x+1)^2+3$. Так как $2(2x+1)$ пробегает все вычеты, получаем следующее условие: если вычет y квадратичный, то $y+3$ — тоже. Но, итерируя $y \mapsto y+3$, мы можем получить любой вычет, в том числе и не квадратичный. Противоречие.

3.7. Ясно, что $p > 2$. Для решения нам понадобится формула

$$0^k + 1^k + \ldots + (p-1)^k \equiv \begin{cases} 0, & 1 \leqslant k \leqslant p-2; \\ -1, & k = p-1 \end{cases} \pmod p.$$

При $k = p-1$ это следует из малой теоремы Ферма. При меньших k выберем первообразный корень t по модулю p; тогда сумма в левой части (по модулю p) останется той же самой при домножении на t^k. Поскольку $t^k \not\equiv 1 \pmod p$, отсюда следует, что сумма кратна p.

а) Предположим противное, тогда $f(0)+f(1)+\ldots+f(p-1) \equiv 0+1+\ldots+(p-1) \equiv 0 \pmod p$. С другой стороны, из формул выше получаем $f(0)+f(1)+\ldots+f(p-1) \equiv -1 \pmod p$. Противоречие.

б) Пусть $p-1 = dk$. Применим соображения из пункта а) для многочлена $g = f^k$. Для него

$$-1 \equiv g(0)+g(1)+\ldots+g(p-1) \equiv (f(0))^k + (f(1))^k + \ldots + (f(p-1))^k \equiv \\ \equiv 0^k + 1^k + \ldots + (p-1)^k \equiv 0 \pmod p.$$

3.8. Так как f задает перестановку σ на множестве $\mathbb{Z}_n$, то

$$g = f(f(f(\ldots))) \ (k \text{ итераций})$$

задает перестановку σ^k. Поэтому достаточно взять k такое, что σ^k является тождественной перестановкой (т.е. чтобы k делилось на все длины независимых циклов, на которые распадается σ, подойдет, например, $k = n!$) и положить

$$g = f(f(f(\ldots))) \ (k-1 \text{ итераций}).$$

Список литературы.

1. В. Прасолов. Многочлены. М: МЦНМО, 2003.

2. П.Кожевников, В.Сендеров. Делители значений многочлена. — Сборник «Задачи Санкт-Петербургской олимпиады по математике 2010 года». - СПб.: Невский Диалект, 2010, с. 121-129.

3. Д. Клюев, И. Богданов, А. Канель-Белов. Решение задачи 18.7. Математическое просвещение, серия 3, 2015, выпуск 19, с. 264-266

4. Н. Сафаеи, Об одной задаче В.А. Сендерова, Квант, 2021, № 10, с. 2–11

5. Polynomial Problems from the Awesomemath Summer Program (Xyz)
by Titu Andreescu, Navid Safaei, Alessandro Ventullo.

Polynomials in number theory

Project is prepared and presented by:
Ilya Bogdanov, Boris Frenkin, Pavel Kozhevnikov, Pavel Kozlov, Andrey Ryabichev, Navid Safaei

Abstract

In this project you can get acquainted with some remarkable problems and ideas arising at the intersection of number theory and theory of polynomials. This project consists of several sections each of which is interesting by itself.

Section 0 contains some technical facts which will be quite helpful in other sections.

In Section 1, we investigate the sets of divisors of values of a polynomial with integer coefficients. We start with investigating some concrete polynomials; after that, we suggest to prove some general facts which appear to be quite curious and beautiful. In particular, it appears that for each non-constant polynomial with integer coefficients there are infinitely many primes of the form $p = 4k + 1$ dividing some values of the polynomial. On the other hand, under the extra restriction that the polynomial has at least one real root, the same holds for primes of the form $p = 4k + 3$.

Section 2 is mainly devoted to one difficult number-theoretical problem describing all situations when a product of n consecutive integers increased by a constant is a perfect power. While solving this problem, you will learn both analytical and number-theoretical methods which are quite useful for many other problems.

In Section 3 we collect miscellaneous problems which are interesting by themselves, but they are also related to the problems in other Sections, by means of methods needed for their solutions.

0 Auxiliary facts

0.1 Basic concepts in number theory

Let us list some number-theoretical facts which can be helpful in solving problems.

• Division with remainder and Euclid's algorithm.

• Linear representation of the g.c.d.

• The fundamental theorem of arithmetics (i.e., existence and uniqueness of prime factorization).

Corollary: existence of the canonical representation of integer $n > 1$; namely $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1, \ldots, p_k$ are distinct primes, and $\alpha_1, \ldots, \alpha_k$ are exponents.

The exponent of p in the decomposition of n further denoted by $v_p(n)$.

• Chinese Remainers Theorem.

One of its reformulations reads as follows: consider n (both-sides) infinite arithmetic progressions consisting of integers, such that the steps $d_1, \ldots, d_n$ are pairwise coprime. Then the intersection of those progressions is exactly an arithmetic progression with step $d_1 \cdots d_n$.

• Congruences and residues modulo n.

Congruence $a \equiv b \pmod{n}$ (which reads as 'a and b are congruent modulo n') for integers a, b and a positive integer n means that a and b have equal remainders while diveded by n, or, equivalently, that $n \mid (a-b)$.

A *residue* modulo n is an equivalence class with respect to congruence modulo n (each residue is an arithmetic progression with step n); but, a representative of this class is also called a residue. All n residues form *a complete residue system*, which is denoted by $\mathbb{Z}_n$. If we fix a representative for easch residue, we may put $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. On $\mathbb{Z}_n$, the operations of addition and multiplication are naturally defined. The inverse for a residue a is a residue a^{-1} such that aa^{-1} is equal to 1 in $\mathbb{Z}_n$, i.e., $aa^{-1} \equiv 1 \pmod{n}$. The residue a is invertible (i.e. having an inverse) iff $\gcd(a, n) = 1$.

• Euler's and Fermat's theorems.

Euler's theorem states that for coprime $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ we have $a^{\varphi(n)} \equiv 1 \pmod{n}$, where $\varphi(n)$ is Euler's totient function, i.e., the number of numbers from $\{1, \ldots, n\}$ coprime to n.

Fermat's theorem is a particular case of Euler's theorem for a prime $n = p$ (in which case.$\varphi(p) = p - 1$).

• The *order* of an integer a modulo n is the least positive integer k such that $a^k \equiv 1 \pmod{n}$. (It is clear that the order is defined only if $\gcd(a, n) = 1$.) Let us denote the order of a modulo n by $\mathrm{ord}_n(a)$.

We note the following property of the order: $a^m \equiv 1 \pmod{n}$ iff $\mathrm{ord}_n(a) \mid m$. In particular, by Euler's theorem, it follows that $\mathrm{ord}_n(a) \mid \varphi(n)$.

If $\mathrm{ord}_n(a) = \varphi(n)$, then $1, a, a^2, \ldots, a^{\varphi(n)-1}$ are all the residues which are coprime to n. In this case a is called a *primitive root* modulo n. A primitive root exists iff n equals 2, 4, p^α, or $2p^\alpha$ for a prime $p > 2$ and a positive integer α.

• Let us recall the *LTE-lemma* (Lifting the Exponent Lemma).

Let p be an odd prime, and a, b be distinct integers not divisible by p. If $p \mid a - b$, then

$$v_p(a^n - b^n) = v_p(a - b) + v_p(n),$$

For $p = 2$ the same equality holds whenever $4 \mid a - b$.

• A non-zero residue a modulo an odd prime p is called *quadratic*, if the congruence $x^2 \equiv a \pmod{p}$ has a non-empty solution. The number of (non-zero) quadratic residues is $\frac{p-1}{2}$ — the same as the number of non-quadratic non-zero residues.

Euler's criterion states that a non-zero residue a is quadratic iff $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

0.2 Theory of divisibility in $\mathbb{Q}[x]$

Let us denote by $\mathbb{Q}[x]$ the set of polynomials with rational coefficients, and by $\mathbb{Z}[x]$ the set of polynomials with integer coefficients. We say that polynomials of degree not less than 1 are *non-constant*. A non-constant polynomial $f \in \mathbb{Q}[x]$ of degree d is called *reducible* over $\mathbb{Q}$ (or, reducible in $\mathbb{Q}[x]$) if it can be represented as a product of two polynomial of degree less

than d with retional coefficients. Each non-constant polynomial in $\mathbb{Q}[x]$ is eqither reducible, or *irredusible* over $\mathbb{Q}$. Similarly to the case of integers, one can divide a polynomial in $\mathbb{Q}[x]$ by another nonzero polynomial in $\mathbb{Q}[x]$ with remainder (e.g., via long division). In $\mathbb{Q}[x]$, the g.c.d. of polynomials $f_1, f_2, \ldots, f_k$ is defined as a polynomials of the greatest degree which divides each of $f_1, f_2, \ldots, f_k$. A g.c.d. is unique up to multiplication by a non-zero constant; the g.c.d. of two polynomials can be found by Euclid's algorithm. Polynomials whose g.c.d. equals 1 are called *coprime*. Analogues of the theorem on a linear representation of g.c.d. and the fundamental theorem of arithmetics are the following theorems:

Fact 0.1 (Theorem on linear representation of g.c.d.). For any $f_1, f_2, \ldots, f_k \in \mathbb{Q}[x]$ there exist $u_1, u_2, \ldots, u_k \in \mathbb{Q}[x]$ such that

$$\gcd(f_1, f_2, \ldots, f_k) = u_1 f_1 + u_2 f_2 + \cdots u_k f_k.$$

Fact 0.2 (The fundamental theorem of arithmetic). Each non-constant polynomial $f \in \mathbb{Q}[x]$ can be represented as $f = h_1 \cdot h_2 \cdots h_r$, where h_i are irreducible over $\mathbb{Q}$ polynomials. If $f = h'_1 \cdot h'_2 \cdots h'_s$ is some other such decomposition, then $s = r$, and for some permutation of $h'_1, h'_2, \ldots, h'_r$ we have

$$h'_1 = u_1 h_1, \quad h'_2 = u_2 h_2, \quad \ldots, \quad h'_r = u_r h_r,$$

where $u_1, u_2, \ldots, u_r$ are non-zero rational numbers.

Collecting powers of equal polynomials, one may obtain a *canonical representation*, similar to canonacal representation of a potitive integer as a product of powers of primes.

0.3 Gauss' Lemma

For a polynomial $f \in \mathbb{Z}[x]$, we define the *content* $d(f)$ of f as the g.c.d. of all its coefficients. A polynomial f is *primitive* if $d(f) = 1$.

Fact 0.3. Let $f, g \in \mathbb{Z}[x]$. Then $d(fg) = d(f) \cdot d(g)$. In particular, the product of two primitive polynomials is primitive.

Proof. We start with the second statement. Assume, for the sake of contradiction, that there exist primitive polynomials $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ and $g(x) = b_0 + b_1 x + \cdots + b_m x^m$ in $\mathbb{Z}[x]$ such that their product is not primitive, so that $p \mid d(fg)$ for some prime p.

Let s, t be the least indices such that $p \nmid a_s$, $p \nmid b_t$. Such indices exist since f and g are primitive. The coefficiet of x^{s+t} in fg is equal to

$$c_{s+t} = a_s b_t + (a_{s+1} b_{t-1} + a_{s+2} b_{t-2} + \cdots) + (a_{s-1} b_{t+1} + a_{s-2} b_{t+2} + \cdots).$$

Since a_{s-i} and b_{t-i} are divisible by p for $i > 0$, and $p \mid c_{s+t}$, we obtain $p \mid a_s b_t$ which contradicts the choice of s and t.

To prove the general statement, let us represent arbitrary polynomials $f, g \in \mathbb{Z}[x]$ as

$$f = d(f)f_0, \qquad g = d(g)g_0,$$

where f_0, g_0 are primitive. Since $fg = d(f)d(g) \cdot f_0 \cdot g_0$, and $d(f_0 \cdot g_0) = 1$, we get $d(fg) = d(f)d(g)$, as required.

Fact 0.4 (Gauss' Lemma). A polynomial $\mathbb{Z}$ irreducible over $\mathbb{Z}$ is also irreducible over $\mathbb{Q}$.

Proof. Assume that for some polynomials $h \in \mathbb{Z}[x]$ and $f, g \in \mathbb{Q}[x]$ we have $h = fg$. After multiplying both sides by the l.c.m. of the denominators of all coefficients in f and g, and dividing by the g.c.d. of all numeratorsи, we have:

$$ah = bf_0g_0,$$

where $a, b \in \mathbb{Z}$, and f_0, g_0 are primitive polynomials over $\mathbb{Z}$. By the previous, $a \cdot d(h) = b$, so that after cancellation we have

$$h = d(h)f_0g_0,$$

hence h is reducible over $\mathbb{Z}[x]$.

Using Gauss' lemma and the fundamental theorem of arithmetic for $\mathbb{Q}[x]$, one may prove the following

Fact 0.5 (The fundamental theorem of arithmetic in $\mathbb{Z}[x]$). A non-constant polynomial $f \in \mathbb{Z}[x]$ can be presented as $f = h_1 \cdot h_2 \cdots h_r$, where $h_i \in \mathbb{Z}[x]$ are irreducible over $\mathbb{Q}$ (non-constant) polynomials.

Dividing by constants, one may transform $f = h_1h_2 \cdots h_r$ to *a canonical representation*

$$f = u \cdot g_1^{\alpha_1}g_2^{\alpha_2} \cdots g_k^{\alpha_k},$$

where $g_i \in \mathbb{Z}[x]$ are pairwise coprime primitive irreducible over $\mathbb{Q}$ (non-constant) polynomials, $u \in \mathbb{Z}$, $u \neq 0$, $k \geqslant 1$, $\alpha_i \geqslant 1$.

The canonical representation is unique up to multyplying factors by ± 1.

0.4 Hensel's Lemma

Here we present an important result, which will be helpful further. First, let us note that for a constant polynomila we have:

$$f(x + y) = f(x).$$

Next, for анн linear f we have

$$f(x + y) = f(x) + cy,$$

where c is the coefficient of x, or, in other word, the derivative of f.

The above notes can be generalized for the case of an arbitrary polynomial (e.g., by induction over the degree) in the following way: if f is a polynomials of degree d with integer coefficients, then

$$f(x+y) = f(x) + f_1(x)y + f_2(x)y^2 + \cdots + f_d(x)y^d,$$

where f_i, $i = 1, 2, \ldots, d$ are polynomials with integer coefficients of degree not greater than $d - i$; in fact, $f_i = \frac{f^{(i)}}{i!}$.

The corollary of this statement is the following useful

Fact 0.6 (Hensel's Lemma). Let $f \in \mathbb{Z}$. Then for any prime q, positive integer s, and integers r, n, we have

$$f(n + rq^s) \equiv f(n) + rq^s f'(n) \pmod{q^{2s}}.$$

1 Divisors of polynomial values, with applications

Let us fix the following notation. For $f \in \mathbb{Z}[x]$ denote by $D(f)$ the set of all positive integers m such that $f(n)$ is divisible by m for some integer n. In other words, $m \in D(f)$ iff $f(x) \equiv 0 \pmod{m}$ has an integer root.

More generally, for $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$ denote by $D(f_1, f_2, \ldots, f_k)$ the set of all positive integers m such that the system

$$f_i(x) \equiv 0 \pmod{m}, \;\; i = 1, 2, \ldots, k, \tag{1}$$

has an integer root. Denote by $P(f_1, f_2, \ldots, f_k)$ the set of all primes in $D(f_1, f_2, \ldots, f_k)$.

It is clear that if $f(n)$ is divisible by m, then $f(n + mt)$ is divisible by m для for any integer t. Thus, the set of integers x satisfying (1) is either empty, or is a union of (both-sides) infinite arithmetic progressions with step m.

Obviously, if $m \in D(f)$, then all positive divisors of m also belong to $D(f)$. For a constant polynomial $f = u \in \mathbb{Z}$ the set $D(u)$ coincides with the set of all positive divisors of u. It is easy to show that for a non-constant $f \in \mathbb{Z}$ the set $D(f)$ is infinite.

Problem 1.1. a) Prove that for any positive integers $m_1, \ldots, m_n$ there exists a polynomial $f \in \mathbb{Z}[x]$ such that neither of $m_1, \ldots, m_n$ lies in $D(f)$.

b) Prove that $D(fg) \supset D(f)$ for any two polynomials $f, g \in \mathbb{Z}[x]$.

c) Prove that $D(f(g)) \subset D(f)$ for any two polynomials $f, g \in \mathbb{Z}[x]$.

Problem 1.2. Prove that for any non-constant polynomial $f \in \mathbb{Z}[x]$ the set $P(f)$ is infinite.

Problem 1.3. Prove that if $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$, $k \geqslant 2$, are coprime polynomials, then the set $D(f_1, f_2, \ldots, f_k)$ is finite. (And, therefore, $P(f_1, f_2, \ldots, f_k)$ is finite.)

Problem 1.4. Let $f \in \mathbb{Z}[x]$. Prove that if $m_1, m_2 \in D(f)$ and $\gcd(m_1, m_2) = 1$, then $m_1 m_2 \in D(f)$.

Problem 1.5. Find $P(f)$ if
a) $f(x) = x^2 + 1$;
b) $f(x) = x^2 + x + 1$;
c) $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$, where $p > 2$ is a prime.

Problem 1.6. a) It is clear that if $f \in \mathbb{Z}[x]$ has an integer root, then $P(f)$ is the set of all primes. Show that the converse is false.

b) Assume that $P(f)$ is the set of all primes. Determine if it follows that f has a rational root.

For a polynomial $f \in \mathbb{Z}[x]$ denote by $P_\alpha(f)$ the set of all primes p such that $v_p(f(n)) = \alpha$ for some integer n.

It is clear that if $v_p(f(n)) = \alpha$, then $v_p(f(n + p^{\alpha+1}k)) = \alpha$ for any integer k. Thus the set of integers x such that $v_p(f(x)) = \alpha$, is either empty, or is a union of (both-sides) infinite arithmetic progressions with step $p^{\alpha+1}$.

It is easy to see thet $P_\alpha(f) \subset P(f)$, moreover, for a non-zero $f \in \mathbb{Z}[x]$ we have $P(f) = \bigcup\limits_{\alpha=1}^{\infty} P_\alpha(f)$. Note that for $f \in \mathbb{Z}[x]$ and $k \in \mathbb{N}$ we have $P_\alpha(f) = P_{k\alpha}(f^k)$.

Problem 1.7. Let $f \in \mathbb{Z}[x]$.

a) If $p \in P(f) \setminus P(f, f')$, then $p \in P_\alpha(f)$ for an unbounded set of VALUES OF α.

b) Prove that, in fact, EACH OF the sets $P_\alpha(f) \setminus P(f, f')$ coincides with $P(f) \setminus P(f, f')$ for ALL $\alpha = 1, 2, 3, \ldots$.

Problem 1.8. It is clear that if a polynomial $f \in \mathbb{Z}[x]$ has an integer root, then $D(f) = \mathbb{N}$. Determine if the converse is true.

Problem 1.9. Let $f \in \mathbb{Z}[x]$ be a polynomial such that for any positive integer n the value $f(n)$ is a perfect power, i.e., $f(n) = m(n)^{s(n)}$, for some positive integers $m(n)$ и $s(n) > 1$.

a) Prove that f is reducible (over $\mathbb{Q}$).

b) Prove that there exist a positive integer $s > 1$ and a polynomial $q \in \mathbb{Z}[x]$ such that $f = q^s$.

Problem 1.10. Prove that for a non-constant $f \in \mathbb{Z}[x]$ the set $P(f)$ contains infinitely many primes of the form $4k + 1$.

2 On a problem of V.A. Senderov

Problem 2.1. Let $Q(x)$ be a polynomial with real coefficients such that its leading coefficient is rational. It is known that $Q(x)^k \in \mathbb{Z}[x]$ for some positive integer $k > 1$. Prove that $Q(x) \in \mathbb{Z}[x]$.

Problem 2.2. A polynomial $P(x)$ of even degree with integer coefficients is given. The leading coefficient of $P(x)$ is a perfect square, and $P(n)$ is a perfect square for any large enough positive integer n. Prove that there is a polynomial $Q(x)$ with integer coefficients such that $P(x) = Q(x)^2$.

Problem 2.3. A polynomial $P(x)$ with integer coefficients is given such that $P(n)$ is a perfect square for any large enough positive integer n. Prove that there is a polynomial $Q(x)$ with integer coefficients such that $P(x) = Q(x)^2$.

For every positive integer k, we introduce the polynomial:

$$P_k(x) = x(x+1)\cdots(x+k-1).$$

Problem 2.4. Let $Q(x)$ be a monic polynomial of degree $l > 2$ with real coefficients such that $R(x) = Q(x) - b$ has exactly l different real roots $r_1, r_2, \ldots, r_l$, while $S(x) = Q(x) + b$ has exactly l different real roots $s_1, s_2, \ldots, s_l$, for some positive real b. Sort the elements of the set $\{r_1, r_2, \ldots, r_l, s_1, s_2, \ldots, s_l\}$ under the assumptions $r_1 < r_2 < \cdots < r_l$ and $s_1 < s_2 < \cdots < s_l$

Problem 2.5. Prove that $P_k(x) + c$ is not a square of a polynomial with integer coefficients for any positive integers $k > 4$ and c.

Problem 2.6. Prove that for any complex number a the degree of the g.c.d. of polynomials $P_k(x) - a$ and $P_k'(x)$ does not exceed 2. Moreover, if k is odd then that degree is at most 1.

Problem 2.7. Suppose that there exist polynomials $Q(x)$ and $R(x)$ of degree at least 2 with rational coefficients such that $P_k(x) = R(Q(x))$. Prove that k is even, and $\deg Q(x) = 2$.

Problem 2.8 (V. A. Senderov). Find all positive integers k and c such that $P_k(n) + c$ is a perfect power for any positive integer n.

3 Miscellaneous

Problem 3.1. Let $f, g \in \mathbb{Z}[x]$. Assume that the number $f(n)$ is divisible by $g(n)$ for infinitely many positive integers n.

a) Prove that if the leading coefficient of g equals 1, then $g \mid f$ (in $\mathbb{Z}[x]$).

b) Prove that there exists an infinite arithmetic progression A of positive integers such that $g(n) \mid f(n)$ for any $n \in A$.

Problem 3.2. Let $f \in \mathbb{Z}[x]$, and let a_1, a_2,..., a_m be positive integers. Given that for any integer n the number $f(n)$ is divisible by at lease one of a_1, a_2,..., a_m, prove that there exists a positive integer $k \leq m$ such that $f(n)$ is divisible by a_k for any integer n.

Each polynomial $f \in \mathbb{Z}[x]$ determines a function $\mathbb{Z}_n \to \mathbb{Z}_n$, since $f(m)$ modulo n is uniquely defined by the residue of m modulo n.

Problem 3.3. a) Prove that if the function $\mathbb{Z}_n \to \mathbb{Z}_n$ is determined by a polynomial in $\mathbb{Z}[x]$, then it is also determined by a polynomial in $\mathbb{Z}[x]$ whise degree is at most $n-1$.

b) Find all n such that any fuction $\mathbb{Z}_n \to \mathbb{Z}_n$ can be determined by a polynomial in $\mathbb{Z}[x]$.

c) Find all positive integers $n > 1$ satisfying the following condition: if $f \in \mathbb{Z}$, $\deg f \leqslant n-1$, is such that $f(m)$ is divisible by n for all integers m, then all coefficients of f are divisible by n.

d) Find all n such that any function $\mathbb{Z}_n \to \mathbb{Z}_n$ satisfying

$$\gcd(a-b, n) \mid \gcd(f(a)-f(b), n), \qquad a, b \in \mathbb{Z}_n,$$

is determined by a polynomial from $\mathbb{Z}[x]$.

Problem 3.4. Let $f \in \mathbb{Z}[x]$ defines a bijection modulo any prime number. Prove that f has degree 1.

Problem 3.5. Let $f, g \in \mathbb{Z}[x]$ be polynomials such that for any integer x the number $f(g(x)) - x$ is divisible by a fixed integer n. Prove that $g(f(x)) - x$ is also divisible by n for any integer x.

Polynomials in number theory

(Continuation)

0.5 Algebraic numbers and minimal polynomials

A complex number α is called *algebraic* if there exists a non-zero polynomial $f \in \mathbb{Q}[x]$ such that $f(\alpha) = 0$. E.g., $\sqrt{2}+\sqrt{3}$ is algebraic, since $f(\sqrt{2}+\sqrt{3}) = 0$, где $f(x) = x^4 - 10x^2 + 1$. Obviously, the set of algebraic numbers contains $\mathbb{Q}$.

A non-zero polynomial $f \in \mathbb{Q}[x]$ of minimal degree such that $f(\alpha) = 0$ is called a *minimal polynomial* of algebraic number α. The degree of this polunomial is called the *degree* of α.

It is easy to see that the minimal polynomial of any algebraic number is irreducible in $\mathbb{Q}[x]$. Moreover, any polynomial $h \in \mathbb{Q}[x]$ having α as a root, is divisible by the minimal polynomial. Indeed, let us divide h by the minimal polynomial f with remainder:

$$h = fq + r,$$

where $q, r \in \mathbb{Q}[x]$ and $\deg r < \deg f$. Plug in $x = \alpha$ to obtain $r(\alpha) = 0$. By minimality of f, we see that r vanishes, i.e., h is divisible by f.

The next fact follows immediately from the above.

Fact 0.7. Any irreducible $f \in \mathbb{Q}[x]$ is the minimal polynomial for each of its roots.

Problem 0.8. a) Let $f \in \mathbb{Q}[x]$ be an irreducible polynomial. Prove that f and f' are coprime.

b) Let $f \in \mathbb{Q}[x]$. Prove that f and f' are **not** coprime iff there exists a non-constant $g \in \mathbb{Q}[x]$ such that $g^2 \mid f$.

c) Prove that an irreducible (in $\mathbb{Q}[x]$) polynomial has no multiple complex roots (and hence, the number of its complex roots equals its degree).

A non-empty set of complex numbers $\mathbb{F}$ is called a *number field* if it contains some nonzero number and, along with any numbers $a, b \in \mathbb{F}$, it also contains the numbers $a + b$, ab, $-a$ and a^{-1} (the latter — only if $a \neq 0$). In other words, in the field, one can perform all usual arithmetic operations (addition, multiplication, subtraction, and division by a non-zero number), obtaining numbers that also belong to the field. (In this project, number fields are referred to as fields.)

Since most algebraic transformations use exactly the four mentioned operations, many facts whose proofs boil down to only these operations hold over any field. E.g., denoting by $\mathbb{F}[x]$ the set of polynomials with coefficients from $\mathbb{F}$, it is easy to show that the theorem on the linear representation of g.c.d. and the fundamental theorem of arithmetic are true in $\mathbb{F}[x]$ (see facts 0.1, 0.2).

It is useful to note here that the procedure of determining the g.c.d. of two polynomials (by Euclid's algorithm) does not depend on the field over which we work. This means that the resulting g.c.d. does not depend on the field (the only restriction is that all the coefficients of the polynomials must lie in this field).

Similarly to the definition above, a complex number α is said to be *algebraic over a field* $\mathbb{F}$ if α is a root of a nonzero polynomial in $\mathbb{F}[x]$. Such a polynomial of minimal degree is called *minimal polynomial of* α *over the field* $\mathbb{F}$. The above facts about algebraic numbers also carry over to the case of an arbitrary field.

Important (yet basic) examples of number fields are provided by the following fact.

Fact 0.9. a) Let α be the algebraic niumber. Then the set

$$\mathbb{Q}[\alpha] = \{f(\alpha)\colon f \in \mathbb{Q}[x]\}$$

is a field.

b) Similarly, if α is algebraic over $\mathbb{F}$, then the set

$$\mathbb{F}[\alpha] = \{f(\alpha)\colon f \in \mathbb{F}[x]\}$$

is a field.

The field $\mathbb{F}[\alpha]$ is called the *extension of the field* $\mathbb{F}$ *by the algebraic number* α.

Proof. We prove the more general statement b).

For arbitrary $g(\alpha), h(\alpha) \in \mathbb{F}[\alpha]$ it is clear thet $g(\alpha) + h(\alpha)$, $-g(\alpha)$, and $g(\alpha)h(\alpha)$ lie in $\mathbb{F}[\alpha]$. It remains to show that $g(\alpha)^{-1} \in \mathbb{F}[\alpha]$, if $g(\alpha) \neq 0$,

Let $f \in \mathbb{F}[x]$ be the minimal polynomial of α over $\mathbb{F}$; then g is not divisible by f. since $g(\alpha) \neq 0$. Irreducibility of f now implies that $\gcd(f, g) = 1$, and by the theorem on the linear representation of the g.c.d. there are polynomials $a, b \in \mathbb{F}[x]$ such that $1 = af + bg$. Substituting α into this equality, we get

$$1 = a(\alpha)f(\alpha) + b(\alpha)g(\alpha) = b(\alpha)g(\alpha),$$

i.e., $g(\alpha)^{-1} = b(\alpha)$ is in $\mathbb{F}[x]$.

Remark. Using division by f with a remainder, it is easy to get that each element in $\mathbb{F}[\alpha]$ is represented as $g(\alpha)$, where $g \in \mathbb{F}[x]$ and $\deg g < \deg f$ (check this out!).

The next problem can be solved in different ways; one possible solution is based on the following well-known lemma.

Fact 0.10. Consider a system of homogeneous linear equations, that is — a system of the form

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= 0,\\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= 0,\\
&\vdots\\
a_{k1}x_1 + a_{k2}x_2 + \ldots + a_{kn}x_n &= 0,
\end{aligned}$$

where a_{ij} are fixed (say, rational) coefficients, and x_i are variables. Then, if the number k of equations is less than the number n of variables, then the system has a (rational) solution in which not all values of the variables are zero.

This lemma can be proved, for example, by successive elimination of variables. The lemma is also true over any field: if the coefficients belong to the field $\mathbb{F}$, then one can also find a non-trivial solution in which all the values of the variables lie in $\mathbb{F}$.

The next problem can also be generalized over any field, but for ease of perception we formulate it over the field $\mathbb{Q}$.

Problem 0.11. a) Let α be an algebraic number, and put $\mathbb{F} = \mathbb{Q}[\alpha]$. Then any number in $\mathbb{F}$ is algebraic.

b) Let α be an algebraic number, and let number β be algebraic over $\mathbb{F} = \mathbb{Q}[\alpha]$. Then β is algebraic.

c) The set $\overline{\mathbb{Q}}$ of all algebraic numbers is a field.

d) Moreover, any number algebraic over $\overline{\mathbb{Q}}$ lies in $\overline{\mathbb{Q}}$. (Such fields are called *algebraically closed*.)

Let α and β be two algebraic numbers; put $\mathbb{F} = \mathbb{Q}[\alpha]$. Then the field $\mathbb{F}[\beta]$ is also denoted by $\mathbb{Q}[\alpha, \beta]$. It is easy to check that $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\beta, \alpha]$.

Similarly, one can define the field $\mathbb{Q}[\alpha_1, \ldots, \alpha_n]$ for $\alpha_i \in \overline{\mathbb{Q}}$.

Problem 0.12 (Primitive element theorem). a) Let α and β be two algebraic numbers. Prove that there exists an algebraic number γ such that $\mathbb{Q}[\alpha, \beta] = \mathbb{Q}[\gamma]$. Moreover, this number can be chosen in the form $\gamma = \alpha + t\beta$ for $t \in \mathbb{Q}$.

b) Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be algebraic numbers. Prove that there exists an algebraic number γ such that $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{Q}[\gamma]$. In what form can γ be sought for in this case?

0.6 Cyclotomic polynomials

A complex number z is called a *primitive n-th degree root of unity* if $z^n = 1$, but $z^k \neq 1$ при $1 \leqslant k < n$. The following properties follow easily from the definitions.

Fact 0.13. a) Any n-th degree root of unity is a power of (any) such primitive root.

b) The number $\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ is a primitive n-th degree root of unity.

c) Each primitive n-th degree root of unity has the form $\varepsilon_d = \cos\frac{2\pi d}{n} + i\sin\frac{2\pi d}{n}$, where $\gcd(d, n) = 1$.

d) If ε is a primitive n-th degree root of unity, then each primitive n-th degree roots of unity has the form ε^d, where $\gcd(d, n) = 1$.

The *(n-th) cyclotomic polynomial* is the polynomial

$$\Phi_n(x) = \prod_{\varepsilon}(x - \varepsilon),$$

where ε runs through all primitive n-th degree roots of unity. It follows from the previous fact that

$$\Phi_n(x) = \prod_{d \leqslant n,\ (d,n)=1} (x - \varepsilon^d),$$

where ε is any primitive n-th degree root of unity.

Let us present some examples of cyclotimic polynomials:

$$\Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$
$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1,$$

Here are some useful facts about cyclotomic polynomials:

• The degree of $\Phi_n(x)$ is equal to the number of numbers coprime to n and not exceeding n, i.e., $\varphi(n)$.

• Since every n-th degree root of unity is a d-th degree primitive root of unity, where $d \mid n$, and vice versa, the following formula is true:

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

• $\Phi_n(x) \in \mathbb{Z}[x]$. This can be derived from the previous formula, using induction: $\Phi_n(x)$ is obtained after dividing $x^n - 1$ by a monic polynomial with integer coefficients.

Problem 0.14. Let p be a prime. Prove that:

a) If $p \mid n$, then $\Phi_n(x^p) = \Phi_{np}(x)$;

b) If $p \nmid n$, then $\Phi_n(x^p) = \Phi_{np}(x)\Phi_n(x)$;

c) If $\gcd(n, a) = 1$, then $\Phi_n(x^a) = \prod_{d|a} \Phi_{nd}(x)$;

d) If n is odd, then $\Phi_n(-x) = \Phi_{2n}(x)$.

Problem 0.15. Prove that $x^n - 1 = \Phi_n(x)q(x)$, где $q(x) \vdots x^d - 1$ for each $d \mid n$, $d < n$.

Problem 0.16. Find a) $\Phi_n(0)$; b) $\Phi_n(1)$.

In other sections, we will sometimes need to deal with polynomials in $\mathbb{Z}_p[x]$. Since they can be added, subtracted, multiplied and divided with a remainder just like polynomials in $\mathbb{Q}[x]$, one can define in $\mathbb{Z}_p[x]$ the following usual concepts:

• the greatest common divisor of several polynomials, as well as its linear representation;

• coprime polynomials;

• irreducible polynomials and canonical decomposition into irreducible factors.

But not all facts about polynomians in $\mathbb{Z}_p[x]$ are formulated and proved in exactly the same way as in $\mathbb{Q}[x]$. This can be seen, e.g., in the following problem.

Problem 0.17. a) Prove an analogue of Problem 0.8b for a polynomial $f(x)$ in $\mathbb{Z}_p[x]$.

b) Given a prime p and distinct positive integers m, n not divisible by p. Prove that the polynomials $\Phi_m(x)$ and $\Phi_n(x)$ are coprime in $\mathbb{Z}_p[x]$.

1 Divisors of polynomial values, with applications

Problem 1.11. Let $f_1, f_2, \ldots, f_k \in \mathbb{Z}[x]$ be non-constant polynomials. Prove that
a) the set $P(f_1) \cap P(f_2)$;
b) the set $P(f_1) \cap P(f_2) \cap \cdots \cap P(f_k)$
is infinite.

Problem 1.12. For a polynomial $f \in \mathbb{Z}[x]$
a) with odd degree;
b) having at least one real root,
prove that $P(f)$ contains infinitely many primes of the form $4k + 3$.

Recall that we denote by Φ_n the n-th cyclotomic polynomial.

Problem 1.13. Let m and n be distict positive integers not divisible by a prime p. Prove that $p \notin P(\Phi_m, \Phi_n)$.

Problem 1.14. Prove that $2 \in P(\Phi_n)$ iff $n = 2^k$.

Problem 1.15. a) Let $p \in P(\Phi_n)$. Prove that either p divides n, or $p \equiv 1 \pmod{n}$.
b) Prove the following particular case of *Dirichlet's theorem*: for a given positive integer k the arithmetic progression $kn + 1$ contains infinitely many primes.

Problem 1.16. a) Let m be an integer not divisible by an odd prime p, and let $d = \mathrm{ord}_p(m)$. Prove that for any $i = 0, 1, 2, \ldots$, we have $p \mid \Phi_{n_i}(m)$, where $n_i = dp^i$.
b) Find $P(\Phi_n)$ for any positive integer n.

2 On a problem of V.A. Senderov

Problem 2.9. Determine all positive integers n such that there are polynomials $g(x)$ и $h(x)$ with complex coefficients of degree at least 2 satisfying

$$x^n + \cdots + x^2 + x + 1 = g(h(x)).$$

3 Miscellaneous

Problem 3.6. Find all positive integers n such that for any integer k there exists an integer a such that $a^3 + a - k$ is divisible by n.

Problem 3.7. Let $f = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[x]$, where $d > 1$, and let p be a prime number. Prove that the function $\mathbb{Z}_p \to \mathbb{Z}_p$ determined by f is not a bijection, if

a) $d = p - 1$;

b) d is a divisor of $p - 1$,

Problem 3.8. Let $f \in \mathbb{Z}[x]$ deftermine a bijection modulo n. Prove that there exists $g \in \mathbb{Z}[x]$ such that $f(g(x)) - x$ is divisible by n for any integer x.

Polynomials in number theory

Solutions

0 Auxiliary facts

Collecting powers of equal polynomials, one may obtain a *canonical representation*, similar to canonacal representation of a potitive integer as a product of powers of primes.

0.5 Algebraic numbers and minimal polynomials

0.8. a) Assume the contrary, that there exists a non-constant $d \in \mathbb{Q}[x]$ such that d divides both f and f'. Since f is irreducible, we have $d = c \cdot f$, hence f divides f'. It is impossible, since $\deg f' < \deg f$.

b) First, auume that such g exists. We have

$$f' = g^2 h' + 2gg'h = g \cdot (gh' + 2g'h),$$

hence $g \mid \gcd(f, f')$. Therefore, f and f' are not coprime.

Conversely, if the polynomial g does not exist, then in the canonical decomposition

$$f = h_1 h_2 \dots h_k$$

into irreducible factors, all the polynomials $h_1, \dots, h_k$ are different (more precisely, there are no proportional ones among them). If f and f' are not coprime, then their g.c.d. would be the product of some of h_i; let, for definiteness, it is divisible by h_1, i.e. $h_1 \mid f'$. But

$$f' = h_1' h_2 \dots h_k + h_1 h_2' h_3 \dots h_k + h_1 h_2 h_3' \dots h_k + \dots + h_1 h_2 \dots h_k',$$

where all terms, except possibly the first one, are divisible by h_1. This means that the first term must also be divisible by this polynomial. Since h_1 is irreducible, one of the factors must be divisible by it. This is impossible, because $h_1 \nmid h_i$ for $i \geqslant 2$ by our assumption, and $h_1 \nmid h_1$ by item a).

c) Let the polynomial f be irreducible. By item a), the polynomials f and f' are coprime. By item b), this means that the square of a non-constant polynomial does not divide f; in particular, f is not divisible by a polynomial of the form $(x - \alpha)^2$ for $\alpha \in \mathbb{C}$. This means that f has no multiple roots.

0.11. a) Let $\gamma \in \mathbb{F}[\alpha]$, and let n be the degree of α. Then for each $i = 0, 1, \dots, n$, we have $\gamma^i = g_i(\alpha)$, where $g_i \in \mathbb{F}[x]$ and $\deg g_i < n$.

Let us show that there exist numbers $\mu_0, \dots, \mu_n \in \mathbb{Q}$, not all zeroes, for which

$$\mu_n \gamma^n + \mu_{n-1} \gamma^{n-1} + \dots + \mu_0 = 0;$$

that will even yield that γ is an algebraic number of degree at most n. Rewrite the above equality as

$$\mu_n g_n(\alpha) + \mu_{n-1} g_{n-1}(\alpha) + \dots + \mu_0 g_0(\alpha) = 0.$$

Hence, it suffices to find (simultaneously vanishing) numbers $\mu_0, \mu_1, \ldots, \mu_n \in \mathbb{Q}$ such that

$$\mu_n g_n(x) + \mu_{n-1} g_{n-1}(x) + \ldots + \mu_0 g_0(x) = 0.$$

This equality defines a system of n equations for the variables $\mu_0, \ldots, \mu_n$ (here the i-th equation means that the coefficient of x^{i-1} vanishes, $i = 1, 2, \ldots, n$). By Lemma 0.10 this system has a required solution.

Remark. Another solution to this ppart (as well as to the next one) can be obtained from the principal theorem on symmetric polynomials. For example, it can be shown that if $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_n$ are all the roots of the minimal polynomial for α, and $\beta = \beta_1, \ldots, \beta_k$ are all the similar roots for β, then the polynomial whose roots are the numbers of the form $\alpha_i + \beta_j$ has rational coefficients, and therefore all those numbers are algebraic.

b) Denote the degree of α by n, and the degree of β over $\mathbb{F}$ by k. As in the above solution, any element of the field $\mathbb{F}$ is expressed as the sum of numbers $1, \alpha, \ldots, \alpha^{n-1}$ multiplied by rational coefficients (such a sum is called a *linear combination*). Similarly, each element from $\mathbb{F}[\beta]$ is a linear combination of numbers $1, \beta, \ldots, \beta^{k-1}$ with coefficients from $\mathbb{F}$; in other words, it is a linear combination of numbers of the form $\alpha^i \beta^j$, where $0 \leqslant i < n$ and $0 \leqslant j < k$, with rational coefficients.

Representing each of the numbers $1, \beta, \ldots, \beta^{nk}$ in this form, we can now repeat the argument from the solution above, deriving that β is algebraic of degree at most nk.

c) The above solution shows that, in fact, any element in $\mathbb{Q}[\alpha, \beta]$ is algebraic (of degree at most nk). Hence, if $0 \neq \alpha, \beta \in \overline{\mathbb{Q}}$, then $\alpha + \beta, \alpha\beta, \alpha^{-1}, -\alpha \in \mathbb{Q}[\alpha, \beta] \subset \overline{\mathbb{Q}}$. This establishes the desired result.

d) Let α be a root of the polynomial $p_n x^n + p_{n-1} x^{n-1} + \ldots + p_0 \in \overline{\mathbb{Q}}[x]$. Then α is algebraic over the field $\mathbb{Q}[p_0, p_1, \ldots, p_n]$. Repeating the arguments from b) for this case, we see that α is algebraic.

0.12. a) Let f and g be minimal polynomials of α and β, respectively.

We choose some $t \in \mathbb{Q}$ and consider the number $\gamma = \gamma(t) = \alpha + t\beta$. Let $\mathbb{F} = \mathbb{Q}[\gamma]$.

It is clear that $\mathbb{F} \subseteq \mathbb{Q}[\alpha, \beta]$. If $\beta \in \mathbb{F}$, then $\alpha = \gamma - t\beta \in \mathbb{F}$, and therefore also $\mathbb{Q}[\alpha, \beta] \subseteq \mathbb{F}$, whence $\mathbb{F} = \mathbb{Q}[\alpha, \beta]$. Thus, we need to figure out under what conditions $\beta \notin \mathbb{F}$.

The number β is a common root of two polynomials; $g(x)$ and $f_1(x) = f(\gamma - tx)$ (since $f(\gamma - t\beta) = f(\alpha) = 0$). The coefficients of both polynomials are in $\mathbb{Q}[\gamma] = \mathbb{F}$. Hence, the polynomial $h = \gcd(f_1, g)$ also has coefficients from $\mathbb{F}$. If h is linear, then we get that $\beta \in \mathbb{F}$, which is what we want.

Otherwise, the polynomial h has at least two complex roots, either coinciding or different (these are the common roots of the polynomials f_1 and g). By problem 0.8, the polynomial $g(x)$ has no multiple roots, so the roots of h are also different. One of those common roots is β; let us denote another one by $\beta' \neq \beta$. Then β' is a root of g, and the number $\alpha' = \gamma - t\beta'$ is a root of f. Thus, $\gamma = \alpha' + t\beta' = \alpha + t\beta$, whence

$$t = \frac{\alpha - \alpha'}{\beta' - \beta}.$$

However, the expression on the right side can take only a finite number of values, because each of the polynomials f and g has a finite number of roots. So if we choose $t \in \mathbb{Q}$ coinciding with neither of those values, we get the reqired result.

b) Follows from a) by a straightforward induction. For the inductive step, it suffices to note that $\mathbb{Q}[\alpha_{n-1}, \alpha_n] = \mathbb{Q}[\gamma]$ for some γ; hence

$$\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_n] = \mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_{n-2}, \gamma] = \mathbb{Q}[\gamma']$$

for some γ', by the inductive hepothesis.

The number γ is found in the form $\alpha_1 + t_2\alpha_2 + t_3\alpha_3 + \ldots + t_n\alpha_n$.

0.6 Cyclotomic polynomials

0.14. Using information about the degrees of cyclotomic polynomials, it is easy to obtain that the polynomials on the left and on the right have the same degree and do not have multiple roots. Since the leading coefficient of both polynomials is 1, it only remains to show that every root of the polynomial on the left is also a root of the polynomial on the right.

0.15. Both Φ_n and $x^d - 1$ divide $x^n - 1$ and coprime, since they have no common roots. Hence $x^n - 1$ is divisible by their product.

0.16. a) Notice first that $\Phi_1(0) = -1, \Phi_2(0) = 1$. If $n > 2$, then $\Phi_n(x)$ has no real roots, all the roots' absolute values equal to 1, and the roots fall into pairs of conjugates. Hence $\Phi_n(x)$ is a product of polynomials of the form $x^2 + ax + 1$, therefore, $\Phi_n(0) = 1$.

b) Note that $\Phi_1(1) = 0$, and 1 is not a root of any other cyclotomical polynomial. If n is divisible ny a prime p, then by problem 0.14a, we have $\Phi_n(1) = \Phi_{np}(1)$. Thus it suffices to calculate $\Phi_n(1)$ for square-free positive integers n.

If n is a prime, then $\Phi_n(1) = n$. If n is divisible by two distinct primes p and q, then n/p is an integer greater than 1, and by problem 0.14b, we have

$$\Phi_n(1) = \frac{\Phi_{n/p}(1)}{\Phi_{n/p}(1)} = 1.$$

Finally, we conclude that for $n > 1$

$$\Phi_n(1) = \begin{cases} p & \text{, если } n = p^k \\ 1 & \text{, если } n \neq p^k \end{cases}$$

Remark. The problem can also be solved by induction, using decomposition of $x^n - 1$ as a product of cyclotomic polynomials.

0.17. a) The solution of problem 0.8b works literally, with one exception. Namely, we need a different argument showing that $h_1 \nmid h_1'$. The issue is that, although the degree of h_1' is still smaller than that of h_1, it does not by itself yield the result, as the derivative of a non-constant polynomial may vanish in $\mathbb{Z}_p[x]$ (example: $(x^p-1)' = px^{p-1} = 0$). Thus, we need to show additionally that $h_1' \neq 0$, if $h_1 \in \mathbb{Z}_p[x]$ is irreducible.

THis can be done as follows. From Newton's binomial formula, it is easy to see that $(a+b)^p = a^p + b^p$ for all $a, b \in \mathbb{Z}_p[x]$ (in particular, this holds for elements in $\mathbb{Z}_p$). Applying this property several times, we obtain

$$(a_0 + a_1x + a_2x^2 + \ldots + a_kx^k)^p = a_0 + a_1x^p + a_2x^{2p} + \ldots + a_kx^{pk}.$$

Thus, if we had $h_1' = 0$ (which means that the degrees of monomials in h_1 are all divisible by p), then h_1 would be the p-th power of another polynomial; hence it was not irreducible. This finishes the solution.

b) Arguing indirectly, assume that both $\Phi_m(x)$ and $\Phi_n(x)$ are divisible by some non-constant polynomial $g(x)$ in $\mathbb{Z}_p[x]$. From the factorization of $x^{mn}-1$ into a product of cyclotomic polynomials, we obtain $g(x)^2 \mid x^{mn}-1$ (surely, in $\mathbb{Z}_p[x]$). Part a) now yields that the polynomial $x^{mn}-1$ is not coprime with its derivative mnx^{mn-1} in $\mathbb{Z}_p[x]$, which is obviously wrong, as $p \nmid mn$ and $x \nmid x^{mn}-1$.

1 Divisors of polynomial values, with applications

1.1. a) It suffices to put all coefficients, except for the last one, to be divisible by the product $m_1m_2\cdots m_n$, and set the last coefficient to be 1.

b) Follows from $f(n) \mid f(n)g(n)$.

c) It follows from the fact that the set of values of $f(g)$ at integer points is a subset of the set of values of f at integer points.

1.2. Assume the contrary: let $P(f)$ consist of k primes, i.e. $P(f) = \{p_1, p_2, \ldots, p_k\}$. Take $a \in \mathbb{Z}$ for which $f(a) = b \neq 0$. We define the polynomial g by the equality $g(x) = \frac{f(a+bpx)}{b}$, where $p = p_1p_2\cdots p_k$. It is easy to see that g is a non-constant polynomial with integer coefficients, and $P(g) \subset P(f)$. The constant term $g(0) = 1$, and all other coefficients of the polynomial g are divisible by p, therefore, none of the numbers $p_1, p_2, \ldots, p_k$ can lie in the set $P(g)$. But then the set $P(g)$ is empty, which is a contradiction. (Note that the above argument generalizes Euclid's proof of the infinity of the set of primes.)

1.3. By the theorem on a linear representation of the g.c.d., there exist polynomials $u_1, u_2, \ldots, u_k \in \mathbb{Q}[x]$ such that

$$u_1f_1 + u_2f_2 + \cdots + u_kf_k = 1.$$

If we multiply the polynomials $u_1, \ldots, u_k$ by m that is the l.c.m. of the denominators of all nonzero coefficients $u_1, \ldots, u_k$, we get the polynomials $v_1, v_2, \ldots, v_k \in \mathbb{Z}[x]$. Multiplying

the equality $u_1f_1 + u_2f_2 + \cdots + u_kf_k = 1$ by m, we get $v_1f_1 + v_2f_2 + \cdots + v_kf_k = m$. We see that if for some n the numbers $f_1(n), f_2(n), \ldots, f_k(n)$ are divisible by s, then m is also divisible by s. This implies that the set $D(f_1, f_2, \ldots, f_k)$ can contain only divisors of the number m, and hence it is finite.

1.4. $f(n)$ is divisible by m_i for all n from some arithmetic progression with step m_i. Since $\gcd(m_1, m_2) = 1$, by the Chinese remainders theorem, progressions with steps m_1 and m_2 intersect. Then n from this intersection satisfies $m_1m_2 \mid f(n)$.

1.5. a) -1 is a quadratic residue modulo p of the form $4k + 1$ and non-quadratic residue modulo p of the form $4k + 3$ (e.g., it follows from Euler's criteria). This means that all primes of the form $4k+1$ are in $P(f)$, while all primes of the form $4k+3$ are outside $P(f)$. Moreover, obviously, $2 \in P(f)$.

c) $f(1) = p$, hence $p \in P(f)$.

Let $f(n)$ be divisible by a prime $q \neq p$. Since $x^p - 1$ is divisible by f (in $\mathbb{Z}[x]$), then $n^p \equiv 1 \pmod q$, hence $\mathrm{ord}_p(n)$ equals 1 or p, since it divides p.

In the first case $n \equiv 1 \pmod q$, it follows $f(n) = n^{p-1}+n^{p-2}+\cdots+n+1 \equiv p \pmod q$. We have $p \equiv 0 \pmod q$, откуда $p = q$ — a contradiction.

In the second case $q - 1$ divides $\mathrm{ord}_p(n) = p$, i.e., $q \equiv 1 \pmod p$.

Conversely, let prime $q \equiv 1 \pmod p$. Let a be a primitive root modulo q, and let $n = a^{\frac{q-1}{p}}$. Therefore, $n \not\equiv 1 \pmod q$, but $n^p \equiv 1 \pmod q$, hence $f(n) = \dfrac{n^p - 1}{n - 1}$ is divisible by q.

Thus $P(f)$ consists of all primes of the form $pk + 1$, and p.

1.6. a) If $f_k(x) = kx - 1$ for some positive integer k, then $P(f_k)$ coincides with the set of all primes, except divisors of k. Threrfore, it is clear that for $f(x) = (2x - 1)(3x - 1)$ the set $P(f)$ coincides with the set of all primes.

b) It does not follow. For each prime p and integers t, s at least one of numbers t, s, ts is either zero residue, or a quadratic residue modulo p. Hence, for the polynomial

$$f_{t,s}(x) = (x^2 - t)(x^2 - s)(x^2 - ts)$$

we have $p \in P(f_{t,s})$. It suffises to take t, s such that t, s, ts are not perfect squares.

1.7. a) Let us show by induction on α, that there exists an integer n_α such that $p^\alpha \mid f(n_\alpha)$.

For $\alpha = 1$ the statement follows from $p \in P(f)$. Assume that the statement is proved for some $\alpha \in \mathbb{N}$, and $f(n_\alpha) = p^\alpha m$ for some $m \in \mathbb{Z}$. By Hensel's lemma,

$$f(n_\alpha + p^\alpha z) \equiv p^\alpha(m + zf'(n_\alpha)) \pmod{p^{\alpha+1}}.$$

Since $p \notin P(f, f')$, $f'(n_\alpha)$ is not divisible by p, hence it suffices to choose $z = z_0$ so that $m + z_0f'(n_\alpha)$ is divisible by p, and set $n_{\alpha+1} = n_\alpha + p^\alpha z_0$.

b) Take n_α from a). Then $f(n_\alpha + p^\alpha)$ is divisible by p^α, and $f'(n_\alpha)$ is not divisible by p. Thus from Hensel's lemma it follows that $v_p(f(n_\alpha + p^\alpha) - f(n_\alpha)) = \alpha$. Hence either $v_p(f(n_\alpha))$, or $v_p(f(n_\alpha + p^\alpha))$ is equal to α.

1.8. The converse is not true. Let us prove the existence of such polynomial without rational roots. Take $f_{t,s}$ from the solution of problems 1.6, where t, s and ts are not perfect squares. Assume that an odd prime p is a divisor of neither of s and t. Then $p \notin P(h, h')$ for each of the polynomials $h(x) = x^2 - a$ where a is equal to t, s or ts. Then, according to the problem 1.7, $p^\alpha \in D(f_{t,s})$ for arbitrarily large α.

For a finite set of prime divisors q of the numbers t and s take t', s' not divisible by any such primes q and such that t', s', $t's'$ are not perfect squares. Then $q^\alpha \in D(f_{t',s'})$ for arbitrarily large α.

Finally, for $g(x) = x^2 + x + 2$, according to the problem 1.7, $2^\alpha \in D(g)$ for arbitrarily large α.

By problem 1.4, $f = f_{t,s} f_{t',s'} g$ is a required polynomial such that $D(f) = \mathbb{N}$.

Remark. In fact, a required polynomial can be found just in the form $f_{t,s}$ for an appropriate choice of t and s.

1.9. b) Let $f = a h_1^{\alpha_1} \cdots h_t^{\alpha_t}$, where $a \in \mathbb{Z}$, and $h_1, \dots h_t$ are pairwise non-proportional primitive irreducible polynomials with integer coefficients.

Since $\gcd(h_1, h_1') = 1$, by problems 1.2, 1.3, the set

$$P_1(h_1) \setminus (P(h_1, h_1') \cup P(h_1, a) \cup P(h_1, h_2) \cup \cdots \cup P(h_1, h_t))$$

is infinite; take some p_1 from this set, and by problem 1.7, there exists n_1 such that $v_{p_1}(h_1(n_1)) = 1$. By the choice of p_1, for all m from progression $n_1 + k p_1^2$ we have $v_{p_1}(h_1(m)) = 1$, while $a, h_2(m), \dots, h_t(m)$ are not divisible by p_1. Therefore, for all m from progression $n_1 + k p_1^2$ we have $v_{p_1}(f(m)) = \alpha_1$.

Similarly, we define p_i, $i = 2, \dots, t$ and the corresponding progressions. By the Chinese remainders theorem, all t progressions intersect. Let m belong to all progressions. Then, on one hand, by assumption, $f(m) = u^s$, for some integers u and $s > 1$. On the other hand, $v_{p_i}(f(m)) = \alpha_i$, $i = 1, \dots, t$, therefore all α_i are multiples of s, thus $f = a r^s$, where $r \in \mathbb{Z}[x]$. Since $f(m) = u^s = a r(m)^s$, the constant a is a perfect s-th power. Finally, we represent f in the required form $f = q^s$.

Remark. The condition of the problem can be weakened by requiring that the values of f be perfect powers only on some infinite arithmetic progression A. In the solution when choosing p_i then we also require that p_i is not a divisor of the step of A. Then our progressions with steps p_i^2 intersect with the progression A.

1.10. The problem follows directly from the next one (using problem 1.5a). But we will also provide a direct solution.

We will prove the existence of *one* prime $p = 4k + 1 \in P(f)$; the proof that there are infinitely many such primes can now be obtained in the same way as in problem 1.2.

Let $\deg f = n$. Consider the polynomial $f(x + i)$, where i is the imaginary unit. It is represented as $f(x + i) = P_1(x) + i P_2(x)$, where $P_1(x), P_2(x) \in \mathbb{Z}[x]$, and $\deg P_1 = n$, $\deg P_2 = n - 1 \geqslant 0$. Hence, there exists $k \in \mathbb{Z}$ such that the numbers $a = P_1(k)$ and

$b = P_2(k)$ are nonzero, and $|P_1(k)| > |P_2(k)|$. Replacing $P(x)$ with $P(x+k)$, we can assume that $f(i) = a + bi$, where $|a| > |b| > 0$; then $f(-i) = a - bi$.

Let $d = \gcd(a, b)$, $a = a'd$, $b = b'd$; hence $|a'| \geqslant |a|/|b| > 1$. The number $a'^2 + b'^2$ is greater than 2 and is not divisible by 4; hence it has an odd prime divisor p. Since a' and b' are coprime, $p = 4k + 1$.

Let us set $Q(x) = f(x) - a - bx$. The values of Q at $\pm i$ both equal zero, hence Q is divisible by $(x - i)(x + i) = x^2 + 1$. Since $x^2 + 1$ have the leading coefficient 1, we have $f(x) = a + bx + (x^2 + 1)R(x)$ for some $R(x) \in \mathbb{Z}[x]$.

Now let n be such that $nb' \equiv -a' \pmod{p}$. Hence $a + bn = d(a' + b'n)$ is divisible by p and $b'^2(n^2 + 1) = (b'n)^2 + b'^2 \equiv a'^2 + b'^2 \equiv 0 \pmod{p}$; since b' is not divisible by p, we have $p \mid n^2 + 1$. Therefore, $f(n) = (a + bn) + (n^2 + 1)R(n)$ is also divisible by p.

1.11. We will prove the more general statement b).

If is clear that it suffices to consider the case of irreducible over $\mathbb{Z}$ polynomials f_i (for reducible polynomials it suffices to apply the statement for some of their irreducible divisors).

Let α_i be a root of f_i, for $i = 1, 2, \ldots, k$. By the Primitive element theorem, there exists an algebraic number γ such that $\mathbb{Q}[\alpha_1, \alpha_2, \ldots, \alpha_k] = \mathbb{Q}[\gamma]$. In particular, there exist polynomials $A_i \in \mathbb{Q}[x]$ such that $\alpha_i = A_i(\gamma)$.

Let g be the minimal polynomial of γ. Note that $f_i(A_i(\gamma)) = 0$, so that $f_i(A_i(x))$ is divisible by g for all $i = 1, 2, \ldots, k$, i.e.,

$$f_i(A_i(x)) = g(x)h_i(x).$$

Coefficients of polynomials in the above equalities can be non=integers (but they are rationals); let N be the maximal prime which divides at least one denominator of a coefficient.

By Problem 1.2, there exist infinitely many primes in $P(g)$. Let $p \in P(g)$ be a prime such that $p > N$, and let $p \mid g(n)$. Then the numerators of rationals $f_i(A_i(n)) = g(n)h_i(n)$ are divisible by p, since the denominators of $P_i(n)$ and $Q_i(n)$ are not divisible by p.

The only remaining trouble is that the numbers $A_i(n)$ are rational numbers, but not necessarily integers. However, their denominators are also not divisible by p. Hence if $A_i(n) = k_i/\ell_i$ for coprime integers k_i and ℓ_i, then one can take m_i, such that $k_i \equiv \ell_i m_i \pmod{p}$. Therefore, $f_i(m_i) \equiv f_i(k_i/\ell_i) \equiv 0 \pmod{p}$. Hence $p \in P(f_i)$ for all $i = 1, 2, \ldots, k$.

1.12. If $x \mid f$, then $D(f) = \mathbb{N}$, and the claim is obvious. Otherwise, let $b \neq 0$ be the constant term; replacing f with $f(bx)/b \in \mathbb{Z}[x]$ we may assume that $b = 1$. Without loss of generality, f is irreducible, and its leading coefficient is positive. As in problem 1.10, it suffices to show that there exists at least one prime $p \equiv 3 \pmod{4}$, $p \in P(f)$.

a) Assume that $\deg f$ is odd. Consider a large *negative* integer $-n$ divisible by 4. Then $f(-n) < 0$ and $f(-n) \equiv f(0) \equiv 1 \pmod{4}$, so $f(-n) = -(4k + 3)$ for some positive integer k. Then the prime decomposition of $4k + 3$ must contain a desired prime $p \equiv 3 \pmod{4}$.

b) If $D(f)$ contains a positive integer congruent to 3 modulo 4, one may apply the same reasoning as above. Otherwise, since f is irreducible, all its roots are simple. As it has a real root, there exists an interval (α, β) on which f attains only negative values.

Choose now a rational number $\frac{a}{b} \in (\alpha, \beta)$ (here a and b are coprime) such that b has no prime divisors of the form $4k+3$, while $4 \mid a$ (one may even choose $b = 5^N$ for an appropriate N). Recall that $f(a) \equiv 1 \pmod 4$. Moreover, $f(a) > 0$, otherwise $-f(a)$ is positive integer of the form $4k+3$, and the same reasoning as in the part a) works. Then $f\left(\frac{a}{b}\right) = -\frac{c}{d}$, where $d = b^n \equiv 1 \pmod 4$, and the positive integer c satisfies

$$c = -b^n f\left(\frac{a}{b}\right) \equiv -f(a) \equiv 3 \pmod 4.$$

Therefore, there exists a prime $p \mid c$ such that $p \equiv 3 \pmod 4$. By our assumption, $p \nmid b$; so there exist $a' \in \mathbb{Z}$ such that $a \equiv ba' \pmod p$. Then we have $b^n f(a') \equiv b^n f\left(\frac{a}{b}\right) = -c \equiv 0 \pmod p$, and the desired p has been found.

1.13. Solution 1. Assume the contrary, so that $\Phi_m(x)$ and $\Phi_n(x)$ are divisible by $x - a$ in $\mathbb{Z}_p[x]$, which contradicts the problem 0.17b.

1.13. Solution 2. Assume that $\Phi_m(k)$ and $\Phi_n(k)$ are divisible by p. Then $k^m - 1$ and $k^n - 1$ are divisible by p. Let $m < n$. Then $x^{mn} - 1$ equals $(x^m - 1)\Phi_n(x)h(x)$, where $h \in \mathbb{Z}$. Inserting k, we obtain that $v_p(k^{mn} - 1) > v_p(k^m - 1)$. But since n is not divisible by p, this contradicts LTE-lemma for $a = k^m$ and $b = 1$.

1.14. Immediately follows from the problem 0.14, since $2 \in P(f)$ iff at least one of numbers $f(0)$, $f(1)$ is even.

1.15. a) Assume that $\Phi_n(m)$ is divisible by a prime p. Then $m^n \equiv 1 \pmod p$. Let $d = \mathrm{ord}_p(m)$, then $d \mid n$ and $d \mid p - 1$.

If $d = n$, then $n \mid p - 1$ and $p \equiv 1 \pmod n$.

Otherwise $d < n$, and in $\mathbb{Z}[x]$ we have равенство $x^n - 1 = (x^d - 1) \cdot \Phi_n \cdot f$ for some $f \in \mathbb{Z}[x]$. Hence $m^n - 1 = (m^d - 1) \cdot \Phi_n(m) \cdot f(m)$, where $p \mid m^d - 1$ и $p \mid \Phi_n(m)$. Therefore,

$$v_p(m^n - 1) > v_p(m^d - 1).$$

On the other hand, applying LTE-lemma for $a = m^d$ and $b = 1$, we have

$$v_p(m^n - 1) - v_p(m^d - 1) = v_p(n/d).$$

It follows $p \mid (n/d)$, hence $p \mid n$.

b) Follows from a) and problem 1.2.

1.16. a) Let $k = v_p(m^d - 1)$. Then for any integer a we have:

• if $d \nmid a$, then $p \nmid m^a - 1$ (follows from properties of order modulo p);

• if $d \mid a$, then $v_p(m^a - 1) = k + v_p(a/d)$ follows from LTE-lemma).

Hence $n_i = dp^i$ is the minimal number n satisfying $p^{k+i} \mid m^n - 1$.

Let us derive from decomposition of $x^n - 1$ into cyclotomic polynomials the following formula:

$$\Phi_n = \frac{x^n - 1}{\operatorname{lcm}\{x^d - 1 \colon d \mid n,\ d < n\}}.$$

Indeed, the denominator is a product of distinct polynomials Φ_k for some $k \mid n$, so that the quotient in the RHS is a polynomial. Moreover, the polynomial Φ_n divides the numerator, but does not divide the denominator, and any Φ_d with $d \mid n$, $d < n$, divides the denominator, since $\Phi_d \mid x^d - 1$. Hence, after cancellation we obtain Φ_n.

Insert $x = m$ and $n = n_i$ into the formula, we obtain that the numerator is divisible by p^{k+i}, while the denominotor is divisible by a smaller power of p. Therefore, $p \mid \Phi_{n_i}(m)$.

Note. In fact, in the condition we list *all* cyclomatic polynomials whose values at m are divisible by p. It easily follows from the solutoin of the next item.

b) By problem 1.15a, $P(\Phi_n)$ consists of (1) primes of the form $p = an+1$, and (2) prime divisors of n.

All primes of the form (1) do belong to $P(\Phi_n)$. Indeed, let $p = an + 1$; let us take a primitive root ξ modulo p. Hence $\operatorname{ord}_p(\xi^a) = n$, therefore, for $m = \xi^a$ we have $p \mid m^n - 1$, but $p \nmid m^d - 1$ for all $d < n$; in particular, $p \nmid \Phi_d(m)$ for $d \mid n$. Hence $p \mid \Phi_n(m)$ and, therefore, $p \in P(\Phi_n)$.

For primes of the form (2), the situation is different. Assume that $p \mid n$ and $p \in P(\Phi_n)$: let $p \mid \Phi_n(m)$. Let $d = \operatorname{ord}_p(m)$; since $p \mid \Phi_n(m) \mid m^n - 1$, we have $d \mid n$. On the other hand, $d \mid p - 1$, so that $d \mid \gcd(n, p - 1)$.

Let $j = v_p(n)$. Then the polynomial $\Phi_d \cdot \Phi_{dp} \cdot \ldots \cdot \Phi_{dp^j}$ divides Φ_n, i.e.,

$$x^n - 1 = \Phi_d \cdot \Phi_{dp} \cdot \ldots \cdot \Phi_{dp^j} \cdot f,$$

where $f \in \mathbb{Z}[x]$. Recall that $p^k \mid \Phi_d(m)$ and $p \mid \Phi_{dp^i}(m)$ for all $i = 1, 2, \ldots, j$ (as in item a), $k = v_p(m^d - 1)$). Hence

$$v_p(m^n - 1) \geqslant k + j + v_p(f(m)).$$

On the other hand, $v_p(m^n - 1) = k + j$ by LTE-lemma. Therefore, $p \nmid f(m)$.

Let $k = n/p^j$. If $k \nmid p-1$, then $k \neq d$ (and $d \mid k$). In this case we have $\Phi_n \mid f$, and hence $p \nmid \Phi_n(m)$, since $p \nmid f(m)$, which is not true.

Assume that conversly, $k \mid p - 1$. Hence, as above, there exists $m \in \mathbb{Z}$ such that $p \nmid m$ and $\operatorname{ord}_p(m) = k$. Then, by a), we have $p \mid \Phi_n(m)$, i.e., $p \in P(\Phi_n)$.

Thus $p \in P(\Phi_n)$ iff $n/p^j \mid p - 1$. Note that in this case p is the greatest prime divisor of n.

Finally, the answer is the following. $P(\Phi_n)$ consists of all primes p such that

• either $p \equiv 1 \pmod{n}$;

• or p is the greatest prome divisor of n, and $n/p^{v_p(n)} \mid p - 1$.

2 On a problem of V.A. Senderov

2.1. Write $Q(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0$; then $Q(x)^k$ has the form

$$Q(x)^k = b_{kn}x^{kn} + b_{kn-1}x^{kn-1} + \ldots + b_0.$$

We prove by induction on $n-i$ that all the coefficients a_i are rational. The learing coefficient a_n is rational by problem conditions. To perform the step, suppose now that the coefficients $a_n, a_{n-1}, \ldots, a_{n-s}$ are all rational; we need to prove that $a_{n-s-1} \in \mathbb{Q}$ as well. For that purpose, take the desired equality

$$b_{kn}x^{kn} + b_{kn-1}x^{kn-1} + \ldots + b_0 = (a_n x^n + a_{n-1}x^{n-1} + \ldots + a_0)^k$$

and compare the coefficients of x^{kn-s-1} on both sides:

$$b_{kn-s-1} = a_{n-s-1}a_n^{k-1} + S,$$

where $S = S(a_n, a_{n-1}, \ldots, a_{n-s})$ is a value of some polynomial with rational coefficients at rational point $(a_n, a_{n-1}, \ldots, a_{n-s})$, hence a rational number. This yields that the coefficient $a_{n-s-1} = \frac{b_{n-s-1}-S}{a_n^{k-1}}$ is rational, as desired. So, all coefficients of Q are rational.

Now represent Q in the fore $\dfrac{a}{b}R$, where a and b are coprime positive integers, and R is a primitive polynomial with integer coefficients. Hence, $Q^k = \dfrac{a^k}{b^k}R^k$. By Gauss' lemma, R^k is primitive. Therefore, if $b \neq 1$, then not all coefficients of Q^k are integers.

The other version of completing after the proof that all the coefficients of Q are rational, is the following.

Represent now the polynomial $Q(x)^k$ whose coefficients are integer as a product of two polynomials $Q(x), Q(x)^{k-1} \in \mathbb{Q}[x]$. By Gauss' lemma, there exists a rational q such that the polynomials $qQ(x)$ and $q^{-1}Q(x)^{k-1}$have integer coefficients. Write $q = a/b$ where a, b are coprime integers. Then the polynomials $aQ(x), bQ(x)^{k-1}$ also lie in $\mathbb{Z}[x]$. Therefore, we have $a^{k-1}Q(x)^{k-1} \in \mathbb{Z}[x]$. Since a^{k-1} and b are coprime, there exist integers s, t such that $a^{k-1}s + bt = (a, b) = 1$. Thus the polynomial $a^{k-1}sQ(x)^{k-1} + bsQ(x)^{k-1} = Q(x)^{k-1}$ has integer coefficients.

Proceeding in the same way, we eventually decrease the exponent to 1 thus proving that Q has integer coefficients.

2.2. Let

$$P(x) = b_k^2 x^{2k} + a_{2k-1}x^{2k-1} + \ldots + a_0.$$

be the given polynomial ($b_k > 0$). We will rewrite it in the form

$$P(x) = Q(x)^2 + r(x) = (b_k x^k + b_{k-1}x^{k-1} + \ldots + b_0)^2 + r(x),$$

where $\deg r(x) \leqslant k-1$. To show this is possible, compare the coefficients of x^{t+k} for $t = 0, 1, \ldots, k-1$ on both sides: $a_{k+t} = 2b_k b_t + \sum_{i=1}^{k-1-t} b_{t+i}b_{k-1}$. It is easy to see that the

coefficients $b_{k-1}, b_{k-2}, \ldots, b_1, b_0$ can be uniquely determined via this system of equations. Moreover, all the b_i will be rational. Denote by M the LCM of the denominators of those coeggicients.

By the problem conditions, for every large enough positive integer n we have $P(n) = y_n^2$, where $y_n \in \mathbb{Z}$. Multiplying by M^2 we get the relation $(My_n)^2 = Q_1(n)^2 + M^2 r(n)$, where $Q_1(x) = MQ(x) \in \mathbb{Z}[x]$. If the leading coefficient in r is positive, then for all large enough n we have $(My_n)^2 > Q_1(n)^2$, whence $(My_n)^2 \geqslant (1 + Q_1(n))^2$. Similarly, if the leading coefficient in r is negative, then $(My_n)^2 \leqslant (-1 + Q_1(n))^2$. In both cases, the inequality $2|Q_1(n)| \leqslant |M^2 r(n) - 1|$ holds for all large enoung positive integers n, which cannot hold since $\deg Q_1 > \deg r$.

It follows that $r(x)$ vanishes identically, so that $P(x) = Q(x)^2$. It remains to show that the coefficients of Q are all integers; this dollows from problem 2.1.

2.3. In this problem we do not have additional restrictions as in 2.2; to work this out, we apply the following interesting trick. It is clear that there exists an integer ℓ such that the polynomials $P(x)$ and $P(x + \ell)$ share no common roots (and hence are coprime). Now the polynomial $H(x) = P(x) \cdot P(x + \ell)$ already has an even degree, and its leading coefficient is a perfect square. Also, the values of R at all large enoung positive integers are perfect squares.

By problem 2.2, there exists a polynomial $P_1(x) \in \mathbb{Z}[x]$ such that $P(x) \cdot P(x+\ell) = P_1(x)^2$. Consider its canonical factorization in $\mathbb{Z}[x]$:

$$P_1 = uh_1 h_2 \ldots h_k,$$

where $u \in \mathbb{Z}$, and the h_i are primitive irreducible polynomials. From coprimality of $P(x)$ and $P(x + \ell)$, taking into account Gauss' lemma, it follows that, say, $P(x)$ is a product of some integer u_1 and squares of some of the h_i. Since the value of P at some integer point is a nonzero square, the number u_1 is also a perfect square. Therefore, $P(x)$ is a square of a polynomial with integer coefficients, as desired.

Note that one can solve this problem in another way, repeating the solution of the problem 1.9.

2.4. Notice that each interval of the form (r_i, r_{i+1}) contains a root of the derivative $R'(x) = Q'(x)$; this way, we have found $l - 1$ distinct roots, so these are all the roots of P'. A similar argument applies to the roots of S. Hence, for each $i < l$, the segments $[r_i, r_{i+1}]$ and $[s_i, s_{i+1}]$ share a common point, namely the ith smallest root of $Q'(x)$.

Moreover, if a segment $[r_i, r_{i+1}]$ contains a root of S, then it contains at least two such roots; otherwise the graph of the function $y = S(x)$ would be tangent to $y = 0$, and hence $S(x)$ would have a multiple root, which is not the case. A similar fact holds for a segment between consecutive roots of S. Therefore, if, say, $s_i \in [r_i, r_{i+1}]$, then s_{i+1} also lies on $[r_i, r_{i+1}]$ (in this case point s_{i-1} cannot lie on $[r_i, r_{i+1}]$, as otherwise $[r_{i-1}, r_i]$ would have no common points with $[s_{i-1}, s_i]$). Hence, in any case one of the segments $[r_i, r_{i+1}]$ and $[s_i, s_{i+1}]$ contains the other.

Assume that l is even. Then r_1 is the smallest among all the roots, while r_l is the largest one. Now the arguments above determine the mutual positions of the roots as

$$r_1 < s_1 < s_2 < r_2 < r_3 < s_3 < \ldots < r_{l-1} < s_{l-1} < s_l < r_l.$$

If l is odd, similar arguments lead to the following answer:

$$s_1 < r_1 < r_2 < s_2 < s_3 < r_3 < \ldots < r_{l-1} < s_{l-1} < s_l < r_l.$$

2.5. We will even find all pairs of a positive integger k and an integer c such that

$$P_k(x) + c = Q(x)^2.$$

Notice that c is a square of a positive integer $b = \pm Q(0)$ (since, obviously, $c \neq 0$). Rewrite our equation as

$$x(x+1)\ldots(x+k-1) = Q(x)^2 - b^2 = (Q(x)-b)(Q(x)+b).$$

Without loss of generality, we assume that Q is monic. Notice that $k = 2\deg Q$ is even, and the coefficient of x^{k-1} in $Q(x)^2 - b^2$ should be even as well. This latter equals $0 + 1 + \ldots + (k-1) = k(k-1)/2$; Thus, since k is even, we arrive at $4 \mid k$.

It is easy to see that the polynomials $Q(x) - b$ and $Q(x) + b$ have exactly $l = k/2$ distinct real roots each, and the union of their sets of roots is $\{0, -1, \ldots, -k+1\}$. By problem 2.4, tje roots of $Q(x) - b$ are $1-k, 4-k, \ldots, -3, 0$, while the roots of $Q(x) + b$ are $2-k, 3-k, \ldots, -2, -1$. If $k > 4$, then $\deg(Q(x) \pm b) > 2$, and by the Vieta theorem the sums of the roots of both polynomials must coincide, as well as the sums of pairwise products of the roots. Hence the sums of squares of the roots also must coincide, i.e.,

$$0^2 + 3^2 + \ldots + (k-4)^2 + (k-1)^2 = 1^2 + 2^2 + \ldots + (k-3)^2 + (k-2)^2.$$

But this equality cannot hold, as

$$(t-4)^2 + (t-1)^2 = 2t^2 - 10t + 17 > 2t^2 - 10t + 13 = (t-3)^2 + (t-2)^2$$

for every t.

Consequently, $k = 4$, and $Q(x) - b = x(x+3)$, $Q(x) + b = (x+1)(x+2)$. Therefore, $b = 1$ and $c = b^2 = 1$. So the pair $(k, c) = (4, 1)$ is the unique solution.

2.6. The structure of polynomial $P_k(x)$ yields that the derivative $P_k'(x)$ has exactly $k-1$ roots, and those roots can be enumerated as $r_1, \ldots, r_{k-1}$ so that

$$-(k-1) < r_{k-1} < -(k-2) < r_{k-2)} < \ldots < -1 < r_1 < 0.$$

Moreover, the graph of the function $y = |P_k(x)|$ is symmetric in the line $x = -\frac{k-1}{2}$, so $|P_k(r_i)| = |P_k(r_{k-i})|$ for $1 \leqslant i < k$. The properties of derivaticve yield that $|P_k(x)|$ attains its maximum value on the segment $[-i, -i+1]$ at point r_i. THerefore,

$$\frac{|P_k(r_{i-1})|}{|P_k(r_i)|} \geqslant \frac{|P_k(r_i+1)|}{|P_k(r_i)|} = \frac{|r_i+1|\cdot|r_i+2|\ldots|r_i+k|}{|r_i|\cdot|r_i+1|\ldots|r_i+k-1|} = \frac{|r_i+k|}{|r_i|},$$

so for every $i \leqslant \frac{k}{2}$ inequality $|P_k(r_{i-1})| > |P_k(r_i)|$ holds. By symmetry, for $i \geqslant \frac{k+2}{2}$ the converse inequality $|P_k(r_{i-1})| < |P_k(r_i)|$ holds.

THus, for every complex a at most two roots of equation $P_k(x) = a$ belong to the set $\{r_1, \ldots, r_{m-1}\}$ of roots of $P_k'(x)$. Moreover, if k is odd, then $P_k(r_i) = -P_k(r_{k-i})$, so even at most one of the roots is a root of P_k'. This yields the desired statement, as all the roots of P_k' are simple.

2.7. Notice that $P_k'(x) = R'(Q(x)) \cdot Q'(x)$.

Let r be a complex root of $R'(x)$. Then r is a common root of $R'(x)$ and $R(x) - R(r)$, hence $x - r \mid \gcd(R'(x), R(x) - R(r))$. Substituting $Q(x)$ in place of x, we obtain $Q(x) - r \mid \gcd(R'(Q(x)), R(Q(x)) - R(r))$. Finally, since $R'(Q(x)) \mid P_k'(x)$, it follows that $Q(x) - r \mid \gcd(P_k'(x), P_k(x) - R(r))$.

Problem 2.6 yields now that the degree of $Q(x) - r$ (coinciding with that of $Q(x)$) equals 2, and in this case k must be even. This is exactly what we aimed to prove.

2.8. Solution 1. Due to problem 1.9, we have

$$P_k(x) + c = x(x+1)\ldots(x+k-1) + c = Q(x)^s \qquad (*)$$

for some integer $s \geqslant 2$ and some polynomial Q with complex coefficients. Let a be the leading coefficient of Q; then, since $a^s = 1$, one may replace Q by $\frac{1}{a}Q$ not affecting equality $(*)$. Thus we assume that Q is monic, and by problem 2.1, we in fact have $Q \in \mathbb{Z}[x]$. Without loss of generality, we assume that Q is not a non-trivial power of a different polynomial, otherwise we would replace s with a larger number,

Notice that

$$P_k'(x) = (P_k(x) + c)' = (Q(x)^s)' = Q'(x) \cdot Q(x)^{s-1}.$$

Hence, Q^{s-1} divides $\gcd(P_k + c, P_k')$. But, by problem 2.7, the degree of that g.c.d. does not exceed 2. Therefore, the only possible cases are (1) $s = 3$, $\deg Q = 1$; (2) $s = 2$, $\deg Q = 1$; and (3) $s = 2$, $\deg Q = 2$.

In case (1) we get that $k = 3$ is odd; but in this case, the degree of the g.c.d. should not exceed 1, thus this case is impossible.

In case (2) we have $x(x+1) + c = (x+a)^2$, whence $a = 1/2$, so that $Q \notin \mathbb{Z}[x]$.

In case (3) we have $x(x+1)(x+2)(x+3) + c = (x^2 + ax + b)^2$; comparing the coefficients of x^3 and x^2, we obtain $a = 3$, $b = 1$; therefore, $c = 1$, and we arrive at the unique answer $(k, c) = (4, 1)$.

2.8. Solution 2. Again, we start with equation $(*)$. where $Q \in \mathbb{Z}[x]$. Plugging $x = 0$, we get $c = Q(0)^s = b^s$. Therefore, we have

$$x(x+1)\ldots(x+k-1) = Q(x)^s - b^s.$$

Consequently, $Q(-j)^s = b^s$ for all $j = 0, 1, \ldots, k-1$. If s is odd, the polynomial $Q(x) - b$ has at least k distinct roots, namely $0, -1, \ldots, -k+1$, and hence $\deg Q \geqslant k$. But then $\deg Q^s \geqslant sk > k = \deg(P_k + c)$, which is impossible.

Assume now that s is even. Then $P_k + c$ is a square of a different polynomial; this situation is completely investigated in problem 2.5. So we arrive at the same answer.

2.9. Denote

$$f(x) = x^n + x^{n-1} + \ldots + 1 = \frac{x^{n+1} - 1}{x - 1}.$$

Let α be any complex root of $g'(x)$. As in the solution of 2.7, we obtain

$$h(x) - \alpha \mid \gcd(f'(x), f(x) - g(\alpha)).$$

Therefore, $\deg \gcd(f'(x), f(x) - g(\alpha)) \geqslant 2$.

It follows that there exist at least two (possibly equal) roots r, s of polynomial

$$f'(x) = \frac{nx^{n+1} - (n+1)x^n + 1}{(x-1)^2},$$

such that $f(r) = f(s)$. It is easy to notice that 1 is not a root of f', and that f' has no multiple roots, so that $r \neq s$.

Now the formula for f' yields

$$n(s^{n+1} - 1) = (n+1)(s^n - 1) \quad \text{and} \quad n(r^{n+1} - 1) = (n+1)(r^n - 1).$$

Further, from $f(r) = f(s)$ we get

$$\frac{s^{n+1} - 1}{s - 1} = \frac{r^{n+1} - 1}{r - 1}.$$

The previous relations now give us

$$\frac{s^n - 1}{s - 1} = \frac{r^n - 1}{r - 1}.$$

Subtracting this equality from the previous one, we obtain $s^n = r^n$, whence $s - 1 = r - 1$, i.e., $s = r$, which is impossible. Thus, no value of n satisfies the problem requirements.

3 Miscellaneous

3.1. a) Let us divide f by g with remainder: $f = qg + r$, where $q, r \in \mathbb{Z}[x]$, $\deg r < \deg g$. There exists an integer N such that for all $n > N$ we have $|r(n)| < |g(n)|$. Thus, if $n > N$ satisfies $g(n) \mid f(n)$, then $r(n) = 0$. We get that $r(n) = 0$ for infinitely many values of n, so r is the zero polynomial.

b) After dividing f by g with a remainder in $\mathbb{Q}[x]$, we have $f = \frac{qg}{m} + r$, where $r \in \mathbb{Q}[x]$, $\deg r < \deg g$, $q \in \mathbb{Z}[x]$, $m \in \mathbb{N}$. Then there exists an integer N such that $|r(n)| < |g(n)|/m$ for all $n > N$, and if $n > N$ is such that $g(n) \mid f(n)$, then $r(n) = 0$. We get that $r(n) = 0$ for infinitely many values of n, so r is the zero polynomial.

Further, assume that $g(n) \mid f(n)$ for some $n \in \mathbb{N}$, i.e., $m \mid q(n)$. Then $m \mid q(n + mt)$ for any integer t, and hence $g(n + mt) \mid f(n + mt)$.

3.2. Assume the contrary; then for each $i = 1, 2, \ldots, m$ there exists an integer k_i such that $f(k_i)$ is not divisible by $p_i^{\alpha_i}$, where p_i is a prime, and $p_i^{\alpha_i}$ is a divisor of a_i. If $p_i = p_j$ and $\alpha_i \leqslant \alpha_j$, then one may redefine α_j and k_j as $\alpha_j = \alpha_i$ and $k_j = k_i$. All such changes having been made, we assume that equal primes p_i correspond to equal numbers α_i and k_i. By the Chinese remainders theorem, there exists an integer k in the intersection of progressions of the form $k_i + p_i^{\alpha_i} t$. Then $f(k)$ is not divisible by any of $p_i^{\alpha_i}$, hence is not divisible by any of a_i. A contradiction.

3.3. a) Let f be a polynomial determining the given function. Divide it with remainder by the polynomial $x(x-1)\cdots(x-(n-1))$:

$$f = x(x-1)\cdots(x-(n-1))g + r,$$

where $q, r \in \mathbb{Z}[x]$, $\deg r < n$. Then f and r determine the same function $\mathbb{Z}_n \to \mathbb{Z}_n$.

b) Answer: all prime n (and $n = 1$).

If $n = p$ is prime, for any collection of required values $f(0), f(1), \ldots, f(p-1)$ write down Lagrange's interpolation formula. THis formula provides a polynomial in $\mathbb{Q}[x]$ attaining prescribed values, and the denominators of its coefficients are not divisible by p, so their resifues are invertible modulo p. In order to obtain a desired polynomial in $\mathbb{Z}[x]$, it suffices to replace each coefficient with the corresponding residue modulo p.

Suppose now that n is composite and let p be a prime divisor of n. Then any function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ with $f(0) \not\equiv f(p) \pmod{p}$ cannot be realized by a polynomial.

c) Answer: All prime n.

We will consider polynomials of degree $\leqslant n-1$ with coefficients from the set $\{0, 1, \ldots, n-1\}$, as a replacement of any coefficient with another element of the same residue class does not change the function $\mathbb{Z}_n \to \mathbb{Z}_n$. So we have exactly n^n polynomials under consideration, and this number coincides with the number of functions $\mathbb{Z}_n \to \mathbb{Z}_n$. This allows to use the result of b) as follows.

If p is prime, any function is realized as a polynomial, so different polynomiaqls determine different functions. Hence the zero function is determined by the zero polynomial only.

If n is composite, there exist functions that cannot be determined by a polynomial, hence there is a function which can be realized by two distinct polynomials under consideration, f and g. Then the difference $f - g$ is a nonzero polynomial modulo n, but this polynomial determines the zero function $\mathbb{Z}_n \to \mathbb{Z}_n$.

d) Answer: All positice integers n not divisible by 8, neither by a square of an odd prime.

Let $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. A function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$, satisfying the condition

$$\gcd(a-b, n) \mid \gcd(f(a) - f(b), n), \qquad a, b \in \mathbb{Z}_n,$$

will be referred to as *good*. A good function $f\colon \mathbb{Z}_n \to \mathbb{Z}_n$ determines naturally the functions $f_i : \mathbb{Z}_{p_i^{\alpha_i}} \to \mathbb{Z}_{p_i^{\alpha_i}}$; it is easy to see that all those functions are also good. If f is determined by a polynomial in $\mathbb{Z}[x]$, then all the f_i are determined by the same polynomial. Conversely, if each of the f_i is denermined by a polynomial $g_i \in \mathbb{Z}[x]$, then f is determined by some polynomial $g \in \mathbb{Z}[x]$ whose coefficients are congruent to those of the g_i modulo corresponding numbers (such coefficients are found by the Chinese remainders theorem).

Thus, the question in the problem is reduced to the same question where n is a power of a prime, $n = p^\alpha$.

If $n = p$ is prime, as we already know, every function $Z_p \to \mathbb{Z}_p$ is determined by a polynomial.

Assume now that $\alpha \geqslant 2$. Consider a function $h\colon \mathbb{Z}_{p^\alpha} \to \mathbb{Z}_{p^\alpha}$ such that $h(n) = p$ if $n \equiv p \pmod{p}^2$ and $h(n) = 0$ otherwise. It is easy to see that this function is good.

On the other hand, if o is odd, or if $p = 2$ and $\alpha \geqslant 3$, then this function cannot be determined by a polynomial in $\mathbb{Z}[x]$. Indeed, assume that h is determined by some polynomial $g \in \mathbb{Z}[x]$. We have $g(0) \equiv g(2p) \equiv 0 \pmod{p^2}$ and $g(p) \equiv p \pmod{p^2}$; then $g(p) \equiv g(0)+g'(0)p \pmod{p}^2$, whence $p \nmid g'(0)$. But, if p is odd, then $g(2p) \equiv g(0)+2g'(0)p \pmod{p}^2$; so $p \mid g'(0)$, which is a contradiction. Otherwise, if $p = 2$ and $\alpha \geqslant 3$, then $g(4) \equiv g(0) + 4g'(0) \pmod 8$, which also yields $2 \mid g'(0)$, because $g(0) \equiv g(4) \pmod 8$. This is a contradiction again.

It remains to investigate the case $n = 4$. Consider the function $g\colon \mathbb{Z}_4 \to \mathbb{Z}_4$ defined as $g(0) = 2$, $g(1) = g(2) = g(3) = 0$. This function is determined by the polynomial $(x-1)(x-2)(x-3)$. But it is easy to see that any good function is a sum of a constant and some of the functions x, $g(x)$, $g(x-1)$, $g(x-2)$, $g(x-3)$, so it is also determined by a polynomial.

3.4. Assume the contrary, and consider $g(x) = f(x+1) - f(x)$. The degree of g is not less than 1, and it suffices to take $p \in P(g)$: then the values of f at two consecutive points will be congruent modulo p.

3.5. Each of conditions means that f and g determine mutually inverse bijections $\mathbb{Z}_n \to \mathbb{Z}_n$.

3.6. (This is a problem from APMO2014)

Answer: All integers of the form $n = 3^k$, where k is a nonnegative integer.

In fact, we are looking for positive integers n with the following property $(*)$: *The set*

$$A = \{a^3 + a \,|\, a = 0, 1, \ldots, n-1\}$$

is a complete residue system modulo n, or, equivalently, *If integers* a, b *satisfy* $n \mid a^3 + a - b^3 - b = (a-b)(a^2+ab+b^2+1)$, *then* $n \mid a - b$.

Obviously, $n = 1$ satisfies $(*)$, while $n = 2$ does not.

Let us show first that $n = 3^k$ satisfies $(*)$ for all $k \geqslant 1$. Indeed, it is easy to show that a^2+ab+b^2+1 is not divisible by 3 for any positive integers a and b (one can either consider all possible resirus of a, b modulo 3, or notice that $a^2 + ab + b^2 + 1 = (a-b)^2 + 1 + 3ab$. Hence $3^k \mid (a-b)(a^2+ab+b^2+1)$ implies $3^k \mid a - b$.

Further, note that if A is not a complete residue system modulo r, then it is also not a complete residue system modulo any multiple of r. Hence it remains to prove that any prime $p > 3$ does not satisfy $(*)$.

If $p \equiv 1 \pmod 4$, take $a = 0$, and choose b satisfying $b^2 \equiv 1 \pmod p$. Then a^2+ab+b^2+1 is divisible by p, while $a - b$ is not.

Suppose now that $p \equiv 3 \pmod 4$, thus -1 is a non-quadratic residue modulo n. It suffices to find an integer x such that x^2+x+1 is a non-quadratic residue. Indeed, for such x, the residue $-(x^2+x+1)^{-1}$ is quadratic, hence the exists a non-zero residue a such that

$$-1 \equiv a^2(x^2+x+1) \equiv (ax)^2 + a \cdot ax + a^2 + 1 \pmod p;$$

then $(ax)^2 + a \cdot ax + a^2 + 1$ is divisible by p, while $ax - a$ is not divisible, except the case $x \equiv 1 \pmod p$. Finally, if $x \equiv 1 \pmod p$, then replace it by $x \equiv -2 \pmod p$ with the same resudue for x^2+x+1.

Assume, to the contrary, that each residue of the form x^2+x+1 is either quadratic or zero residue; then the same is true for $4(x^2+x+1) = 4(2x+1)^2+3$. Since $2(2x+1)$ runs over all residues, we obtain the following: if the residue y is either quadratic or zero modulo p, then the same is true for $y+3$. But iterating $y \mapsto y+3$ it is possible to obtain all the residues including a non-quadratic residue, which is a contradiction.

3.7. It is clear that $p > 2$. We need the following statement:

$$0^k + 1^k + \ldots + (p-1)^k \equiv \begin{cases} 0, & 1 \leqslant k \leqslant p-2; \\ -1, & k = p-1 \end{cases} \pmod p.$$

For $k = p-1$, it follows from Fermat's theorem. For $k < p-1$, let us take a primitive root t modulo p; then the LHS after multiplying by t^k remains the same modulo p. Since $t^k \not\equiv 1 \pmod p$, it follows that this sum is divisible by p.

a) Assume the contrary, then $f(0) + f(1) + \ldots + f(p-1) \equiv 0 + 1 + \ldots + (p-1) \equiv 0 \pmod p$. On the other hand, from the above we obtain $f(0) + f(1) + \ldots + f(p-1) \equiv -1 \pmod p$. A contradiction.

b) Let $p - 1 = dk$. Apply the idea from the solution of a) for the polynomial $g = f^k$. We have

$$-1 \equiv g(0) + g(1) + \ldots + g(p-1) \equiv (f(0))^k + (f(1))^k + \ldots + (f(p-1))^k \equiv$$
$$\equiv 0^k + 1^k + \ldots + (p-1)^k \equiv 0 \pmod p.$$

3.8. Since f determines a permutation σ on the set $\mathbb{Z}_n$, then

$$g = f(f(f(\ldots))) \ \ (k \,\text{iterations})$$

defines the permutation σ^k. Therefore, it suffices to take k such that σ^k is the identity permutation (i.e., so that k is divisible by the length of all independent cycles of σ, e.g., we can take $k = n!$), and set

$$g = f(f(f(\ldots))) \ \ (k-1 \,\text{iterations}).$$

Список литературы.

1. В. Прасолов. Многочлены. М: МЦНМО, 2003.

2. П.Кожевников, В.Сендеров. Делители значений многочлена. — Сборник «Задачи Санкт-Петербургской олимпиады по математике 2010 года». - СПб.: Невский Диалект, 2010, с. 121-129.

3. Д. Клюев, И. Богданов, А. Канель-Белов. Решение задачи 18.7. Математическое просвещение, серия 3, 2015, выпуск 19, с. 264-266

4. Н. Сафаеи, Об одной задаче В.А. Сендерова, Квант, 2021, № 10, с. 2–11

5. Polynomial Problems from the Awesomemath Summer Program (Xyz)
by Titu Andreescu, Navid Safaei, Alessandro Ventullo.

Минимизация ранга восполнением матриц

представляют А. Воропаев, Т. Гараев, С. Дженжер,
О. Никитенко, А. Петухов, А. Скопенков *

Содержание

1 Мотивировки и некоторые основные результаты **1**

2 Вырожденные матрицы **5**

3 Ранг матрицы **6**

4 Вложения по модулю 2 графов в поверхности **7**

5 Ранг матриц с соотношениями **10**

6 Classification of symmetric bilinear forms **11**

7 Rank of matrix with relations: generalization **13**

1 Мотивировки и некоторые основные результаты

Замечание (мотивировки; формально не используется далее)

«*Восполнение матриц — задача восстановления недостающих элементов в матрице, известной только частично. Одним из примеров такой задачи является восполнение матрицы с рейтингами фильмов в задаче Нетфликса: дана матрица рейтингов, в которой i,j-ый элемент равен оценке, поставленной пользователем i фильму j, если такая оценка есть, и пропущен в противном случае; мы хотим восполнить недостающие элементы этой матрицы, чтобы предсказать, насколько пользователям понравятся эти фильмы, и дать хорошие рекомендации...*» [MC] Пропущенные элементы матрицы заполняются так, чтобы минимизировать *ранг* восполненной матрицы. Все нужные определения (например, ранга) даны далее.

Для простоты мы рассматриваем матрицы над множеством $\mathbb{Z}_2 = \{0,1\}$ всех остатков по модулю 2 (с операциями сложения и умножения). Мы приведем интересные

А. Воропаев (Москва). *Т. Гараев:* Московский Государственный Университет. *С. Дженжер, А. Скопенков:* Московский Физико-Технический Институт. *О. Никитенко:* Алтайский Технический Университет (Барнаул). *А. Петухов:* Институт Проблем Передачи Информации им. А.А. Харкевича (Москва). *А. Скопенков:* Независимый Московский Университет, https://users.mccme.ru/skopenko/.
Благодарим Е. Когана за разрешение использовать его текст [Ko21], В. Ретинского и Я. Абрамова за полезные обсуждения, Д. Деомидова и Ф. Нилова за переводы фрагментов текста, А. Рябичева и издательство МЦНМО за разрешение использовать подготовленные ими рисунки.

элементарные результаты из линейной алгебры. Эти результаты позволяют построить алгоритмы, оценивающие ранг частично заполненных матриц для частного случая восполнения диагонали (предложение 1.1 и теоремы 1.3, 1.4, см. также предложение 1.2). Далее мы рассмотрим более сложную задачу. Вместо соотношений вида $M_{ij} = a_{ij}$ для некоторых элементов M_{ij} матрицы M (где a_{ij} это известные элементы) мы рассмотрим более сложные соотношения на элементы матрицы. Мы оценим минимальный ранг матриц с такими соотношениями (теоремы 5.1, 7.1).

Краткий обзор истории этой и близких задач см. в [MC, NKS] и [Ko21, Remark 4]. Эти результаты имеют приложения к вложениям графов в неориентируемые поверхности (включая вложение по модулю 2, см. начало §5) и вложениям k-мерных «гиперграфов» в $2k$-мерные поверхности, см. [KS21, KS21e, DS22]. В частности, теоремы 1.3, 1.4 влекут существование полиномиальных (по количеству рёбер) алгоритмов, распознающих «слабую реализуемость» «графов с вращениями» на неориентируемых поверхностях (см. замечание ниже).

Обозначим через $\mathbb{Z}_2^{s\times n} = (\mathbb{Z}_2^s)^n$ множество всех $s \times n$ матриц с элементами из $\mathbb{Z}_2$.

Предложение 1.1. *(a) Пусть имеется симметричная матрица с элементами из $\mathbb{Z}_2$. Тогда следующие условия равносильны:*

- *можно поменять некоторые элементы на главной диагонали так, чтобы все ненулевые строки матрицы оказались равны;*
- *нельзя сделать такую одинаковую перестановку строк и столбцов*[1]*, что в верхнем левом углу полученной матрицы будет стоять подматрица вида:*

$$\begin{pmatrix} * & 1 & 1 \\ 1 & * & 0 \\ 1 & 0 & * \end{pmatrix} \quad \textit{или} \quad \begin{pmatrix} * & 1 & 0 & 0 \\ 1 & * & 0 & 0 \\ 0 & 0 & * & 1 \\ 0 & 0 & 1 & * \end{pmatrix},$$

*где через * обозначены произвольные (возможно, различные) элементы.*

(b) Существует алгоритм сложности $O(n^2)$, который для любой матрицы $M \in \mathbb{Z}_2^{n\times n}$ определяет, можно ли поменять некоторые элементы на главной диагонали так, чтобы в получившейся матрице все ненулевые строки были равны.

Часть «только тогда» пункта (a) можно сдавать отдельно.

Алгоритмические результаты в этом тексте могут быть пропущены участниками, ориентированными на теорию, поскольку эти результаты являются простыми следствиями математических результатов. Сложность алгоритма — количество «элементарных» шагов в этом алгоритме. Алгоритм имеет сложность $O(f(n))$, если сложность не превосходит $Cf(n)$ для некоторой константы $C > 0$ для всех n.

Квадратная матрица $M \in \mathbb{Z}_2^{n\times n}$ называется **вырожденной**, если сумма её нескольких различных столбцов (ненулевого количества столбцов) равна нулевому столбцу (т. е. столбцу, состоящему только из нулей). Иначе матрица называется **невырожденной**. Вводные задачи о вырожденных матрицах, полезные для следующего результата, приведены в §2.

[1] Это означает, что строки и столбы последовательно занумерованы числами от 1 до n и выбрана перестановка f этих чисел; строки и столбцы переставляются так, что i,j-ый элемент становится $f(i), f(j)$-ым.

Предложение 1.2. *(a) Для любой матрицы $M \in \mathbb{Z}_2^{n\times n}$ можно поменять несколько элементов на главной диагонали так, чтобы получившаяся матрица была вырожденной.*

(b) То же с заменой «вырожденной» на «невырожденной».

Рассмотрим матрицу $M \in \mathbb{Z}_2^{s\times n}$. **Ранг** $\operatorname{rk} M$ — максимальное количество столбцов матрицы M таких, что сумма никаких из них не равна нулю. (Это «размерность» «векторного пространства», образованного столбцами матрицы). Вводные задачи на ранг, полезные для следующих результатов, приведены в §3.

Для $M \in \mathbb{Z}_2^{n\times n}$ обозначим через $R(M)$ минимальный из рангов всех матриц, полученных путем изменения некоторых чисел на главной диагонали матрицы M.

Матрица называется **диагональной**, если все её значения вне главной диагонали равны 0.

Теорема 1.3. *(a') Чтобы сделать квадратную матрицу ранга k из квадратной матрицы ранга n изменением некоторых чисел на главной диагонали, необходимо изменить не менее $|n-k|$ чисел.*

(a) Для любой невырожденной матрицы $M \in \mathbb{Z}_2^{n\times n}$ неравенство $R(M) \leqslant k$ равносильно существованию диагональной матрицы D с не более чем k нулями на главной диагонали такой, что $\operatorname{rk}(M+D) \leqslant k$.

(b) Для любого фиксированного k существует алгоритм сложности $O(n^{k+3})$, определяющий для любой матрицы $M \in \mathbb{Z}_2^{n\times n}$, верно ли, что $R(M) \leqslant k$.

Единичной матрицей E называется диагональная матрица, у которой все значения на диагонали равны 1.

Теорема 1.4. *(a) Для любой невырожденной матрицы $M \in \mathbb{Z}_2^{n\times n}$ и диагональной матрицы $D \in \mathbb{Z}_2^{n\times n}$ верно, что $2\operatorname{rk}(M+D) \geqslant \operatorname{rk}(M+E)$.*

(b) Существует алгоритм сложности $O(n^4)$, который для матрицы $M \in \mathbb{Z}_2^{n\times n}$ находит число k такое, что $k/2 \leqslant R(M) \leqslant k$.

Замечание (определение слабой реализуемости; формально не используется далее)

Иероглифом называется (неориентированное циклическое) слово длины $2n$ из n букв, в котором каждая буква встречается дважды.

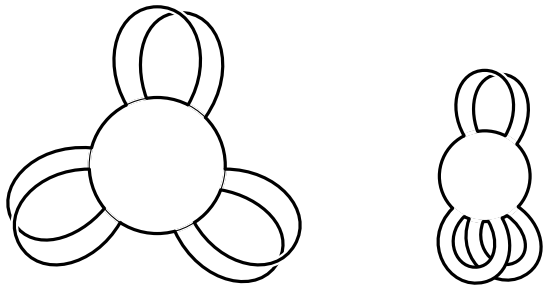


Рис. 1: Диск с ленточками, соответствующий иероглифу *aabbcc* (слева) и *aabcbc* (справа)

Возьмем границу выпуклого многоугольника. Отметим на ней непересекающиеся отрезки, отвечающие буквам данного слова, в том порядке, в котором буквы идут в слове. Для каждой буквы соединим (необязательно в плоскости) соответствующие ей два

отрезка ленточкой (т. е. «растянутым» и «помятым» прямоугольником) так, чтобы разные ленточки не пересекались. Ленточки могут быть перекрученными или неперекрученными. *Диском с ленточками*, отвечающим данному слову, называется объединение построенных (двумерного) выпуклого многоугольника и ленточек.

Назовем иероглиф *слабо реализуемым* на ленте Мёбиуса, если из неё можно вырезать некоторый диск с ленточками, соответствующий данному иероглифу. Можно аналогично определить слабую реализуемость на бутылке Клейна и других неориентируемых поверхностях.

Две буквы a, b в иероглифе H *перекрещиваются в* H, если они чередуются в циклической последовательности данного иероглифа (т. е. если они идут в циклическом порядке $abab$, а не $aabb$). Определим *матрицу перекрещиваний* $M(H) \in \mathbb{Z}_2^{n\times n}$ иероглифа H следующим образом. На главной диагонали поставим нули. Поставим единицу в клетку (i, j) для $i \neq j$, если буквы i, j перекрещиваются в H, в противном случае поставим ноль.

Верен следующий результат: *Иероглиф H слабо реализуем на ленте Мёбиуса тогда и только тогда, когда $R\big(M(H)\big) \leqslant 1$.*

См. подробнее [Bi20], [Ko21, Appendix], [Sk20, §2].

Рекомендации участникам

Если условие задачи является формулировкой утверждения, то в задаче требуется это утверждение доказать. 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 утверждения могут потребоваться последующие задачи. 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. *Замечания* и задачи, помеченные звёздочками, формально не используются в дальнейшем. В тексте определения важных понятий помечены **жирным шрифтом**, чтобы затем было проще их найти. Приглашаем Вас *обсуждать* с жюри возникающие вопросы. Те, кто успешно работают над проектом, завоюют право получить интересные *дополнительные задачи для исследования.*

Участник (или команда), решающий задачи проекта, получает «боб» за каждое **письменное решение для пользователя** (не являющееся просто ответом), оцененное в «+» или «+.».

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 один боб. Решения можно сдавать и **устно**, и **письменно для соавтора**, отдавая один боб за каждые пять попыток (неважно, удачных или нет).

Пожалуйста, сообщите нам, если Вы знаете решения каких-то из предложенных задач. Это не противоречит Вашему участию в проекте, но это и не обязывает Вас решать этот проект. После проверки у Вас некоторых из задач, названных Вами решёнными заранее, Вы сможете пользоваться результатами всех этих задач. При этом решения этих задач не будут считаться Вашим достижением на ЛКТГ. Зато у Вас появится возможность дойти до более сложных задач. Мы будем рады их выдать, они уже готовы!

(В проекте задачи были разбиты следующим образом: сначала задачи до теоремы 4.3 включительно, затем некоторые решения к простым задачам из §§1–2, затем остальные задачи и оставшиеся решения.)

2 Вырожденные матрицы

2.1. *(a1-a4) Какие из следующих матриц являются вырожденными?*

$$A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

2.2. *(a) Вырожденность матрицы сохраняется при перестановке столбцов (строк).*

(b) Вырожденность матрицы сохраняется при добавлении одного столбца (одной строки) к другому (другой).

(c) Любая матрица может быть превращена в диагональную преобразованиями из пунктов (a,b).

(d) Матрица вырождена тогда и только тогда, когда она не может быть превращена в единичную преобразованиями из (a,b).

(f) Квадратная матрица вырождена тогда и только тогда, когда сумма её некоторых строк (ненулевого количества строк) является нулевой строкой.

(g) Существует алгоритм сложности $O(n^3)$, определяющий, является ли матрица $n \times n$ вырожденной.

Для матрицы $M \in \mathbb{Z}_2^{n\times n}$ положим $\det M := 0$, если она вырождена, и $\det M := 1$ иначе. Это число называется *определителем* матрицы M. Другое обозначение:

$$\det\begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{pmatrix} = \begin{vmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{vmatrix}, \quad \det M = \begin{vmatrix} M_{1,1} & \dots & M_{1,n} \\ \vdots & \ddots & \vdots \\ M_{n,1} & \dots & M_{n,n} \end{vmatrix}.$$

2.3. *(a)* $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad + bc$.

(b) $\det(a_1+b_1, a_2, \dots, a_n) = \det(a_1, a_2, \dots, a_n)+\det(b_1, a_2, \dots, a_n)$. *Здесь и ниже* $a_j, b_1 \in \mathbb{Z}_2^n$ *это столбцы длины* n.

(c) $\det(a_1, \dots, a_n) = \sum\limits_{i=1}^{n} a_{i,n} \det(a_1^-, \dots, a_{i-1}^-, a_{i+1}^-, \dots, a_n^-)$, *где каждый столбец* $a_i^- \in \mathbb{Z}_2^{n-1}$ *получается из столбца* a_i *удалением последней координаты.*

*(d)** $\det M = \sum\limits_{\sigma\in S_n} \prod\limits_{i=1}^{n} M_{i,\sigma(i)}$, *где* S_n *— множество перестановок (т.е. взаимно однозначных соответствий)* $\sigma : [n] \to [n]$.

2.4. *(a1-a4) Для каждой матрицы из задачи 2.1 выясните, можно ли изменить некоторые элементы на главной диагонали так, чтобы полученная матрица была вырожденной.*

(b1-b4) То же с заменой «вырожденной» на «невырожденной».

Лемма 2.5. *(a) Пусть $M \in \mathbb{Z}_2^{n\times n}$ — матрица с нулями на главной диагонали. Определим последовательность $M^{(i)}$, $i = 0, 1, 2, \dots, n$ рекурсивно.*

- $M^{(0)} := M$;
- $M^{(i)}$ *есть результат замены в* $M^{(i-1)}$ *элемента* $M^{(i-1)}_{i,i} = 0$ *на* $1 + \delta_i$, *где* $\delta_i := \det M^{(i-1)}_{[i]\times[i]}$ *есть определитель верхней левой* $i \times i$*-подматрицы матрицы* $M^{(i-1)}$.

Тогда матрица $M^{(n)}$ *невырождена.*

(b) Существует алгоритм сложности $O(n^4)$, *который для матрицы* $M \in \mathbb{Z}_2^{n\times n}$ *находит набор таких значений из* $\mathbb{Z}_2$, *что после подстановки их на главную диагональ матрицы* M *получится невырожденная матрица.*

3 Ранг матрицы

3.1. *(a1-a4) Найдите* $\operatorname{rk} M$ *для матриц*

$$M = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

(b1-b4) Найдите $R(M)$ *для матриц из задачи 2.1.*

3.2. *Выберем матрицу* $M \in \mathbb{Z}_2^{s\times n}$.

(a) Из матрицы M *можно выбрать* $\operatorname{rk} M$ *столбцов так, чтобы любой столбец был суммой нескольких выбранных столбцов.*

(b) Пусть имеется k *столбцов (не обязательно матрицы* M*) таких, что любой столбец матрицы* M *есть сумма нескольких из них. Тогда* $\operatorname{rk} M \leqslant k$.

(c) Ранг подматрицы не превосходит ранга матрицы.

3.3. *(a) Перестановка столбцов (или строк) не меняет ранга матрицы.*

(b) Добавление одного столбца к другому столбцу (или одной строки к другой) не меняет ранга матрицы.

(c) Ранг матрицы равен максимальному количеству её строк таких, что сумма никаких из них не равна нулевой строке.

(d) Ранг матрицы равен максимальному размеру её невырожденной квадратной подматрицы.

Квадратная матрица, в которую выставлены значения из $\mathbb{Z}_2$, называется **чётной**, если все её значения на главной диагонали равны нулю.

3.4. *(a) Для любой* $M \in \mathbb{Z}_2^{s\times n}$ *все ненулевые строки равны тогда и только тогда, когда* $\operatorname{rk} M \leqslant 1$.

(b) Для симметричной матрицы $M \in \mathbb{Z}_2^{n\times n}$ *все ненулевые строки равны тогда и только тогда, когда, используя одинаковые перестановки строк и столбцов, из неё можно получить матрицу, левый верхний угол которой состоит из единиц, а элементы вне этого квадрата равны нулю.*

(c) Ранг любой ненулевой чётной симметричной матрицы больше единицы.

3.5. *Величина* $R(M)$ *необязательно сохраняется при*

(a) перестановках столбцов;

(b) добавлении одного столбца к другому.

3.6. *(a) Существует алгоритм сложности $O(n^3)$, вычисляющий ранг матрицы из $\mathbb{Z}_2^{s\times n}$, $s \leqslant n$.*

(b) Для всякого числа k существует алгоритм сложности $O(n^2)$, проверяющий свойство «*$\operatorname{rk} M \leqslant k$*» для $M \in \mathbb{Z}_2^{s\times n}$, $s \leqslant n$.*

Лемма 3.7. *Пусть M, D — это матрицы одного размера, в клетках которых стоят элементы $\mathbb{Z}_2$. Тогда*

(a) $\operatorname{rk}(M + D) \leqslant \operatorname{rk} M + \operatorname{rk} D$;

(b) $\operatorname{rk}(M + D) \geqslant \operatorname{rk} M - \operatorname{rk} D$.

3.8. *Существует алгоритм сложности $O(n^{k+3})$, находящий по матрице $M \in \mathbb{Z}_2^{n\times n}$ диагональную матрицу D такую, что*

(a) $\operatorname{rk}(M + D) \leqslant k$,

(b) $\operatorname{rk}(M + D) = k$,

при условии, что такая матрица D существует.

3.9. *Для любых ли $m, k \leqslant n$ и матрицы $M \in \mathbb{Z}_2^{n\times n}$ ранга m верно следующее: если матрица ранга k может быть получена изменением некоторого количества диагональных элементов матрицы M, то это может быть сделано изменением ровно $|m - k|$ элементов?*

3.10. *(a,b,c) Найдите число матриц ранга k в $\mathbb{Z}_2^{n\times n}$ для $k = 0, 1, 2$.*

4 Вложения по модулю 2 графов в поверхности

Данный раздел не нужен для понимания дальнейшего текста, однако он дает мотивацию к §5.

Мы будем обозначать через S либо тор, либо сферу с ручками, либо ленту Мёбиуса, либо бутылку Клейна, либо какую-то другую 2-мерную поверхность. Их простое определение можно найти, например, в §2.1 в

[Sk20]=https://www.mccme.ru/circles/oim/obstruct.pdf

Далее изображения графов на S могут иметь самопересечения. *Вложением* называется изображение графа без самопересечений.

4.1. *Существуют вложения графов (a1,a2,a3) K_5, K_6, K_7 в тор;*

(b1,b2) K_5, K_6 в ленту Мёбиуса;

(c) K_8 в сферу с двумя ручками;

(d) K_m в сферу с каким-то числом (зависящим от m) ручек.

Замечание. *В данной задаче требуются не строгие доказательства, а большие, понятные и желательно красивые рисунки.*

4.2. *Граф K_5 может быть изображён на плоскости так, что изображения (то есть образы) любых двух несмежных рёбер пересекаются в чётном числе точек.*

Точкой самопересечения изображения называется точка на изображении, которая отвечает более чем одной точке графа.

Говорят, что изображение графа находится **в общем положении**, если

- любой точке самопересечения отвечают ровно две точки графа;
- изображение любой вершины не является точкой самопересечения;

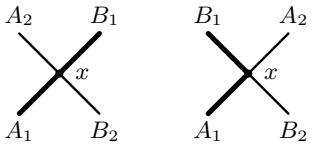


Рис. 2: Трансверсальное пересечение и нетрансверсальное пересечение

- изображение графа имеет конечное число точек самопересечения, и
- в любых таких точках самопересечение трансверсальное (рис. 2)[2].

Изображение графа в общем положении называется $\mathbb{Z}_2$**-вложением**, если изображения любых двух несмежных рёбер пересекаются в чётном числе точек.

Замечание. Пусть S — либо плоскость, либо тор, либо лента Мёбиуса. Если граф допускает $\mathbb{Z}_2$-вложение в S, то этот граф допускает вложение в S. Тем не менее, существует граф, имеющий $\mathbb{Z}_2$-вложение в сферу с 4 ручками, но не вложимый в неё. См. ссылки в [Bi21, Remark 1.3.b,c].

Теорема 4.3. *Если граф K допускает $\mathbb{Z}_2$-вложение в сферу с g ручками, то*
(a) $g \geqslant (m-4)/3$ *для* $K = K_m$.
(b) $g \geqslant (m-5)^2/16$ *для* $K = K_m$.
(c) $g \geqslant (n-2)^2/4$ *для* $K = K_{n,n}$.

Идея доказательства теоремы 4.3 заключается в том, что на поверхности, в которую большой граф допускает $\mathbb{Z}_2$-вложение, пересечения кривых устроены достаточно сложно (в смысле ранга некоторой матрицы; см. утверждение 4.5). Точнее, теорема 4.3.a [PT19] следует из теорем 4.4 и 5.1.b вместе с утверждением 4.5 (все ниже). Теорема 4.3.b следует из пункта теоремы 4.3.c (докажите!). Теорема 4.3.c доказана в [FK19], см. структурированное изложение в [DS22]. Аналогично, утверждения 4.5 и 5.2 (вместе с теоремой 4.4 и её неориентированным аналогом) влекут несуществование $\mathbb{Z}_2$-вложения K_8 в тор, и K_7 в ленту Мёбиуса (или даже K_7 в бутылку Клейна, чей аналог для невложимости не следует из неравенства Эйлера). Аналогичным образом результат о невложимости в более высоких размерностях следует из теоремы 7.1.

Обозначим через $|X|_2 \in \mathbb{Z}_2$ чётность числа элементов в конечном множестве X.

Говорят, что замкнутые кривые $\gamma_1, \dots, \gamma_p$ на S находятся в **общем положении**, если изображение графа (несвязного объединения p циклов), полученное из этих кривых, находится в общем положении. Их $p \times p$*-матрица пересечений* G определена как

$$G_{i,j} := \begin{cases} |\gamma_i \cap \gamma_j|_2, & \text{если } i \neq j, \\ |\gamma_i \cap \gamma_i'|_2, & \text{если } i = j, \end{cases}$$

где γ_i' — это кривая, близкая к кривой γ_i и в общем положении с ней.

Пользуйтесь следующей «гомологической теоремой Бетти» без доказательства.

[2]Строго говоря, трансверсальность легко определить только для PL (кусочно-линейного) изображения графа. PL кривые на торе легко определить, если рассматривать тор как склейку многоугольника. Тогда *PL кривая на торе* — это семейство ломаных на многоугольнике, удовлетворяющее некоторым условиям (выпишите эти условия!). Похожим образом любая поверхность S может быть получена склейкой многоугольника. (Для ленты Мёбиуса и бутылки Клейна см. [Sk20, §2.1]; для сферы с ручками см. визуализацию в https://www.youtube.com/watch?v=G1yyfPShgqw и в https://www.youtube.com/watch?v=U5N5mg3MePM.) Это позволяет определить PL кривые на S. Тогда изображение графа на S называется *PL (кусочно-линейным)*, если изображение любого ребра этого графа PL. Другая формализация приведена в [Sk20, §4, §5].

Теорема 4.4. *Для любых кривых $\gamma_1, \dots, \gamma_p$ в общем положении*

(a) на сфере с g ручками ранг их матрицы пересечений не превосходит $2g$.

(b) на диске с m лентами Мёбиуса ранг их матрицы пересечений не превосходит m.

Здесь *диск с k лентами Мёбиуса* — это фигура, изображённая на рис. 1, слева. Более точно, диск с m лентами Мёбиуса — это объединение диска и m попарно непересекающихся ленточек, концы которых приклеены к $2m$ попарно непересекающимся дугам на граничной окружности диска (ленточки могут не лежать в плоскости диска) так, что

• ориентации концов каждой из ленточек, заданные ориентацией граничной окружности диска, «сохраняют направление вдоль ленточки», и

• ленточки «разделены», т. е. существуют m попарно непересекающихся дуг A_i граничной окружности диска такие, что концы i-ой ленточки приклеены к двум непересекающимся дугам, содержащимся в A_i, $i = 1, 2, \dots, m$.

Вы можете делать аппроксимации общего положения на интуитивном уровне.

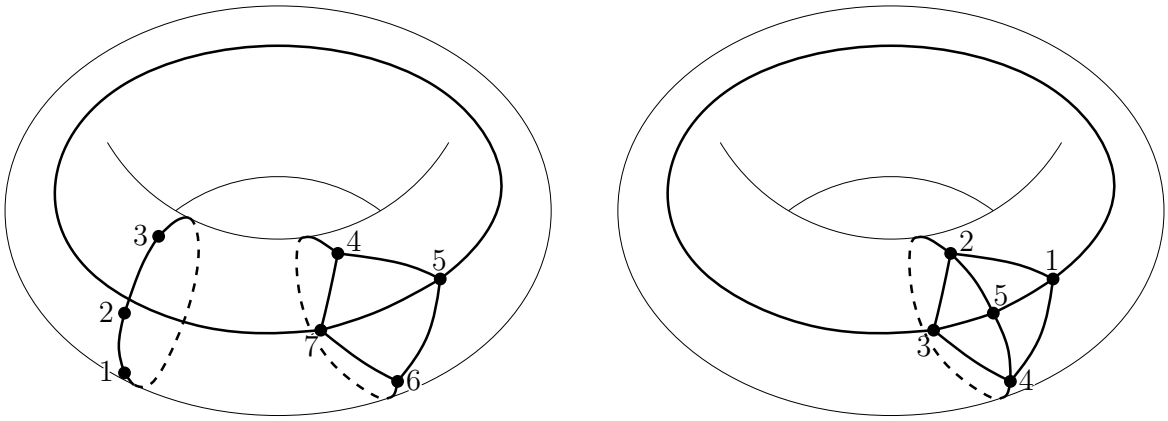


Рис. 3: Слева: K_3 и K_4 на торе. Справа: K_5 на торе

4.5. *Рассмотрим произвольное вложение (или $\mathbb{Z}_2$-вложение) $f\colon K_n \to S$. Рассмотрим произвольное отображение $f'\colon K_n \to S$ в общем положении с f и близкое к f. Для любых попарно различных $i, j, k \in [n]$ обозначим через $\langle ijk\rangle$ цикл длины три в K_n. Положим*

$$ijk \wedge pqr := \left|f\langle ijk\rangle \cap f'\langle pqr\rangle\right|_2.$$

Тогда

(4.5.1) $123 \wedge 456 = 0$.

(4.5.2) $123 \wedge 456 + 123 \wedge 567 + 123 \wedge 467 + 123 \wedge 457 = 0$.
$123 \wedge 345 + 123 \wedge 346 + 123 \wedge 356 + 123 \wedge 456 = 0$.
$123 \wedge 234 + 123 \wedge 235 + 123 \wedge 245 + 123 \wedge 345 = 0$.
$123 \wedge 123 + 123 \wedge 124 + 123 \wedge 134 + 123 \wedge 234 = 0$.

См. рис. 3, слева. Для одной формулы, охватывающей эти четыре, см. свойство линейной зависимости в §5.

(4.5.3) $125 \wedge 345 + 135 \wedge 245 + 145 \wedge 235 = 1$.

См. рис. 3, справа. Подсказка: выведите из (B) ниже.

Замечание. (A) Для любых попарно различных точек A_1, A_2, A_3, A_4 на прямой существует только одна «чередующаяся» раскраска в два цвета.

(B) Для любых попарно различных точек A_1, A_2, A_3, A_4 на окружности

$$|A_1A_2 \cap A_3A_4| + |A_1A_3 \cap A_2A_4| + |A_1A_4 \cap A_2A_3| = 1.$$

(B') Для любого отображения $f\colon K_5 \to \mathbb{R}^2$ «общего положения» число точек пересечений, образованных образами несмежных рёбер в $\mathbb{R}^2$, нечётно.

Простая импликация $(A) \Rightarrow (B')$ приводится в [Sk14] (в линейном случае; в PL случае импликация аналогична).

В отличие от невложимости, отсутствие $\mathbb{Z}_2$-вложимости не следует из неравенства Эйлера [Sk20, §2.4] (как и (B') не следует из формулы Эйлера для планарных графов).

5 Ранг матриц с соотношениями

Мы сокращаем $\{i\}$ до i. Назовём $\binom{[m]}{3}$-*матрицей* такую симметричную квадратную матрицу с элементами из $\mathbb{Z}_2$, строки и столбцы которой соответствуют всем 3-элементным подмножествам множества $[m]$, и для которой выполнены следующие свойства:

(тривиальность) $A_{P,Q} = 0$, если $P \cap Q = \varnothing$;

(линейная зависимость) для любых 4-элементного и 3-элементного подмножеств $F, P \subset [m]$

$$\sum_{i \in F} A_{F-i,P} = 0.$$

(нетривиальность) для любых $i \in [m]$ и 4-элементного подмножества $F \subset [m] - i$ выполнено $A_{F,i} = 1$, где

$$A_{F,i} := \sum_{\{X,Y\}\,:\,F \cup i = X \cup Y,\ |X|=|Y|=3,\ X\cap Y = i} A_{X,Y} = \sum_{\{\sigma,\tau\}\,:\,F=\sigma\sqcup\tau,\ |\sigma|=|\tau|=2} A_{i\sqcup\sigma,i\sqcup\tau}.$$

По утверждению 4.5, некоторая $\binom{[m]}{3}$-матрица строится по $\mathbb{Z}_2$-вложению $f\colon K_m \to S$ в поверхность. Действительно, положим $A_{\{i,j,k\},\{p,q,r\}} := ijk \wedge pqr$. Если поверхность S ориентируема, то такая матрица A чётна (т. е., $A_{P,P} = 0$ для любого 3-элементного подмножества $P \subset [m]$).

Теорема 5.1. *(a) Если A является $\binom{[m]}{3}$-матрицей, то* $\operatorname{rk} A \geqslant \dfrac{m-4}{3}$.

(b) Более того, если A чётна, то $\operatorname{rk} A \geqslant \dfrac{2(m-4)}{5}$.

Вы можете отдельно представлять решения следующих частных случаев теоремы 5.1. Более сильные оценки доказаны в §7.

5.2. *(a)* Не существует $\binom{[7]}{3}$-матрицы ранга* 1.

(b) Не существует чётной $\binom{[8]}{3}$-матрицы ранга менее* 3.

Теорему 5.1 можно вывести из предложений 5.7.a,b.

Следующее утверждение в дальнейшем не используется. В его доказательстве не обязательно явно предоставлять матрицу, достаточно описать её построение. Мы знаем только решение, использующее утверждения 4.1, 4.5 и теорему 4.4.

5.3. *(a) Существует ненулевая* $\binom{[4]}{3}$*-матрица.*
(b) Существует $\binom{[5]}{3}$*-матрица.*
(c) Для любого $m \geqslant 5$ *существует* $\binom{[m]}{3}$*-матрица.*
(a',b',c') То же для чётных матриц.
(d) Существует $\binom{[5]}{3}$*-матрица ранга* 1*.*
(e) Существует чётная $\binom{[5]}{3}$*-матрица ранга* 2*.*
(f) Существует $\binom{[6]}{3}$*-матрица ранга* 1*.*
(g) Существует* $\binom{[8]}{3}$*-матрица ранга более* 2*.*

5.4. *Пусть* B *— квадратная матрица размера* $\binom{m-1}{3}$*, полученная из* $\binom{[m]}{3}$*-матрицы удалением строк и столбцов, соответствующих всем подмножествам, содержащим элемент* m*. Тогда* B *является* $\binom{[m-1]}{3}$*-матрицей.*

5.5. *(a) Пусть* B *— квадратная матрица размера* $\binom{m-3}{3}$*, полученная из* $\binom{[m]}{3}$*-матрицы* A *удалением строк и столбцов, соответствующих подмножествам, содержащим хотя бы один элемент множества* $X := \{m, m-1, m-2\}$*. Если* $A_{X,X} = 1$*, то* $\operatorname{rk} A > \operatorname{rk} B$*.*
(b) Пусть B *— квадратная матрица, полученная из* $\binom{[m]}{3}$*-матрицы* A *удалением строк и столбцов, соответствующих подмножествам, содержащим хотя бы один элемент* 3*-элементных подмножеств* $X, Y \subset [m]$*. Если* $A_{X,X} = A_{Y,Y} = 0$ *и* $A_{X,Y} = 1$*, то* $\operatorname{rk} A \geqslant \operatorname{rk} B + 2$*.*

Обозначим через r_m минимальный ранг $\binom{[m]}{3}$-матрицы. Обозначим через $\widetilde{r_m}$ минимальный ранг чётной $\binom{[m]}{3}$-матрицы. Очевидно, $r_m = \widetilde{r_m} = 0$ для $m \leqslant 4$, и $r_m \leqslant \widetilde{r_m}$. Нетривиальность означает, что $r_5, \widetilde{r_5} \geqslant 1$. Теорема 5.1 утверждает, что $r_m \geqslant \dfrac{m-4}{3}$ и $\widetilde{r_m} \geqslant \dfrac{2(m-4)}{5}$.

5.6. *(a,b) Найдите* r_5, r_6 *и* $\widetilde{r_5}, \widetilde{r_6}, \widetilde{r_7}$*.*
(c) Обе последовательности $r_m, \widetilde{r_m}$ *не убывают.*

Предложение 5.7. *(a)* $r_m \geqslant \min\{r_{m-3} + 1, \widetilde{r_m}\}$ *(точнее, либо* $r_m = \widetilde{r_m}$*, либо* $r_m \geqslant r_{m-3} + 1$*);*
(b) $\widetilde{r_m} \geqslant \widetilde{r_{m-5}} + 2$*.*

6 Classification of symmetric bilinear forms

Fix a symmetric matrix $A \in \mathbb{Z}_2^{n \times n}$. For $U, V \in \mathbb{Z}_2^n$ let

$$A(U, V) = U \cdot_A V := \sum_{i,j=1}^{n} A_{i,j} U_i V_j \quad (= U^T A V).$$

A **basis** of $\mathbb{Z}_2^n$ is an inclusion-minimal ordered set of vectors such that every vector from $\mathbb{Z}_2^n$ is the sum of some vectors from this set.

Теорема 6.1. *For* $n = 2$ *there is a basis* X_1, X_2 *of* $\mathbb{Z}_2^2$ *and numbers* $\gamma_1, \gamma_2 \in \mathbb{Z}_2$ *such that either*

(i) for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2) \cdot_A (b_1X_1 + b_2X_2) = \gamma_1 a_1 b_1 + \gamma_2 a_2 b_2, \quad \text{or}$$

(ii) for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2) \cdot_A (b_1X_1 + b_2X_2) = a_1 b_2 + a_2 b_1.$$

Recall that problems stated after theorems are hints to proofs of the theorems.

6.2. *Assume that $n = 2$, $X \in \mathbb{Z}_2^2$ and $X \cdot_A X = 1$.*

(a) For any $P \in \mathbb{Z}_2^2$ there is $\lambda_{X,P} \in \mathbb{Z}_2$ such that for $P_X := P + \lambda_{X,P}X$ we have $P_X \cdot_A X = 0$.

(b) There is a basis $X_1 = X$, X_2 of $\mathbb{Z}_2^2$ and numbers $\gamma_1 = 1, \gamma_2 \in \mathbb{Z}_2$ such that the property (i) of Theorem 6.1 holds.

6.3. *Assume that $n = 2$, $X, Y \in \mathbb{Z}_2^2$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$. Then $X_1 := X$, $Y_1 := Y$ is a basis of $\mathbb{Z}_2^2$ such that the property (ii) of Theorem 6.1 holds.*

Теорема 6.4. *For $n = 3$ there is a basis X_1, X_2, X_3 of $\mathbb{Z}_2^3$ and numbers $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}_2$ such that either*

(i) for any $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2 + a_3X_3) \cdot_A (b_1X_1 + b_2X_2 + b_3X_3) = \gamma_1 a_1 b_1 + \gamma_2 a_2 b_2 + \gamma_3 a_3 b_3, \quad \text{or}$$

(ii) for any $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2 + a_3X_3) \cdot_A (b_1X_1 + b_2X_2 + b_3X_3) = a_1 b_2 + a_2 b_1 + \gamma_3 a_3 b_3.$$

6.5. *Assume that $X, Y \in \mathbb{Z}_2^3$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$.*

(a) For any $P \in \mathbb{Z}_2^3$ there are $\lambda_{X,Y,P}, \lambda_{Y,X,P} \in \mathbb{Z}_2$ such that for $P_{X,Y} := P + \lambda_{X,Y,P}Y + \lambda_{Y,X,P}X$ we have $P_{X,Y} \cdot_A X = P_{X,Y} \cdot_A Y = 0$.

(b) There is a basis $X_1 = X$, $X_2 = Y$, X_3 of $\mathbb{Z}_2^3$ and a number $\gamma_3 \in \mathbb{Z}_2$ such that the property (ii) of Theorem 6.4 holds.

Теорема 6.6. *There are k, l and a basis $X_1, Y_1, \ldots, X_k, Y_k, Z_1, \ldots, Z_{n-2k}$ of $\mathbb{Z}_2^n$ such that $2k + l \leqslant n$ and for any $a, a', b, b' \in \mathbb{Z}_2^k$ and $c, c' \in \mathbb{Z}_2^{n-2k}$ we have*

$$\begin{gathered}(a_1X_1 + b_1Y_1 + \ldots + a_kX_k + b_kY_k + c_1Z_1 + \ldots + c_{n-2k}Z_{n-2k}) \cdot_A \\ \cdot_A (a'_1X_1 + b'_1Y_1 + \ldots + a'_kX_k + b'_kY_k + c'_1Z_1 + \ldots + c'_{n-2k}Z_{n-2k}) = \\ = a_1b'_1 + a'_1b_1 + \ldots + a_kb'_k + a'_kb_k + c_1c'_1 + \ldots + c_lc'_l.\end{gathered}$$

If A is even, then $l = 0$.

6.7. *Assume that $X \in \mathbb{Z}_2^n$ and $X \cdot_A X = 1$.*

(a) State and prove the n-dimensional analogue of Assertion 6.2.a.

(b) There is a basis $X, E_1, \ldots, E_{n-1}$ of $\mathbb{Z}_2^n$ and a symmetric matrix $B \in \mathbb{Z}_2^{(n-1)\times(n-1)}$ such that for any $a, b \in \mathbb{Z}_2$ and $\lambda, \mu \in \mathbb{Z}_2^{n-1}$ we have

$$(aX + \lambda_1E_1 + \ldots + \lambda_{n-1}E_{n-1}) \cdot_A (bX + \mu_1E_1 + \ldots + \mu_{n-1}E_{n-1}) = ab + \lambda \cdot_B \mu.$$

6.8. *Assume that $X, Y \in \mathbb{Z}_2^n$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$.*

(a) State and prove the n-dimensional analogue of Assertion 6.5.a.

(b) There is a basis $X, Y, E_1, \ldots, E_{n-2}$ of $\mathbb{Z}_2^n$ and a symmetric matrix $B \in \mathbb{Z}_2^{(n-2)\times(n-2)}$ such that for any $a_X, a_Y, b_X, b_Y \in \mathbb{Z}_2$ and $\lambda, \mu \in \mathbb{Z}_2^{n-2}$ we have

$$(a_XX + a_YY + \lambda_1E_1 + \ldots + \lambda_{n-2}E_{n-2}) \cdot_A (b_XX + b_YY + \mu_1E_1 + \ldots + \mu_{n-2}E_{n-2}) = a_Xb_Y + a_Yb_X + \lambda \cdot_B \mu.$$

7 Rank of matrix with relations: generalization

The following results are 'higher-dimensional' (and more strong) generalizations of Theorem 5.1, Assertions 5.4 and 5.5, and Proposition 5.7. They give a simplified well-structured exposition of [PT19, Theorem 1].

An $\binom{[m]}{l}$-*matrix* is a symmetric square matrix with $\mathbb{Z}_2$-entries whose rows and whose columns correspond to all l-element subsets of $[m]$, and for which (triviality) and the following properties hold:

(linear dependence) for each $(l+1)$-element and l-element subsets $F, P \subset [m]$

$$\sum_{i\in F} A_{F-i,P} = 0.$$

(non-triviality) for each $i \in [m]$ and $(2l-2)$-element subset $F \subset [m]-i$ we have $A_{F,i} = 1$, where

$$A_{F,i} := \sum_{\{X,Y\}\,:\,F\cup i=X\cup Y,\ X\cap Y=i,\ |X|=|Y|=l} A_{X,Y} = \sum_{\{\sigma,\tau\}\,:\,F=\sigma\sqcup\tau,\ |\sigma|=l-1} A_{i\sqcup\sigma,i\sqcup\tau}.$$

Analogously to Assertion 4.5, an $\binom{[m]}{l}$-matrix is constructed by a $\mathbb{Z}_2$-embedding of the $(l-1)$-dimensional skeleton of the $(m-1)$-dimensional simplex to a $2(l-1)$-dimensional manifold.

Теорема 7.1. *Suppose $l \geqslant 3$ and A is an $\binom{[m]}{l}$-matrix.*

(a) Then $\operatorname{rk} A \geqslant \dfrac{m-2l+2}{l-1}$. *(b) If, moreover, A is even, then* $\operatorname{rk} A \geqslant \dfrac{2(m-2l+2)}{l}$.

You can deduce Theorem 7.1 from Propositions 7.4.a,b.

7.2. *Let A' be the square matrix of size $\binom{m-1}{l}$ obtained from an $\binom{[m]}{l}$-matrix by deleting rows and columns corresponding to all subsets containing m. Then A' is an $\binom{[m-1]}{l}$-matrix.*

7.3. *Let A be an $\binom{[m]}{l}$-matrix and $X := \{m-l+1, m-l+2, \dots, m\}$.*

(a,b') Let B be the square matrix of size $\binom{m-l}{l}$ obtained from A by deleting rows and columns corresponding to subsets containing at least one of the elements of X.

If $A_{X,X} = 1$, then $\operatorname{rk} A > \operatorname{rk} B$.

If $A_{X,X} = A_{Y,Y} = 0$ and $A_{X,Y} = 1$ for some $Y \subset [m]$, then $\operatorname{rk} A \geqslant \operatorname{rk} B + 2$.

(b) Let C be the square matrix obtained from A by deleting rows and columns corresponding to subsets containing at least one element of X or of certain l-element subset $Y \subset [m]$. If $A_{X,X} = A_{Y,Y} = 0$ and $A_{X,Y} = 1$, then $\operatorname{rk} A \geqslant \operatorname{rk} C + 2$.

(a') For l-element subsets $P, Q \subset [m-l+1]$ define

$$D_{P,Q} := A_{P,Q} + A_{P,X}A_{Q,X}.$$

If $A_{X,X} = 1$, then $\operatorname{rk} D < \operatorname{rk} A$ *and D is an $\binom{[m-l+1]}{l}$-matrix.*

Assertions 7.3.a,b are only required to illustrate the idea of Assertions 7.3.a',b' by proving much easier results giving estimates $\operatorname{rk} A \geqslant \dfrac{m-2l+2}{l}$ and, for A even, $\operatorname{rk} A \geqslant \dfrac{2(m-2l+2)}{2l-1}$.

Denote by r_m the minimal rank of an $\binom{[m]}{l}$-matrix. Denote by $\widetilde{r_m}$ the minimal rank of an even $\binom{[m]}{l}$-matrix. Clearly, $r_m = \widetilde{r_m} = 0$ for $m \leqslant 2l-2$, both sequences $r_m, \widetilde{r_m}$ are non-decreasing, and $r_m \leqslant \widetilde{r_m}$. The non-triviality implies that $r_{2l-1}, \widetilde{r_{2l-1}} \geqslant 1$. Theorem 7.1 asserts that $r_m \geqslant \dfrac{m-2l+2}{l-1}$ and $\widetilde{r_m} \geqslant \dfrac{2(m-2l+2)}{l}$.

Предложение 7.4. *(a)* $r_m \geqslant \min\{r_{m-l+1}+1, \widetilde{r_m}\}$ *(more precisely, either* $r_m = \widetilde{r_m}$*, or* $r_m \geqslant r_{m-l+1}+1$*);*

(b) $\widetilde{r_m} \geqslant \widetilde{r_{m-l}} + 2$.

Proof of Proposition 7.4.a also uses an algebraic version (b) of the higher-dimensional analogue of the following result (a).

Предложение 7.5. *(a) Denote by* $X = \binom{[5]}{2}$ *the set of unordered pairs of* 2*-element subsets of* $[5]$*. For any* $i \in [5]$ *and a partition* $[5]-i = \sigma \sqcup \tau$ *into disjoint* 2*-element sets denote*

$$T_{i,\{\sigma,\tau\}} := \big\{\{\alpha,\beta\} \in X \ : \ \alpha \subset \sigma \sqcup i, \ \beta \subset \tau \sqcup i\big\}.$$

Denote by A_i *the sum modulo* 2 *(i. e., the symmetric difference) of sets* $T_{i,\{\sigma,\tau\}}$ *over all non-ordered partitions* $[5]-i = \sigma \sqcup \tau$ *as above. Then*

$$A_i = \big\{\{\alpha,\beta\} \in X \ : \ \alpha \cap \beta = \varnothing\big\}$$

and so is independent of i*.*

(b) Let A *be a symmetric square matrix with* $\mathbb{Z}_2$*-entries whose rows and whose columns correspond to all* l*-element subsets of* $[m]$*. If* A *satisfies the linear dependence property (from the definition of an* $\binom{[m]}{l}$*-matrix), then* $A_{F,i}$ *depends only on* $F \sqcup i$ *not on* (F,i)*.*

Указания и решения к §§1–7

Доказательство предложения 1.1 см. в [Bi20].

1.2. (a) Изменим числа на главной диагонали матрицы M таким образом, чтобы сумма элементов в каждой строке стала чётной. Тогда получившаяся матрица будет вырожденной.

(b) Используйте индукцию. См. лемму 2.5.a.

1.3. (a) Любая матрица с коэффициентами из $\mathbb{Z}_2$, полученная из матрицы M заменой элементов на главной диагонали, может быть представлена единственным образом как $M+D$, где D — диагональная матрица. По лемме 3.7.b, для всякой диагональной матрицы D с более чем k нулями на главной диагонали, мы имеем $\operatorname{rk}(M+D) \geqslant \operatorname{rk} M - \operatorname{rk} D > n-(n-k) = k$.

(b) Алгоритм (b) строится с помощью (a) и леммы 2.5.b. Заметим, что алгоритм леммы 2.5.b имеет сложность $O(n^4)$. Легко видеть, что перебор всех диагональных матриц $n \times n$ с не более k нулями на главной диагонали использует

$$O\left(n\binom{n}{0} + n\binom{n}{1} + \ldots + n\binom{n}{k}\right) \overset{(*)}{=} O\left((k+1)n\binom{n}{k}\right) = O\left(n \cdot n^k\right) = O\left(n^{k+1}\right)$$

операций. Здесь равенство (*) выполняется, так как можно считать, что $n \geqslant 2k$. Таким образом, ввиду утверждения 3.6.b, сложность всего алгоритма равна $O(n^4)+O(n^{k+1}n^2) = O(n^{k+3})$ (т. к. $k \geqslant 1$).

1.4. (a) Обозначим через n число столбцов в M и в D. По лемме 3.7.b мы имеем

$$\begin{aligned} 2\operatorname{rk}(M+D) = \operatorname{rk}(M+D) + \operatorname{rk}((M+E)+(E+D)) \geqslant \\ \geqslant (\operatorname{rk} M - \operatorname{rk} D) + (\operatorname{rk}(M+E) - \operatorname{rk}(E+D)) = \\ = n - \operatorname{rk} D + \operatorname{rk}(M+E) - (n - \operatorname{rk} D) = \operatorname{rk}(M+E). \end{aligned}$$

(b) Обозначим через M_n матрицу, полученную применением алгоритма леммы 2.5.b к матрице M. Положим $k := \mathrm{rk}(M_n + E)$. Тогда $R(M) = \mathrm{rk}(M + D)$ для некоторой диагональной матрицы D. Вместе с пунктом (a) это влечёт $k/2 \leqslant R(M) \leqslant k$, что и требовалось.

Число k может быть вычислено за $O(n^3)$ операций. Таким образом, общая сложность алгоритма равна $O(n^4) + O(n^3) = O(n^4)$.

2.1. *Ответ:* Матрицы A_1, A_2, A_3 вырождены. Матрица A_4 невырождена.

2.2. Указание: в (a)-(b) выделите максимальную невырожденую подматрицу; в (c) воспользуйтесь индукцией.

Пункт (a) понятен.

Зафиксируем матрицу M.

(b) Для матрицы M' обозначим через $\mathrm{row}_{i\to i+j}M'$ модификацию матрицы M', при котором i-ая строка переходит в сумму i-ой и j-ой строки; $\mathrm{col}_{i\to i+j}M'$ определяются аналогично.

Для доказательства пункта (b) достаточно показать, что M вырождена тогда и только тогда, когда $\mathrm{row}_{i\to i+j}M$ вырождена и тогда и только тогда, когда $\mathrm{row}_{i\to i+j}M$ вырождена.

Далее, заметим, что $\mathrm{row}_{i\to i+j}\mathrm{row}_{i\to i+j}M = M = \mathrm{col}_{i\to i+j}\mathrm{col}_{i\to i+j}M$. Таким образом, достаточно показать, что если M вырождена, то и $\mathrm{row}_{i\to i+j}M$, и $\mathrm{col}_{i\to i+j}M$ вырождены.

Предположим, что сумма столбцов с номерами $c_1, c_2, \ldots, c_s$ в M равна 0. Тогда сумма столбцов с теми же номерами в $\mathrm{row}_{i\to i+j}M$ равна 0. Если $i \notin \{c_1, \ldots, c_s\}$, то сумма столбцов с теми же номерами в матрице $\mathrm{col}_{i\to i+j}M$ равна 0. Если $i, j \in \{c_1, \ldots, c_s\}$, то сумма столбцов с номерами $\{c_1, \ldots, c_s\}\backslash j$ в матрице $\mathrm{col}_{i\to i+j}M$ равна 0. Если $i \in \{c_1, \ldots, c_s\}$, $j \notin \{c_1, \ldots, c_s\}$, тогда сумма столбцов с номерами $\{c_1, \ldots, c_s\}\cup\{j\}$ в матрице $\mathrm{col}_{i\to i+j}M$ равна 0. Это доказывает (b).

(c) Мы явно покажем, как матрицу M привести к диагональному виду.

Если все элементы в матрице M равны 0, то M диагональна. Пусть в матрице M есть ненулевой элемент. Переставим строку с этим элементом с верхней строкой, и столбец с этим элементом с левым столбцом. Прибавим верхнюю строку полученной матрицы к остальным строкам с ненулевым левым элементом. Аналогично прибавим левый столбец полученной матрицы к остальным столбцам с ненулевым верхним элементом. В полученной матрице в левом столбце и верхней строке все элементы нулевые, кроме левого верхнего. Удалим из полученной матрицы верхнюю строку и левый столбец.

Повторим описанную процедуру индуктивно к полученной подматрице. В итоге M приведется к диагональной матрице.

(d) С помощью п. (c) мы можем перевести матрицу M в диагональную матрицу, пользуясь преобразованиями из п. (a,b); также матрица M вырождена тогда и только тогда, когда полученная матрица диагональна. Остается заметить, что диагональная матрица невырождена тогда и только тогда, когда она равна единичной.

(f) Следует из прямых аналогов пунктов (a)-(d) для строк.

(g) Алгоритм строится по пункту (c). У алгоритма есть n больших шагов, один из которых описан во втором абзаце решения пункта (c). Каждый большой шаг содержит не более одной перестановки строк, не более одной одной перестановки столбцов и до $2n$ прибавлений строк и столбцов. Таким образом, сложность всего алгоритма равна $O(n) + n \cdot O(n^2) = O(n^3)$.

2.3. (a) Формула справедлива, так как матрица из $\mathbb{Z}_2^{2\times 2}$ вырождена тогда и только

тогда, когда или в ней есть нулевая строка, или нулевой столбец, или в когда в ней совпадают строки и совпадают столбцы (в последнем случае все элементы матрицы единицы).

Другое решение. Ниже приведены все матрицы из $\mathbb{Z}_2^{2\times 2}$ с точностью до перестановки строк и столбцов:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix},\begin{pmatrix}1&1\\0&1\end{pmatrix},\begin{pmatrix}0&0\\0&0\end{pmatrix},\begin{pmatrix}1&1\\1&1\end{pmatrix},\begin{pmatrix}1&1\\0&0\end{pmatrix},\begin{pmatrix}1&0\\1&0\end{pmatrix},\begin{pmatrix}1&0\\0&0\end{pmatrix}.$$

Первые две матрицы невырождены, в то время как оставшиеся вырождены. Легко проверить формулу на данных матрицах.

(d) Следует из пунктов (b,c).

Далее приводим альтернативное прямое решение.

Рассмотрим шахматную доску размера $n\times n$. *Правильной расстановкой ладей* для данной шахматной доски называется такая расстановка n ладей на доске, что они не бьют друг друга. *Правильной M-расстановкой ладей* для данной шахматной доски называется такая правильная расстановка ладей, что все ладьи стоят на клетках, отвечающих единичным элементам матрицы M.

Обозначим через $\det^* M$ чётность числа правильных M-расстановок ладей. Тогда (d) можно переформулировать так: $\det M = \det^* M$. Равенство следует из того, что

- преобразования из 2.2.a, 2.2.b сохраняют $\det^* M$ и
- $\det M' = \det^* M'$ для диагональной матрицы M'.

2.4. Для любой невырожденной матрицы из задачи 2.1 мы показали, как поменять элементы на главной диагонали, что бы сделать её невырожденной; покажем обратное для A_4:

$$A_1 \to \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix},\quad A_2, A_3 \to \begin{pmatrix}0&1&1\\1&0&1\\1&1&1\end{pmatrix},\quad A_4 \to \begin{pmatrix}0&1&1\\0&1&1\\1&0&0\end{pmatrix}.$$

2.5. (a) В следующем абзаце мы докажем индукцией по $i \geqslant 1$, что определитель $\Delta_i := \det M^{(i)}_{[i]\times[i]}$ левой верхней $i\times i$-угловой подматрицы матрицы $M^{(i)}$ равен 1. Таким образом, $\det M^{(n)} = \Delta_n = 1$.

База $i = 1$ выполняется, поскольку $\Delta_1 = 1+\delta_0 = 1$. Докажем шаг индукции $i-1 \to i$. Применим формулу разложения определителя Δ_i по последней строке соответствующей подматрицы матрицы $M^{(i)}$ (утверждение 2.3.c). Поскольку $M^{(i-1)}_{i,i} = M_{i,i} = 0$ и $\Delta_{i-1} = 1$, мы получаем $\Delta_i = \delta_i + (1+\delta_i)\Delta_{i-1} = 1$.

(b) Алгоритм строится по пункту (a). Алгоритм по сути является вычислением определителей n квадратных подматриц размеров $1, 2, \ldots, n$. Значит, по утверждению 2.2.g его сложность равна $O(1^3 + 2^3 + \ldots + n^3) = O(n\cdot n^3) = O(n^4)$.

3.1. *Ответы:* (a1) 0; (a2) 1; (a3), (a4) 3; (b1) 0; (b2), (b3) 1; (b4) 2.

3.2 Указание к пункту (b): найдите число различных сумм из k столбцов.

Пункт (a) следует из определения ранга матрицы.

(b) По определению ранга, число различных сумм из столбцов матрицы M равно $2^{\operatorname{rk} M}$. С другой стороны, число таких сумм не превосходит 2^k. Следовательно, $2^k \geqslant 2^{\operatorname{rk} M}$ и $k \geqslant \operatorname{rk} M$.

3.3. Доказательства пунктов (a), (b) аналогичны доказательствам пунктов 2.2.a,b.

3.4. Пункт (a) ясен.

(b) Если для ненулевой симметричной матрицы M существует такая перестановка столбцов и строк, то $\operatorname{rk} M = 1$ по утверждению 3.2.b.

Возьмём симметричную матрицу M ранга 1. В качестве требуемой перестановки можно взять любую перестановку, отображающую ненулевые строки матрицы M в первую строку. Действительно, возьмём любые ненулевые строки с номерами i, j. Если $M_{i,j} = 0$, то существует такая ненулевая строка с номером k, для которой $M_{i,k} = 1$. Тогда строки с номерами j и k являются различными ненулевыми строками матрицы M ранга 1. Противоречие. Следовательно, $M_{i,j} = 1$.

(c) Возьмите ненулевые строки и примените аргументы из предыдущего пункта.

3.5. (a) $R\begin{pmatrix}1&0&1\\0&0&1\\0&1&0\end{pmatrix} = 2, \quad R\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} = 1.$

(b) $R\begin{pmatrix}1&0&1\\0&1&1\\0&1&0\end{pmatrix} = 2, \quad R\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} = 1.$

3.6. Подсказка к пункту (a): см. утверждение 2.2.

(a) Алгоритм из доказательства утверждения 2.2.c обеспечивает диагональную матрицу того же ранга и имеет требуемую сложность. Ранг диагональной матрицы равен количеству ненулевых элементов в ней.

(b) Нужно построить такое множество S_k из столбцов, что

• эти столбцы составляют невырожденную подматрицу;

• первые k столбцов матрицы M являются суммами некоторых столбцов из множества S_k.

Если $|S_k| > r$ для некоторого $k = 1, \ldots, n$, то ответ «нет». Если для любого $k = 1, \ldots, n$ справедливо неравенство $|S_k| \leqslant r$, то ответ «да».

Ответ корректен, так как $|S_1| \leqslant |S_2| \leqslant \ldots \leqslant |S_n|$, и $|S_n| > r$ равносильно неравенству $\operatorname{rk} M > r$.

Положим $S_1 := \varnothing$, если первый столбец матрицы M равен 0, и $S_1 := \{1\}$ иначе.

Определим S_{k+1} по S_k. Составим множество всех сумм столбцов матрицы M с индексами из S_k (требуется $O(n)$ операций, так как $|S_k| \leqslant r$). Затем сравним $(k+1)$-ый столбец матрицы M со всеми суммами из этого множества (на это потребуется не более $2^r O(n) = O(n)$ операций). Если $(k+1)$-ый столбец матрицы M равен хотя бы одной сумме, то $S_{k+1} := S_k$. Иначе $S_{k+1} := S_k \cup \{k+1\}$.

Легко проверить, что общая сложность алгоритма равна $O(n^2)$.

3.7. Пункт (b) следует из пункта (a), поскольку

$$\operatorname{rk} M = \operatorname{rk}(M + D + D) \leqslant \operatorname{rk}(M + D) + \operatorname{rk} D \implies \operatorname{rk}(M + D) \geqslant \operatorname{rk} M - \operatorname{rk} D.$$

Теперь мы докажем пункт (a). Выберем столбцы из утверждения 3.2.a для матрицы M и матрицы D. Тогда каждый столбец матрицы $M + D$ является суммой нескольких из выбранных $\operatorname{rk} M + \operatorname{rk} D$ столбцов. По утверждению 3.2.b $\operatorname{rk}(M + D) \leqslant \operatorname{rk} M + \operatorname{rk} D$.

3.8. Утверждение и доказательство утверждения 3.8 аналогичны утверждению и доказательству теоремы 1.3.b.

3.9. Ответ: нет. Для матрицы M ниже и $k = 1$ утверждение неверно.

$$\begin{pmatrix}0&1&1\\1&0&1\\1&1&0\end{pmatrix}$$

3.10. *Ответы:* (a) 1; (b) $(2^n-1)^2$; (c) $(2^n-1)^2(2^n-2)^2/6$.

(a) Существует ровно одна матрица ранга 0: матрица, у которой все элементы нулевые.

(b) Для матрица ранга 1 все столбцы, содержащие ненулевой элемент, совпадают. Следовательно, такие матрицы находятся во взаимно однозначном соответствии с упорядоченными парами, образованными

- непустым подмножеством множества столбцов («ненулевые столбцы»), и
- ненулевым вектором $v \in \mathbb{Z}_2^n$ («вектор-столбец»).

Поэтому существуют $(2^n-1)^2$ таких матриц.

(c) Зафиксируем матрицу M ранга 2. Тогда существует пара (v, w) столбцов матрицы M, образующих невырожденную матрицу. Любой другой столбец — это либо 0, либо v, либо w, либо $v+w$ (см. утверждение 3.2). Это множество $S = S_M$ из четырёх векторов не зависит от выбора двух столбцов v, w; мы назовем его *оболочкой столбцов* матрицы M. (Оно является двумерным векторным подпространством в $\mathbb{Z}_2^n$.)

Каждая оболочка столбцов определяется любой упорядоченной парой векторов в ней. Любая оболочка столбцов содержит ровно 6 таких упорядоченных пар. Значит, всего существует $(2^n-1)(2^n-2)/6$ оболочек столбцов. Мы докажем, что существуют ровно $(2^n-1)(2^n-2)$ матриц ранга 2 для данной оболочки столбцов. Таким образом, существует $(2^n-1)^2(2^n-2)^2/6$ матриц ранга 2.

Первое доказательство. Сопоставим матрице M два множества — множество столбцов X матрицы M, которые равны v или $v+w$, и множество столбцов Y матрицы M, которые равны w или $v+w$. Из условия $\operatorname{rk} M = 2$ следует, что оба множества должны быть непустыми и $X \neq Y$. Более того, саму матрицу M по паре (X, Y) множеств можно восстановить. Пар (X, Y) различных непустых множеств ровно $(2^n-1)(2^n-2)$.

Второе доказательство. Для данного 4-элементного множества $S = \{0, v, w, v+w\}$ рассмотрим матрицу M, оболочкой столбцов которой является S. Рассмотрим матрицу M в качестве отображения ϕ_M из множества $[n]$ столбцов в S. Условие $\operatorname{rk} M = 2$ равносильно следующему условию:

(*) образ отображения ϕ_M содержит по крайней мере два вектора из $v, w, v+w$.

Существует всего 4^n отображений $[n] \to S$. Существует всего 2^n отображений $[n] \to \{0, v\}$. То же самое верно для пары $\{0, v\}$, заменённой на $\{0, w\}$ или $\{0, v+w\}$. Есть лишь одно отображение $[n] \to \{0\}$. Значит, существуют ровно $4^n - 3 \cdot 2^n + 2 = (2^n-1)(2^n-2)$ отображений, удовлетворяющих условию (*).

Замечание. Вообще, количесто матриц ранга k из $\mathbb{Z}_2^{m\times n}$ равно

$$\frac{2^{k(k-1)/2}\Pi_{i=0}^{k-1}(2^{m-i}-1)\Pi_{i=0}^{k-1}(2^{n-i}-1)}{\Pi_{i=0}^{k-1}(2^{k-i}-1)}.$$

См. теорему 7.1.5 в [ACM29, p. 299] (эта теорема ещё более общая; для нашего случая матриц над $\mathbb{Z}_2$ возьмите $q = 2$, $\mathrm{GF}(2) = \mathbb{Z}_2$).

4.1. (a1-a3) Изящная реализация графа K_5 на торе показана на рис. 4, слева. Реализации графов K_6 и K_7 аналогичны, см. рис. 4, в центре.

Другое решение (эта идея также работает для (c, d)): нарисуйте граф K_5 на плоскости с *одним* самопересечением, в малой окрестности точки самопересечения прикрепите ручку, а потом поднимите одно из рёбер как мост над другим ребром, проведя его по ручке, см. рис. 5, слева.

(b2) См. рис. 4, справа.

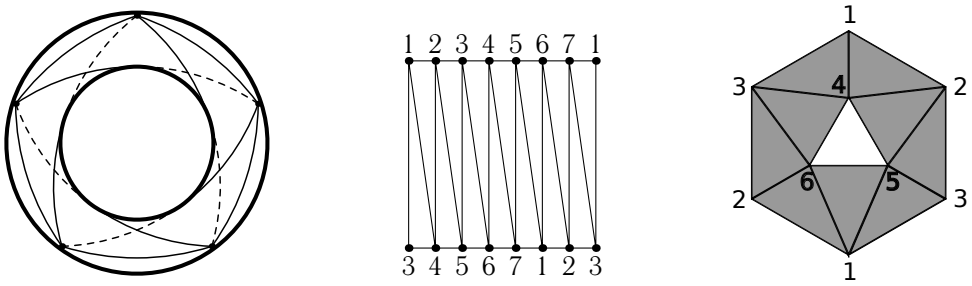


Рис. 4: Реализация непланарных графов

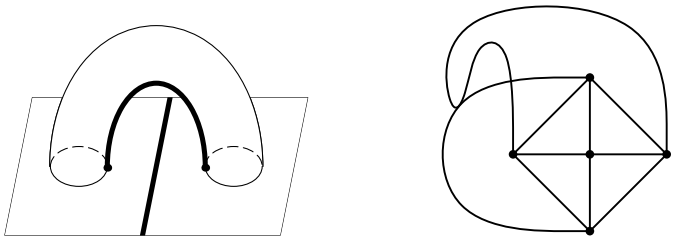


Рис. 5: Слева: разрешение самопересечения добавлением ручки. Справа: «чётная не общего положения реализация» графа K_5 на плоскости

4.2. См. рис. 5, справа.

5.1. (b) Индукция по m. База $m \leqslant 4$ очевидна. Из предложения 5.7.b и предположения индукции получаем

$$\widetilde{r_m} \geqslant \widetilde{r_{m-5}} + 2 \geqslant \frac{2(m-5-4)}{5} + 2 = \frac{2(m-4)}{5}.$$

(a) Индукция по m. База $m \leqslant 4$ очевидна. Из предложения 5.7.a, теоремы 5.1.b и предположения индукции получаем

$$r_m \geqslant \min\{r_{m-3}+1, \widetilde{r_m}\} \geqslant \min\left\{\frac{m-3-4}{3}+1, \frac{2(m-4)}{5}\right\} = \frac{m-4}{3}.$$

5.3. Через A^f обозначим $\binom{[m]}{3}$-матрицу, построенную по вложению $f\colon K_m \to S$, как описано в начале §5.

(a) Рассмотрим подграф K_4 на вершинах $1,2,3,4$ графа K_5. Рис. 3 справа задает вложение f графа K_4 в тор. Матрица A^f — искомая.

(b) Рис. 3 справа задает вложение f графа K_5 в тор. Матрица A^f — искомая.

(c) По утверждению 4.1.d, существует вложение f графа K_m в сферу с ручками. Матрица A^f — искомая.

(a', b', c') Матрицы из пунктов (a), (b) и (c) — искомые.

(d, e, f) Следуют из задач 5.6.a,b.

5.4. Следует из определений $\binom{[m]}{3}$-матрицы и $\binom{[m-1]}{3}$-матрицы.

5.5. (a, b) См. доказательство предложений 7.4.a,b ниже.

5.6. (a) Так как $\binom{[m]}{3}$-матрица для $m \geqslant 5$ невырождена, то $r_5, r_6 \geqslant 1$. Значения $r_5 = r_6 = 1$ достигаются на матрицах A^f для f из утверждения 4.1.b1, b2.

(b) Из утверждения 3.4.c следует, что $\widetilde{r_5}, \widetilde{r_6}, \widetilde{r_7} \geqslant 2$. Значения $\widetilde{r_5} = \widetilde{r_6} = \widetilde{r_7} = 2$ достигаются на матрицах A^f для f из утверждений 4.1.a1, a2, a3.

(c) Для $\binom{[m]}{3}$-матрицы A её $\binom{[m-1]}{3}$-подматрица B, введённая в утверждении 5.4, имеет такой же ранг, или меньший. Следовательно, $r_m \geqslant r_{m-1}$. Если матрица A чётная, то и матрица B чётная. Следовательно, $\widetilde{r_m} \geqslant \widetilde{r_{m-1}}$.

5.7. (a) (Take $l = 3$.) Take an $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = r_m$. If A is even, then $r_m = \widetilde{r_m}$, so we are done. Otherwise there is an l-element subset $X \subset [m]$ such that $A_{X,X} = 1$. Let B be the 'restriction' of A to l-element subsets of $[m] - X$.

Then

$$r_m = \operatorname{rk} A \geqslant \operatorname{rk} B + 1 \geqslant r_{m-l} + 1, \quad \text{where}$$

- the first inequality follows by Assertion 5.5.a;
- the second inequality holds because B is a $\binom{[m]-X}{l}$-matrix by Assertion 5.4.

(b) (Take $l = 3$.) Take an even $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = \widetilde{r_m}$. By the non-triviality $A \neq 0$. Hence there are l-element subsets $X, Y \subset [m]$ such that $A_{X,Y} = 1$. Let C be the 'restriction' of A to l-element subsets of $[m] - X - Y$.

Then

$$\widetilde{r_m} = \operatorname{rk} A \geqslant \operatorname{rk} C + 2 \geqslant \widetilde{r_{m-2l+1}} + 2, \quad \text{where}$$

- the first inequality follows by Assertion 5.5.b;
- the second inequality holds because C is a $\binom{[m]-X-Y}{l}$-matrix by Assertion 5.4, and because $A_{X,Y} = 1$, so by the triviality $X \cap Y \neq \varnothing$, hence $|[m] - X - Y| \geqslant m - 2l + 1$.

6.7. (a) $\lambda_{X,P} = X \cdot_A P$.

6.8. (a) $\lambda_{X,Y,P} = X \cdot_A P$, $\lambda_{Y,X,P} = Y \cdot_A P$.

7.2. (For 5.4 take $l = 3$.) It is obvious that all the conditions for the mentioned submatrix are satisfied.

7.3. (a) (For 5.5.a take $l = 3$.) Let B' be the 'restriction' of A to X and to l-element subsets of $[m] - X$. Then

$$\operatorname{rk} A \geqslant \operatorname{rk} B' = \operatorname{rk} B + 1,$$

where equality holds because by the triviality $B'_{X,Z} = 0$ for any $Z \subset [m] - X$.

(b) (For 5.5.b take $l = 3$.) Let C' be the 'restriction' of A to X, Y and l-element subsets of $[m] - X - Y$. Then

$$\operatorname{rk} A \geqslant \operatorname{rk} C' = \operatorname{rk} C + 2,$$

where equality holds because by the triviality $C'_{X,Z} = C'_{Y,Z} = 0$ for any $Z \subset [m] - X - Y$.

(b') Take a basis of $\mathbb{Z}_2^{\binom{m}{l}}$ corresponding to l-element subsets of $[m]$. Define a bilinear form A on $\mathbb{Z}_2^{\binom{m}{l}}$ by setting $A(P, Q) := A_{P,Q}$ for basic vectors P, Q. Take any l-element set $P \subset [m]$. Let

$$\overline{P} = \overline{P}(X, Y) := P + A_{X,P}Y + A_{Y,P}X.$$

Recall that

$$A_{X,Y} = A_{Y,X} = 1 \quad \text{and} \quad A_{X,X} = A_{Y,Y} = 0. \tag{*}$$

Hence

$$A(\overline{P}, X) = A(\overline{P}, Y) = 0 \tag{**}$$

(i. e., $\overline{P}$ is the orthogonal projection of P to the orthogonal complement of $\langle X, Y\rangle$ with respect to A). By the triviality, for $P \subset [m] - X$ we have $\overline{P} = P + A_{Y,P}X$. Hence for every l-element sets $P, Q \subset [m] - X$ we have

$$A(\overline{P}, \overline{Q}) = A_{P,Q} + 0 + 0 + 0 = B_{P,Q}. \tag{***}$$

(I. e., B is the Gramian matrix with respect to A of the 'projections' $\overline{P}$ of l-element sets $P \subset [m]-X$.) Let B' be the Gramian matrix with respect to A of X, Y and the 'projections' $\overline{R}$ of l-element sets $R \subset [m] - X$. I. e., $B'_{P,Q} = A(\widehat{P}, \widehat{Q})$, where $\widehat{P} = P$ if $P \in \{X, Y\}$, and $\widehat{P} = \overline{P}$ otherwise ($\widehat{Q}$ is defined analogously). Then

- $B'_{X,Y} = B'_{Y,X} = 1$, $B'_{X,X} = B'_{Y,Y} = 0$ (by (*)),
- $B'_{X,P} = B'_{P,X} = B'_{Y,P} = B'_{P,Y} = 0$ for $P \neq X, Y$ (by (**)), and
- $B'_{P,Q} = B_{P,Q}$ for $P, Q \subset [m] - X$ (by (***)).

Hence $\operatorname{rk} B + 2 = \operatorname{rk} B' \leqslant \operatorname{rk} A$.

(a') In this paragraph we prove that $\operatorname{rk} D < \operatorname{rk} A$. Take a basis of $\mathbb{Z}_2^{\binom{m}{l}}$ corresponding to l-element subsets of $[m]$. Define a bilinear form A on $\mathbb{Z}_2^{\binom{m}{l}}$ by setting $A(P, Q) := A_{P,Q}$ for basic vectors P, Q. Let P_X be the orthogonal projection of P to the orthogonal complement of X (with respect to A), i. e., $P_X := P + A_{P,X}X$. We have

$$A(P_X, Q_X) = A(P, Q) + A(A_{P,X}X, Q) + A(P, A_{Q,X}X) + A(A_{P,X}X, A_{Q,X}X) =$$
$$= A_{P,Q} + A_{P,X}A_{X,Q} + A_{P,X}A_{Q,X} + A_{P,X}A_{Q,X}A_{X,X} = A_{P,Q} + A_{P,X}A_{Q,X} = D_{P,Q}.$$

Then D is the Gramian matrix (with respect to A) of the projections of subsets of $[m-l+1]$. Let D' be the Gramian matrix (with respect to A) of X and the projections of subsets of $[m - l + 1]$. We have $D_{P,Q} = D'_{P,Q}$ for all subsets $P, Q \subset [m - l + 1]$. Furthermore, $D'_{X,P} = D'_{P,X} = 0$ for any basic vector $P \neq X$ and $D'_{X,X} = A_{X,X} = 1$. Thus $\operatorname{rk} D = \operatorname{rk} D' - 1 < \operatorname{rk} A$.

In this paragraph we prove that D satisfies the triviality property. If $P \cap Q = \varnothing$, then either $P \cap X = \varnothing$, or $Q \cap X = \varnothing$. Hence $D_{P,Q} = A_{P,Q} + A_{P,X}A_{Q,X} = 0 + 0 = 0$.

In this paragraph we prove that D satisfies the linear dependence property. For each $(l + 1)$-element and l-element subsets $F, P \subset [m - l + 1]$ we have

$$\sum_{i \in F} D_{F-i,P} = \sum_{i \in F} A_{F-i,P} + A_{P,X} \sum_{i \in F} A_{F-i,X} = 0.$$

In this paragraph we prove that D satisfies the non-triviality property. By Proposition 7.5.b for D, we may assume that $i \neq m - l + 1$. Then for each summand $D_{i \sqcup \sigma, i \sqcup \tau}$ of $D_{F,i}$ at least one of the sets $i \sqcup \sigma, i \sqcup \tau$ does not contain $m - l + 1$ and hence does not intersect X. Hence $D_{i \sqcup \sigma, i \sqcup \tau} = A_{i \sqcup \sigma, i \sqcup \tau} + A_{i \sqcup \sigma, X}A_{i \sqcup \tau, X} = A_{i \sqcup \sigma, i \sqcup \tau}$. Thus $D_{F,i} = A_{F,i} = 1$.

7.4. (a) Take an $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = r_m$. If A is even, then $r_m = \widetilde{r_m}$, so we are done. Otherwise there is an l-element subset $X \subset [m]$ such that $A_{X,X} = 1$. Without loss of generality $X = \{m - l + 1, m - l + 2, \ldots, m\}$. Then by Assertion 7.3.a'

$$r_m = \operatorname{rk} A \geqslant \operatorname{rk} D + 1 \geqslant r_{m-l+1} + 1, \quad \text{where}$$

- D is the matrix defined in Assertion 7.3.a';
- the first inequality follows from Assertion 7.3.a';
- the second inequality holds because D is an $\binom{[m-l+1]}{l}$-matrix by Assertion 7.3.a'.

(b) Take an even $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = \widetilde{r_m}$. By the non-triviality $A \neq 0$. Let X, Y, B be defined as in Assertion 7.3.b'. Then

$$\widetilde{r_m} = \operatorname{rk} A \geqslant \operatorname{rk} B + 2 \geqslant r_{m-l} + 2, \quad \text{where}$$

- the first inequality follows from Assertion 7.3.b';

• the second inequality holds because B is an even $\binom{[m]-X}{l}$-matrix by Assertion 7.2.

7.5. (a) It suffices to check that for each pair $\{\alpha,\beta\}$ the number of sets $T_{i,\{\sigma,\tau\}}$ containing $\{\alpha,\beta\}$ is odd if and only if $\alpha\cap\beta=\varnothing$ (hence this parity not depend on i). Clearly, $|\alpha\cap\beta|\leqslant 2$.

Assume $|\alpha\cap\beta|=2$. Then $\{\alpha,\beta\}\notin T_{i,\{\sigma,\tau\}}$ for all i,σ,τ and hence $\{\alpha,\beta\}\notin A_i$ for all $i\in[5]$.

Assume $|\alpha\cap\beta|=1$. It suffices to consider the case $\alpha=\{1,2\}$, $\beta=\{1,3\}$. Then $\{\alpha,\beta\}\in T_{i,\{\sigma,\tau\}}$ iff $i=1$ and $\{\sigma,\tau\}$ is either $\big\{\{2,4\},\{3,5\}\big\}$ or $\big\{\{2,5\},\{3,4\}\big\}$ Therefore $\{\alpha,\beta\}\notin A_i$ for all $i\in[5]$.

Assume $|\alpha\cap\beta|=0$. It suffices to consider the case $\alpha=\{1,2\}$, $\beta=\{3,4\}$. Then $\{\alpha,\beta\}\in T_{i,\{\sigma,\tau\}}$ iff either

• $i=1$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{1,3,4\}\big\}$, or
• $i=2$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{2,3,4\}\big\}$, or
• $i=3$ and $\{\sigma,\tau\}=\big\{\{1,2,3\},\{3,4,5\}\big\}$, or
• $i=4$ and $\{\sigma,\tau\}=\big\{\{1,2,4\},\{3,4,5\}\big\}$, or
• $i=5$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{3,4,5\}\big\}$.

Therefore $\{\alpha,\beta\}\in A_i$ for every $i\in[5]$.

(b) It suffices to prove that $A_{G\sqcup i,j}=A_{G\sqcup j,i}$ for each $i,j\in[m]$ and $(2l-3)$-element subset $G\subset[m]-i-j$. Denote $\overline{\sigma}:=\{i,j\}\sqcup\sigma$. Then

$$A_{G\sqcup j,i}+A_{G\sqcup i,j}\overset{(1)}{=}\sum_{\{(\sigma,\tau)\,:\,G=\sigma\sqcup\tau,\ |\sigma|=l-2\}}(A_{\overline{\sigma},i\sqcup\tau}+A_{\overline{\sigma},j\sqcup\tau})\overset{(2)}{=}$$

$$=\sum_{\{(\sigma,\tau)\,:\,G=\sigma\sqcup\tau,\ |\sigma|=l-2\}}\ \sum_{t\in\tau}A_{\overline{\sigma},\overline{\tau-t}}\overset{(3)}{=}\sum_{t\in G}\ \sum_{\{(\sigma,\nu)\,:\,G-t=\sigma\sqcup\nu,\ |\sigma|=l-2\}}A_{\overline{\sigma},\overline{\nu}}\overset{(4)}{=}0,\quad\text{where}$$

• equality (1) holds because $A_{G\sqcup j,i}$ is equal to the sum of the first summands $A_{\overline{\sigma},i\sqcup\tau}$, and $A_{G\sqcup i,j}$ is equal to the sum of the second summands $A_{\overline{\sigma},j\sqcup\tau}$;
• equality (2) holds by the linear dependence for $F=\overline{\tau}$, $P=\overline{\sigma}$;
• equality (3) is obtained by changes of the order of summation and of variable $\nu=\tau-t$;
• equality (4) holds because ordered decompositions (σ,ν) of $G-t$ into $(l-2)$-element subsets σ,ν split into pairs $\{(\sigma,\nu),(\nu,\sigma)\}$ and $A_{\overline{\sigma},\overline{\nu}}+A_{\overline{\nu},\overline{\sigma}}=0$.

Список литературы

[ACM29] *D. Hachenberger, D. Jungnickel.* Topics in Galois Fields (2020).

[Bi20] * *А. Бикеев.* Реализуемость дисков с ленточками на ленте Мёбиуса. Математическое просвещение. Сер. 3. Вып.28. 2021. С 150-158. Исправления в печати. arXiv:2010.15833.

[Bi21] *A. I. Bikeev,* Criteria for integer and modulo 2 embeddability of graphs to surfaces, arXiv:2012.12070v2.

[DS22] *S. Dzhenzher and A. Skopenkov,* To the Kühnel conjecture on embeddability of k-complexes into $2k$-manifolds, arXiv:2208.04188.

[FK19] *R. Fulek, J. Kynčl,* $\mathbb{Z}_2$-genus of graphs and minimum rank of partial symmetric matrices, 35th Intern. Symp. on Comp. Geom. (SoCG 2019), Article

No. 39; pp. 39:1–39:16, https://drops.dagstuhl.de/opus/volltexte/2019/10443/pdf/LIPIcs-SoCG-2019-39.pdf. We refer to numbering in arXiv version: arXiv:1903.08637.

[IF] * http://www.map.mpim-bonn.mpg.de/Intersection_form

[Ko21] *E. Kogan.* On the rank of $\mathbb{Z}_2$-matrices with free entries on the diagonal, arXiv:2104.10668.

[KS21] * *E. Kogan and A. Skopenkov.* A short exposition of the Patak-Tancer theorem on non-embeddability of k-complexes in $2k$-manifolds, arXiv:2106.14010.

[KS21e] *E. Kogan and A. Skopenkov.* Embeddings of k-complexes in $2k$-manifolds and minimum rank of partial symmetric matrices, arXiv:2112.06636.

[MC] https://en.wikipedia.org/wiki/Matrix_completion#Low_rank_matrix_completion

[NKS] *L. T. Nguyen, J. Kim, B. Shim.* Low-rank matrix completion: a contemporary survey. arXiv:1907.11705

[PT19] *P. Paták and M. Tancer.* Embeddings of k-complexes into $2k$-manifolds. arXiv:1904.02404.

[Sk14] * *A. Skopenkov,* Realizability of hypergraphs and Ramsey link theory, arXiv:1402.0658.

[Sk20] * *А. Скопенков,* Алгебраическая топология с геометрической точки зрения, МЦНМО, Москва, 2020 (2ое издание).
Фрагмент книги: http://www.mccme.ru/circles/oim/obstruct.pdf. Фрагмент английской версии:
https://www.mccme.ru/circles/oim/obstructeng.pdf.

Low rank matrix completion

presented by S. Dzhenzher, T. Garaev, O. Nikitenko,
A. Petukhov, A. Skopenkov, A. Voropaev*

Contents

1 Motivation and some main results 1

2 Degenerate matrices 4

3 The rank of a matrix 5

4 Modulo 2 embeddings of graphs to surfaces 6

5 Rank of matrix with relations 9

6 Classification of symmetric bilinear forms 10

7 Rank of matrix with relations: generalization 12

1 Motivation and some main results

Remark (motivation; formally is not used later)

'Matrix completion is the task of filling in the missing entries of a partially observed matrix... One example is the movie-ratings matrix, as appears in the Netflix problem: Given a ratings matrix in which each entry (i, j) represents the rating of movie j by customer i, if customer i has watched movie j and is otherwise missing, we would like to predict the remaining entries in order to make good recommendations to customers on what to watch next...' [MC] The remaining entries are predicted so as to minimize the *rank* of the completed matrix. All the required definitions (of rank etc.) are given below. For a brief overview of the history of this and related problems, see [MC, NKS], [Ko21, Remark 4].

Here for simplicity we consider matrices with entries in the set $\mathbb{Z}_2 = \{0, 1\}$ of all residues modulo 2 (with the sum and product operations). We present interesting elementary results in linear algebra. These results allow us to construct algorithms estimating minimal rank of partial matrices for the particular case of filling the diagonal (Proposition 1.1 and Theorems

S. Dzhenzher, A. Skopenkov: Moscow Institute of Physics and Technology. *T. Garaev:* Moscow State University. *O. Nikitenko:* Altay Technical University (Barnaul). *A. Petukhov:* Institute for Information Transmission Problems (Moscow). *A. Skopenkov:* Independent University of Moscow, https://users.mccme.ru/skopenko/. *A. Voropaev:* (Moscow).

We are grateful to E. Kogan for allowing us to use his text [Ko21], to V. Retinskiy and Ya. Abramov for useful discussions, to D. Deomidov and F. Nilov for translating parts of the text, to A. Ryabichev and MCCME publishing house for allowing us to use figures they prepared.

1.3, 1.4, see also Proposition 1.2). Then we consider a more complicated problem. Instead of relations $M_{ij} = a_{ij}$ for some elements M_{ij} of matrix M (where a_{ij} are given numbers) we consider more complicated relations on matrix elements. We estimate minimal rank of matrices with such relations (Theorems 5.1, 7.1.)

These results have applications to embeddings of graphs in surfaces (including embedding modulo 2, see §4), and of k-dimensional 'hypergraphs' to $2k$-dimensional surfaces, see [KS21, KS21e, DS22]. In particular, Theorems 1.3 and 1.4 give polynomial (in the number of edges) algorithms recognizing 'weak realizability' of 'graphs with rotations' on non-orientable surfaces (see the remark on weak realizability below).

Denote by $\mathbb{Z}_2^{s\times n} = (\mathbb{Z}_2^s)^n$ the set of all $s \times n$ matrices with entries in $\mathbb{Z}_2$.

Proposition 1.1. *(a) For a symmetric matrix with $\mathbb{Z}_2$-entries the following conditions are equivalent:*

- *some entries on the main diagonal can be changed so that in the resulting matrix all non-zero rows are equal;*
- *it is impossible to make the same permutation of rows and of columns*[1] *so that the upper left square will be one of the submatrices*

$$\begin{pmatrix} * & 1 & 1 \\ 1 & * & 0 \\ 1 & 0 & * \end{pmatrix} \quad \text{or} \quad \begin{pmatrix} * & 1 & 0 & 0 \\ 1 & * & 0 & 0 \\ 0 & 0 & * & 1 \\ 0 & 0 & 1 & * \end{pmatrix},$$

*where by * are denoted arbitrary (possibly different) elements.*

(b) There is an algorithm with the complexity of $O(n^2)$ deciding for a matrix $M \in \mathbb{Z}_2^{n\times n}$ whether some entries on the main diagonal can be changed so that in the resulting matrix all non-zero rows are equal.

You can submit separately your solution of the 'only if' implication of part (a).

The algorithmic results in this text could be omitted by theoretically-minded students because they are easy corollaries of mathematical results. The *complexity* of an algorithm is the number 'elementary' steps in this algorithm. An algorithm has complexity $O(f(n))$ if there is $C > 0$ such that the complexity does not exceed $Cf(n)$ for any n.

A square matrix $M \in \mathbb{Z}_2^{n\times n}$ is called **degenerate** if the sum of its several columns (a non-zero number of columns) is the zero column (i. e., the column consisting of zeros only). A matrix is called **non-degenerate** otherwise. Introductory problems on degenerate matrices useful for the following result are presented in §2.

Proposition 1.2. *(a) For any matrix $M \in \mathbb{Z}_2^{n\times n}$ some entries on the main diagonal can be changed so that the resulting matrix would be degenerate.*

(b) The same with 'degenerate' replaced by 'non-degenerate'.

The **rank** $\operatorname{rk} M$ of a matrix $M \in \mathbb{Z}_2^{s\times n}$ is the maximal number of columns of M none of whose sums is zero. (This is the 'dimension' of the 'vector space' formed by the columns of the matrix.) Introductory problems on rank useful for the following results are presented in §3.

For a matrix $M \in \mathbb{Z}_2^{n\times n}$ let $R(M)$ be the minimal rank of all the matrices obtained by changing some entries on the main diagonal of M.

A matrix is said to be **diagonal** if all its entries outside of the main diagonal are zeros.

[1] This means that the rows and columns are numbered by $1, \dots, n$ (where $n = 3, 4$) and the permutation of the set $[n]$ is applied both to the rows and to the columns.

Theorem 1.3. *(a') To make a square matrix of rank k out of a square matrix of rank n by changing some diagonal entries, one needs to change at least $|n-k|$ entries.*

(a) For any non-degenerate matrix $M \in \mathbb{Z}_2^{n\times n}$ the inequality $R(M) \le k$ is equivalent to the existence of a diagonal matrix D with at most k zeroes on the main diagonal such that $\operatorname{rk}(M+D) \le k$.

(b) For any fixed k there is an algorithm with the complexity of $O(n^{k+3})$ deciding for a matrix $M \in \mathbb{Z}_2^{n\times n}$ whether $R(M) \le k$.

The **identity matrix** E is the diagonal matrix whose diagonal elements are units.

Theorem 1.4. *(a) For any non-degenerate matrix $M \in \mathbb{Z}_2^{n\times n}$ and diagonal matrix $D \in \mathbb{Z}_2^{n\times n}$ we have $2\operatorname{rk}(M+D) \ge \operatorname{rk}(M+E)$.*

(b) There is an algorithm with the complexity of $O(n^4)$ calculating for a matrix $M \in \mathbb{Z}_2^{n\times n}$ a number k such that $k/2 \le R(M) \le k$.

Remark (weak realizability; formally is not used later)

A *hieroglyph* on n letters is an unoriented cyclic letter sequence of length $2n$ such that each letter from the sequence appears in the sequence twice.

Take a hieroglyph on n letters. Take a convex polygon with $2n$ sides. Put the letters in the hieroglyph on the sides of the convex polygon in the nonoriented cyclic order. For each letter glue the ends of a ribbon to the pair of sides corresponding to the letter so that the glued ribbons are pairwise disjoint. The ribbons can be either twisted or not twisted. Call the resulting surface a *disk with ribbons* corresponding to the hieroglyph (see Figure 1).

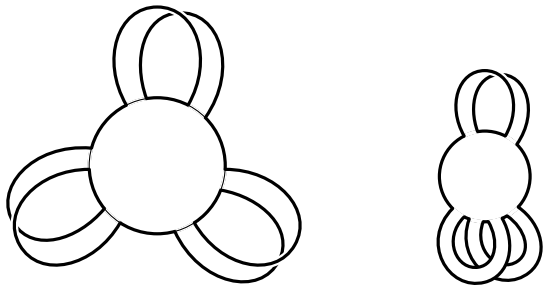


Figure 1: Disk with ribbons corresponding to the hieroglyph *aabbcc* (left) and *aabcbc* (right)

A hieroglyph H is called *weakly realizable* on the Möbius band if some disk with ribbons corresponding to H can be cut out of the Möbius band. Analogously one defines weak realizability on the Klein bottle and other non-orientable surfaces.

Two letters a, b in a hieroglyph H *overlap in* H if they interlace in the cyclic sequence of the hieroglyph (i. e., if they appear in the sequence in the order *abab* but not *aabb*). Define the *overlap matrix* $M(H) \in \mathbb{Z}_2^{n\times n}$ of a hieroglyph H as follows. Put zeros on the main diagonal. Put 1 in the cell (i,j) for $i \ne j$ if the letters i, j overlap in H, and put 0 otherwise.

Hieroglyph H is weakly realizable on the Möbius band if and only if $R(M(H)) \le 1$.

See more in [Bi20], [Ko21, Appendix], [Sk20, §2].

Recommendations for participants

If a mathematical statement is formulated as a problem, then the objective is to prove this statement. (Open-ended questions are called challenges or 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, 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. *Remarks* and problems marked by star are not used in the sequel. Important definitions are highlighted in **bold** for easy navigation. You are welcomed to *consult* the jury on any questions on the project. If you successfully work on the project, you can get interesting *extra problems*.

For every solution **written for a user** marked with either '+' or '+.' a student (or a group of students) gets a 'bean' (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 participant (or team) initially has 1 bean. You may submit a solution **in oral form** or as **written for a developer**; you lose a bean with every 5 attempts (successful or not).

Please notify us if you already know solutions of several problems. If you confirm your knowledge by presenting some solutions, you will be allowed not to receive plus-marks for the problems, but to use them in solutions of other problems.

(In the project the tasks were separated as follows: the tasks before and including Theorem 4.3, then some solutions to simple tasks from §§1–2, then other tasks and solutions.)

2 Degenerate matrices

2.1. *(a1-a4) Which of the following matrices are degenerate?*

$$A_1 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}, \quad A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix}, \quad A_4 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

2.2. *(a) Degeneracy is not changed under permutation of columns (rows).*

(b) Degeneracy is not changed under adding one column (row) to another.

(c) Any matrix can be changed to a diagonal matrix by transformations from (a,b).

(d) A matrix is degenerate if and only if it cannot be changed by transformations from (a,b) to the identity matrix.

(f) A square matrix is degenerate if and only if the sum of its several rows (a non-zero number of rows) is the zero row.

(g) There is an algorithm with the complexity of $O(n^3)$ checking the degeneracy of an $n \times n$ matrix.

For a matrix $M \in \mathbb{Z}_2^{n\times n}$ define $\det M := 0$ if M is degenerate, and $\det M := 1$ otherwise. This is called the *determinant* of M. Another notation is

$$\det \begin{pmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{pmatrix} = \begin{vmatrix} M_{1,1} & M_{1,2} \\ M_{2,1} & M_{2,2} \end{vmatrix}, \quad \det M = \begin{vmatrix} M_{1,1} & \dots & M_{1,n} \\ \vdots & \ddots & \vdots \\ M_{n,1} & \dots & M_{n,n} \end{vmatrix}.$$

2.3. *(a)* $\begin{vmatrix} a & b \\ c & d \end{vmatrix} = ad + bc$.

(b) $\det(a_1 + b_1, a_2, \dots, a_n) = \det(a_1, a_2, \dots, a_n) + \det(b_1, a_2, \dots, a_n)$. *Here and below $a_j, b_1 \in \mathbb{Z}_2^n$ are columns of length n.*

(c) $\det(a_1,\dots,a_n) = \sum_{i=1}^{n} a_{i,n}\det(a_1^-,\dots,a_{i-1}^-,a_{i+1}^-,\dots,a_n^-)$, *where every column* $a_i^- \in \mathbb{Z}_2^{n-1}$ *is obtained from the column* a_i *by deleting the last coordinate.*

*(d)** $\det M = \sum_{\sigma\in S_n}\prod_{i=1}^{n} M_{i,\sigma(i)}$, *where* S_n *is the set of all permutations (i. e., 1–1 correspondences)* $\sigma:[n]\to[n]$.

2.4. *(a1-a4) For every matrix of Problem 2.1 find if some entries on the main diagonal can be changed so that the resulting matrix would be degenerate.*

(b1-b4) The same with 'degenerate' replaced by 'non-degenerate'.

Lemma 2.5. *(a) Let* $M\in\mathbb{Z}_2^{n\times n}$ *be a matrix with zeros on the main diagonal. Define the sequence* $M^{(i)}$, $i=0,1,2,\dots,n$ *recursively as follows:*

- $M^{(0)} := M$, *and*
- $M^{(i)}$ *is the result of replacing in* $M^{(i-1)}$ *the element* $M_{i,i}^{(i-1)}=0$ *by* $1+\delta_i$, *where* $\delta_0=0$ *and* $\delta_i := \det M_{[i]\times[i]}^{(i-1)}$ *is the determinant of the left upper* $i\times i$*-corner submatrix of* $M^{(i-1)}$.

Then the matrix M_n *is non-degenerate.*

(b) There is an algorithm with the complexity of $O(n^4)$ *which for a matrix* $M\in\mathbb{Z}_2^{n\times n}$ *finds some numbers from* $\mathbb{Z}_2$ *to replace the entries on the main diagonal of* M *so that the resulting matrix is non-degenerate.*

3 The rank of a matrix

3.1. *(a1-a4) Find* $\operatorname{rk} M$ *for*

$$M=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&0&0&0\end{pmatrix},\quad \begin{pmatrix}1&1&1&1\\1&1&1&1\\1&1&1&1\end{pmatrix},\quad \begin{pmatrix}1&1&1&0\\1&0&1&0\\1&1&1&1\end{pmatrix},\quad \begin{pmatrix}0&1&1&1\\0&0&1&1\\1&0&0&1\end{pmatrix}.$$

(b1-b4) Find $R(M)$ *for the matrices from Problem 2.1.*

3.2. *Take a matrix* $M\in\mathbb{Z}_2^{s\times n}$.

(a) One can choose $\operatorname{rk} M$ *columns of* M *such that every column is the sum of some chosen columns.*

(b) Assume that there are k *columns (not necessarily of* M*) such that every column of* M *is the sum of some of them. Then* $\operatorname{rk} M\le k$.

(c) The rank of a submatrix does not exceed the rank of a matrix.

3.3. *(a) A permutation of columns (or of rows) does not change the rank of a matrix.*

(b) Adding one column to another one (or one row to another one) does not change the rank of a matrix.

(c) The rank of a matrix equals to the maximal number of its rows none of whose sums is zero.

(d) The rank of a matrix equals to the maximal size of its non-degenerate square submatrix.

A square matrix with $\mathbb{Z}_2$-entries is called **even** if all the entries on the main diagonal are zeros.

3.4. *(a) For $M \in \mathbb{Z}_2^{s\times n}$ all non-zero rows are equal if and only if* $\operatorname{rk} M \le 1$.

(b) For a symmetric matrix $M \in \mathbb{Z}_2^{n\times n}$ all non-zero rows are equal if and only if by same permutation of rows and of columns it is possible to obtain a matrix whose upper left square is filled by ones, and all other elements are zeros.

(c) The rank of any non-zero symmetric even matrix is greater than one.

3.5. *The number $R(M)$ is not necessarily preserved by*

(a) permutation of columns;

(b) adding one column to another one.

3.6. *(a) There is an algorithm with the complexity of $O(n^3)$ which calculates the rank of a matrix from $\mathbb{Z}_2^{s\times n}$, $s \le n$.*

(b) For a fixed integer k there is an algorithm with the complexity of $O(n^2)$ deciding for $M \in \mathbb{Z}_2^{s\times n}$, $s \le n$, whether* $\operatorname{rk} M \le k$.

Lemma 3.7. *Let M, D be matrices of the same size with entries in $\mathbb{Z}_2$. Then*

(a) $\operatorname{rk}(M + D) \le \operatorname{rk} M + \operatorname{rk} D$;

(b) $\operatorname{rk}(M + D) \ge \operatorname{rk} M - \operatorname{rk} D$.

3.8. *There is an algorithm with the complexity of $O(n^{k+3})$ finding for $M \in \mathbb{Z}_2^{n\times n}$ a diagonal matrix D such that*

(a) $\operatorname{rk}(M + D) \le k$; *(b)* $\operatorname{rk}(M + D) = k$

under the assumption that such a matrix D exists.

3.9. *Is it correct that for any $m, k \le n$ and a matrix $M \in \mathbb{Z}_2^{n\times n}$ of rank m, if a matrix of rank k can be obtained by changing some entries on the diagonal of M, then this can be done by changing exactly $|m - k|$ entries?*

3.10. *(a,b,c) Find the number of matrices of rank k in $\mathbb{Z}_2^{n\times n}$ for $k = 0, 1, 2$.*

4 Modulo 2 embeddings of graphs to surfaces

This section is formally not used later, but serves as an additional motivation for §5.

Denote by S the torus, or sphere with handles, or the Möbius band, or the Klein bottle, or a 2-dimensional surface. Their simple definitions can be found e. g. in §2.1 of

[Sk20]=https://www.mccme.ru/circles/oim/obstructeng.pdf

Below graph drawings on S may have self-intersections. An *embedding* is a graph drawing without self-intersections.

4.1. *There are embeddings (a1,a2,a3) of K_5, K_6, K_7 in the torus;*

(b1,b2) of K_5, K_6 in the Möbius band;

(c) of K_8 in the sphere with two handles;

(d) of K_m in the sphere with some number of handles (depending on m).

Remark. *In this problem you need to give not rigorous proofs, but large, comprehensible, and preferably beautiful pictures.*

4.2. *The graph K_5 can be drawn in the plane so that the drawings (i. e., the images of) every two non-adjacent edges intersect at an even number of points.*

A *self-intersection point* of a drawing is a point on the drawing to which corresponds more than one point of the graph itself.

A graph drawing is said to be **general position** if

- to every self-intersection point there corresponds exactly two points of the graph;
- every drawing of a vertex is not a self-intersection point,
- the drawing has finitely many self-intersection points, and

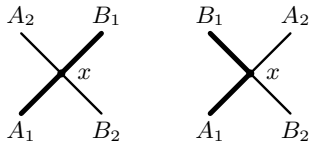


Figure 2: A transverse intersection and a non-transverse intersection

- at every such point the self-intersection is transverse (Figure 2)[2].

A general position graph drawing is a $\mathbb{Z}_2$**-embedding** if the drawings of every two non-adjacent edges intersect at an even number of points.

Remark. Let S be either the plane or the torus or the Möbius band. If a graph has a $\mathbb{Z}_2$-embedding to S, then the graph has an embedding in S. However, there is a graph having a $\mathbb{Z}_2$-embedding to the sphere with 4 handles but not an embedding in the sphere with 4 handles. See references in [Bi21, Remark 1.3.b,c].

Theorem 4.3. *If graph K has a $\mathbb{Z}_2$-embedding to the sphere with g handles, then*

(a) $g \geq (m-4)/3$ *for* $K = K_m$.

(b) $g \geq (m-5)^2/16$ *for* $K = K_m$.

(c) $g \geq (n-2)^2/4$ *for* $K = K_{n,n}$.

Theorem 4.3 is proved by showing that on a surface to which a large graph has a $\mathbb{Z}_2$-embedding, the intersections of closed curves are sufficiently complicated (in the sense of rank of certain matrix; cf. Assertion 4.5). More precisely, Theorem 4.3.a [PT19] follows by Theorems 4.4 and 5.1.b together with Assertion 4.5 (all below). Theorem 4.3.b follows by Theorem 4.3.c (prove!). Theorem 4.3.c is proved in [FK19], see a well-structured exposition in [DS22]. Analogously, Assertions 4.5 and 5.2 (together with Theorem 4.4 and its non-orientable analogue) imply the non-$\mathbb{Z}_2$-embeddability of K_8 to the torus, and of K_7 to the Möbius band (or even of K_7 to the Klein bottle; the non-embeddability of K_7 to the Klein bottle does not follow from the Euler inequality). Analogous non-embeddabiliy result in higher dimensions follows by Theorem 7.1.

Denote by $|X|_2 \in \mathbb{Z}_2$ the parity of the number of elements in a finite set X.

Closed curves $\gamma_1, \dots, \gamma_p$ on S are said to be in **general position** if the graph drawing (of disjoint union of p cycles) formed by this curves is in general position. Their *intersection* $p \times p$- *matrix* G is defined as

$$G_{i,j} := \begin{cases} |\gamma_i \cap \gamma_j|_2, & i \neq j, \\ |\gamma_i \cap \gamma_i'|_2, & i = j, \end{cases}$$

[2]Strictly speaking, the transversality is only easy to define for PL (piecewise-linear) graph drawings. PL curves on the torus can be easily defined by regarding the torus as obtained from a rectangle by gluing. A *PL curve on the torus* is then a family of polygonal lines in the rectangle satisfying certain conditions (work out these conditions!). In a similar way, other surfaces S can be obtained from plane polygons by gluing. (For Möbius band and Klein bottle see [Sk20, §2.1]; for spheres with handles see visualization in https://www.youtube.com/watch?v=G1yyfPShgqw and in https://www.youtube.com/watch?v=U5N5mg3MePM.) This allows one to define PL curves on S. A graph drawing on S is called *PL* if the drawing of every edge is PL. Another formalizations are given in [Sk20, §4, §5].

where γ_i' is a curve close to γ_i in general position to γ_i. Please use the following 'Homology Betti Theorem' without proof.

Theorem 4.4. *For any closed general position curves $\gamma_1, \dots, \gamma_p$ on*

(a) the sphere with g handles the rank of their intersection matrix does not exceed $2g$.

(b) the disk with m Möbius bands the rank of their intersection matrix does not exceed m.

Here the *disk with k Möbius bands* is the figure shown on the left of fig. 1. More precisely, the *disk with m Möbius bands* is the union of a disk and m pairwise disjoint ribbons having their ends glued to $2m$ pairwise disjoint arcs on the boundary circle of the disk (the ribbons do not have to lie in the plane of the disk) so that

• the orientations of the ends of each ribbon given by an orientation of the boundary circle of the disk have 'the same direction along the ribbon', and

• the ribbons are 'separated', i. e. there are m pairwise disjoint arcs A_i on the boundary circle of the disk such that the ends of the i-th ribbon are glued to two disjoint arcs contained in A_i, $i = 1, 2, \dots, m$.

You can make approximations by general position drawings at an intuitive level.

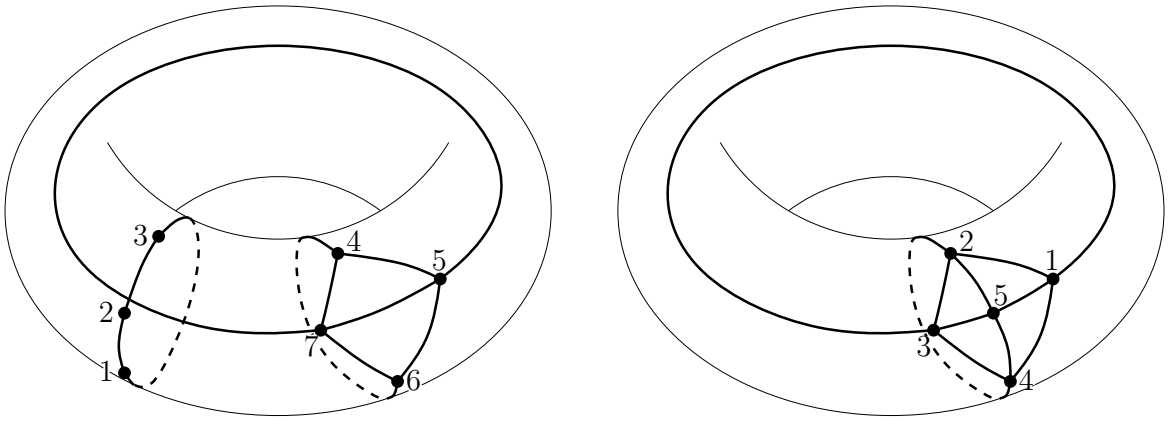


Figure 3: Left: K_3 and K_4 on the torus. Right: K_5 on the torus

4.5. *Take any embedding (or $\mathbb{Z}_2$-embedding) $f\colon K_n \to S$. Take any map $f'\colon K_n \to S$ in general position to f, and close to f. For any pairwise different numbers $i, j, k \in [n]$ denote by $\langle ijk\rangle$ the cycle of length 3 in K_n passing through i, j, k. Let*

$$ijk \wedge pqr := \left|f\langle ijk\rangle \cap f'\langle pqr\rangle\right|_2.$$

Then

(4.5.1) $123 \wedge 456 = 0$.

(4.5.2) $123 \wedge 456 + 123 \wedge 567 + 123 \wedge 467 + 123 \wedge 457 = 0$.
$123 \wedge 345 + 123 \wedge 346 + 123 \wedge 356 + 123 \wedge 456 = 0$.
$123 \wedge 234 + 123 \wedge 235 + 123 \wedge 245 + 123 \wedge 345 = 0$.
$123 \wedge 123 + 123 \wedge 124 + 123 \wedge 134 + 123 \wedge 234 = 0$.

See Figure 3, left. For one formula covering these four formulas see the linear dependence property in §5.

(4.5.3) $125 \wedge 345 + 135 \wedge 245 + 145 \wedge 235 = 1$.

See Figure 3, right. Hint: deduce from (B) below.

Remark. (A) For any pairwise distinct points A_1, A_2, A_3, A_4 in the line there is exactly one 'intertwined' coloring into two colors.

(B) For any pairwise distinct points A_1, A_2, A_3, A_4 on the circle

$$|A_1A_2 \cap A_3A_4| + |A_1A_3 \cap A_2A_4| + |A_1A_4 \cap A_2A_3| = 1.$$

(B') For any 'general position' map $f\colon K_5 \to \mathbb{R}^2$ the number of intersection points in $\mathbb{R}^2$ formed by images of disjoint edges is odd.

A simple deduction of $(A) \Rightarrow (B')$ is presented in [Sk14] (for the linear case; for the PL case the deduction is analogous). Observe that (B') does not follow from Euler formula for planar graphs. Analogously, the non-$\mathbb{Z}_2$-embeddability to surfaces (unlike the non-embeddability) does not follow from the Euler inequality for surfaces [Sk20, §2.4].

5 Rank of matrix with relations

We shorten $\{i\}$ to i. An $\binom{[m]}{3}$-*matrix* is a symmetric square matrix with $\mathbb{Z}_2$-entries whose rows and whose columns correspond to all 3-element subsets of $[m]$, and for which the following properties hold:

(triviality) $A_{P,Q} = 0$ if $P \cap Q = \emptyset$;

(linear dependence) for each 4-element and 3-element subsets $F, P \subset [m]$

$$\sum_{i \in F} A_{F-i,P} = 0.$$

(non-triviality) for each $i \in [m]$ and 4-element subset $F \subset [m] - i$ we have $A_{F,i} = 1$, where

$$A_{F,i} := \sum_{\{X,Y\}\,:\,F\cup i = X\cup Y,\ X\cap Y = i,\ |X|=|Y|=3} A_{X,Y} = \sum_{\{\sigma,\tau\}\,:\,F=\sigma\sqcup\tau,\ |\sigma|=|\tau|=2} A_{i\sqcup\sigma,i\sqcup\tau}.$$

By Assertion 4.5, an $\binom{[m]}{3}$-matrix is constructed from a $\mathbb{Z}_2$-embedding $f\colon K_m \to S$ to a surface. Indeed, set $A_{\{i,j,k\},\{p,q,r\}} := ijk \wedge pqr$. If the surface S is orientable, then the constructed matrix A is even (i. e., $A_{P,P} = 0$ for each 3-element subset $P \subset [m]$).

Theorem 5.1. *(a) If A is an $\binom{[m]}{3}$-matrix, then* $\operatorname{rk} A \geq \dfrac{m-4}{3}$.

(b) If, moreover, A is even, then $\operatorname{rk} A \geq \dfrac{2(m-4)}{5}$.

You can submit separately proofs of the following particular cases of Theorem 5.1. For more strong estimates see §7.

5.2. *(a)* There are no $\binom{[7]}{3}$-matrices of rank* 1.

(b) There are no even $\binom{[8]}{3}$-matrices of rank smaller than* 3.

You can deduce Theorem 5.1 from Proposition 5.7.a,b.

The following assertion is not used in the sequel. In its proof you do not need to explicitly give the matrix, just describe the construction. We only know a proof using Assertions 4.1, 4.5, and Theorem 4.4.

5.3. *(a) There is a non-zero* $\binom{[4]}{3}$*-matrix.*
(b) There is a $\binom{[5]}{3}$*-matrix.*
(c) For any $m \geq 5$ *there is an* $\binom{[m]}{3}$*-matrix.*
(a',b',c') The same for even matrices.
(d) There is a $\binom{[5]}{3}$*-matrix of rank* 1*.*
(e) There is an even $\binom{[5]}{3}$*-matrix of rank* 2*.*
(f) There is a $\binom{[6]}{3}$*-matrix of rank* 1*.*
(g) There is an* $\binom{[8]}{3}$*-matrix of rank greater than* 2*.*

5.4. *Let* A' *be the square matrix of size* $\binom{m-1}{3}$ *obtained from an* $\binom{[m]}{3}$*-matrix by deleting rows and columns corresponding to all subsets containing* m*. Then* A' *is an* $\binom{[m-1]}{3}$*-matrix.*

5.5. *(a) Let* B *be the square matrix of size* $\binom{m-3}{3}$ *obtained from an* $\binom{[m]}{3}$*-matrix* A *by deleting rows and columns corresponding to subsets containing at least one element of* $X := \{m, m-1, m-2\}$*. If* $A_{X,X} = 1$*, then* $\operatorname{rk} A > \operatorname{rk} B$*.*

(b) Let C *be the square matrix obtained from an* $\binom{[m]}{3}$*-matrix* A *by deleting rows and columns corresponding to subsets containing at least one element of certain* 3*-element subsets* $X, Y \subset [m]$*. If* $A_{X,X} = A_{Y,Y} = 0$ *and* $A_{X,Y} = 1$*, then* $\operatorname{rk} A \geq \operatorname{rk} C + 2$*.*

Denote by r_m the minimal rank of an $\binom{[m]}{3}$-matrix. Denote by $\widetilde{r_m}$ the minimal rank of an even $\binom{[m]}{3}$-matrix. Clearly, $r_m = \widetilde{r_m} = 0$ for $m \leq 4$, and $r_m \leq \widetilde{r_m}$. The non-triviality implies that $r_5, \widetilde{r_5} \geq 1$. Theorem 5.1 asserts that $r_m \geq \dfrac{m-4}{3}$ and $\widetilde{r_m} \geq \dfrac{2(m-4)}{5}$.

5.6. *(a,b) Find* r_5, r_6 *and* $\widetilde{r_5}, \widetilde{r_6}, \widetilde{r_7}$*.*
(c) Both sequences $r_m, \widetilde{r_m}$ *are non-decreasing.*

Proposition 5.7. *(a)* $r_m \geq \min\{r_{m-3} + 1, \widetilde{r_m}\}$ *(more precisely, either* $r_m = \widetilde{r_m}$ *or* $r_m \geq r_{m-3} + 1$*);*
(b) $\widetilde{r_m} \geq \widetilde{r_{m-5}} + 2$*.*

6 Classification of symmetric bilinear forms

Fix a symmetric matrix $A \in \mathbb{Z}_2^{n \times n}$. For $U, V \in \mathbb{Z}_2^n$ let

$$A(U, V) = U \cdot_A V := \sum_{i,j=1}^{n} A_{i,j} U_i V_j \quad (= U^T A V).$$

A **basis** of $\mathbb{Z}_2^n$ is an inclusion-minimal ordered set of vectors such that every vector from $\mathbb{Z}_2^n$ is the sum of some vectors from this set.

Theorem 6.1. *For* $n = 2$ *there is a basis* X_1, X_2 *of* $\mathbb{Z}_2^2$ *and numbers* $\gamma_1, \gamma_2 \in \mathbb{Z}_2$ *such that either*
(i) for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}_2$ *we have*

$$(a_1 X_1 + a_2 X_2) \cdot_A (b_1 X_1 + b_2 X_2) = \gamma_1 a_1 b_1 + \gamma_2 a_2 b_2, \quad \text{or}$$

(ii) for any $a_1, a_2, b_1, b_2 \in \mathbb{Z}_2$ *we have*

$$(a_1 X_1 + a_2 X_2) \cdot_A (b_1 X_1 + b_2 X_2) = a_1 b_2 + a_2 b_1.$$

Recall that problems stated after theorems are hints to proofs of the theorems.

6.2. *Assume that $n = 2$, $X \in \mathbb{Z}_2^2$ and $X \cdot_A X = 1$.*

(a) For any $P \in \mathbb{Z}_2^2$ there is $\lambda_{X,P} \in \mathbb{Z}_2$ such that for $P_X := P + \lambda_{X,P}X$ we have $P_X \cdot_A X = 0$.

(b) There is a basis $X_1 = X$, X_2 of $\mathbb{Z}_2^2$ and numbers $\gamma_1 = 1, \gamma_2 \in \mathbb{Z}_2$ such that the property (i) of Theorem 6.1 holds.

6.3. *Assume that $n = 2$, $X, Y \in \mathbb{Z}_2^2$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$. Then $X_1 := X$, $Y_1 := Y$ is a basis of $\mathbb{Z}_2^2$ such that the property (ii) of Theorem 6.1 holds.*

Theorem 6.4. *For $n = 3$ there is a basis X_1, X_2, X_3 of $\mathbb{Z}_2^3$ and numbers $\gamma_1, \gamma_2, \gamma_3 \in \mathbb{Z}_2$ such that either*

(i) for any $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2 + a_3X_3) \cdot_A (b_1X_1 + b_2X_2 + b_3X_3) = \gamma_1a_1b_1 + \gamma_2a_2b_2 + \gamma_3a_3b_3, \quad \text{or}$$

(ii) for any $a_1, a_2, a_3, b_1, b_2, b_3 \in \mathbb{Z}_2$ we have

$$(a_1X_1 + a_2X_2 + a_3X_3) \cdot_A (b_1X_1 + b_2X_2 + b_3X_3) = a_1b_2 + a_2b_1 + \gamma_3a_3b_3.$$

6.5. *Assume that $X, Y \in \mathbb{Z}_2^3$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$.*

(a) For any $P \in \mathbb{Z}_2^3$ there are $\lambda_{X,Y,P}, \lambda_{Y,X,P} \in \mathbb{Z}_2$ such that for $P_{X,Y} := P + \lambda_{X,Y,P}Y + \lambda_{Y,X,P}X$ we have $P_{X,Y} \cdot_A X = P_{X,Y} \cdot_A Y = 0$.

(b) There is a basis $X_1 = X$, $X_2 = Y$, X_3 of $\mathbb{Z}_2^3$ and a number $\gamma_3 \in \mathbb{Z}_2$ such that the property (ii) of Theorem 6.4 holds.

Theorem 6.6. *There are k, l and a basis $X_1, Y_1, \ldots, X_k, Y_k, Z_1, \ldots, Z_{n-2k}$ of $\mathbb{Z}_2^n$ such that $2k + l \le n$ and for any $a, a', b, b' \in \mathbb{Z}_2^k$ and $c, c' \in \mathbb{Z}_2^{n-2k}$ we have*

$$(a_1X_1 + b_1Y_1 + \ldots + a_kX_k + b_kY_k + c_1Z_1 + \ldots + c_{n-2k}Z_{n-2k}) \cdot_A$$

$$\cdot_A (a'_1X_1 + b'_1Y_1 + \ldots + a'_kX_k + b'_kY_k + c'_1Z_1 + \ldots + c'_{n-2k}Z_{n-2k}) =$$

$$= a_1b'_1 + a'_1b_1 + \ldots + a_kb'_k + a'_kb_k + c_1c'_1 + \ldots + c_lc'_l.$$

If A is even, then $l = 0$.

6.7. *Assume that $X \in \mathbb{Z}_2^n$ and $X \cdot_A X = 1$.*

(a) State and prove the n-dimensional analogue of Assertion 6.2.a.

(b) There is a basis $X, E_1, \ldots, E_{n-1}$ of $\mathbb{Z}_2^n$ and a symmetric matrix $B \in \mathbb{Z}_2^{(n-1)\times(n-1)}$ such that for any $a, b \in \mathbb{Z}_2$ and $\lambda, \mu \in \mathbb{Z}_2^{n-1}$ we have

$$(aX + \lambda_1E_1 + \ldots + \lambda_{n-1}E_{n-1}) \cdot_A (bX + \mu_1E_1 + \ldots + \mu_{n-1}E_{n-1}) = ab + \lambda \cdot_B \mu.$$

6.8. *Assume that $X, Y \in \mathbb{Z}_2^n$ and $X \cdot_A Y = 1$, $X \cdot_A X = Y \cdot_A Y = 0$.*

(a) State and prove the n-dimensional analogue of Assertion 6.5.a.

(b) There is a basis $X, Y, E_1, \ldots, E_{n-2}$ of $\mathbb{Z}_2^n$ and a symmetric matrix $B \in \mathbb{Z}_2^{(n-2)\times(n-2)}$ such that for any $a_X, a_Y, b_X, b_Y \in \mathbb{Z}_2$ and $\lambda, \mu \in \mathbb{Z}_2^{n-2}$ we have

$$(a_XX+a_YY+\lambda_1E_1+\ldots+\lambda_{n-2}E_{n-2}) \cdot_A (b_XX+b_YY+\mu_1E_1+\ldots+\mu_{n-2}E_{n-2}) = a_Xb_Y+a_Yb_X+\lambda \cdot_B \mu.$$

7 Rank of matrix with relations: generalization

The following results are 'higher-dimensional' (and more strong) generalizations of Theorem 5.1, Assertions 5.4 and 5.5, and Proposition 5.7. They give a simplified well-structured exposition of [PT19, Theorem 1].

An $\binom{[m]}{l}$-*matrix* is a symmetric square matrix with $\mathbb{Z}_2$-entries whose rows and whose columns correspond to all l-element subsets of $[m]$, and for which (triviality) and the following properties hold:

(linear dependence) for each $(l+1)$-element and l-element subsets $F, P \subset [m]$

$$\sum_{i\in F} A_{F-i,P} = 0.$$

(non-triviality) for each $i \in [m]$ and $(2l-2)$-element subset $F \subset [m]-i$ we have $A_{F,i} = 1$, where

$$A_{F,i} := \sum_{\{X,Y\}\,:\,F\cup i=X\cup Y,\ X\cap Y=i,\ |X|=|Y|=l} A_{X,Y} = \sum_{\{\sigma,\tau\}\,:\,F=\sigma\sqcup\tau,\ |\sigma|=l-1} A_{i\sqcup\sigma,i\sqcup\tau}.$$

Analogously to Assertion 4.5, an $\binom{[m]}{l}$-matrix is constructed by a $\mathbb{Z}_2$-embedding of the $(l-1)$-dimensional skeleton of the $(m-1)$-dimensional simplex to a $2(l-1)$-dimensional manifold.

Theorem 7.1. *Suppose $l \geq 3$ and A is an $\binom{[m]}{l}$-matrix.*

(a) Then $\operatorname{rk} A \geq \dfrac{m-2l+2}{l-1}$. *(b) If, moreover, A is even, then* $\operatorname{rk} A \geq \dfrac{2(m-2l+2)}{l}$.

You can deduce Theorem 7.1 from Propositions 7.4.a,b.

7.2. *Let A' be the square matrix of size $\binom{m-1}{l}$ obtained from an $\binom{[m]}{l}$-matrix by deleting rows and columns corresponding to all subsets containing m. Then A' is an $\binom{[m-1]}{l}$-matrix.*

7.3. *Let A be an $\binom{[m]}{l}$-matrix and $X := \{m-l+1, m-l+2, \dots, m\}$.*

(a,b') Let B be the square matrix of size $\binom{m-l}{l}$ obtained from A by deleting rows and columns corresponding to subsets containing at least one of the elements of X.

If $A_{X,X} = 1$, then $\operatorname{rk} A > \operatorname{rk} B$.

If $A_{X,X} = A_{Y,Y} = 0$ and $A_{X,Y} = 1$ for some $Y \subset [m]$, then $\operatorname{rk} A \geq \operatorname{rk} B + 2$.

(b) Let C be the square matrix obtained from A by deleting rows and columns corresponding to subsets containing at least one element of X or of certain l-element subset $Y \subset [m]$. If $A_{X,X} = A_{Y,Y} = 0$ and $A_{X,Y} = 1$, then $\operatorname{rk} A \geq \operatorname{rk} C + 2$.

(a') For l-element subsets $P, Q \subset [m-l+1]$ define

$$D_{P,Q} := A_{P,Q} + A_{P,X}A_{Q,X}.$$

If $A_{X,X} = 1$, then $\operatorname{rk} D < \operatorname{rk} A$ *and D is an $\binom{[m-l+1]}{l}$-matrix.*

Assertions 7.3.a,b are only required to illustrate the idea of Assertions 7.3.a',b' by proving much easier results giving estimates $\operatorname{rk} A \geq \dfrac{m-2l+2}{l}$ and, for A even, $\operatorname{rk} A \geq \dfrac{2(m-2l+2)}{2l-1}$.

Denote by r_m the minimal rank of an $\binom{[m]}{l}$-matrix. Denote by $\widetilde{r_m}$ the minimal rank of an even $\binom{[m]}{l}$-matrix. Clearly, $r_m = \widetilde{r_m} = 0$ for $m \leq 2l-2$, both sequences $r_m, \widetilde{r_m}$ are non-decreasing, and $r_m \leq \widetilde{r_m}$. The non-triviality implies that $r_{2l-1}, \widetilde{r_{2l-1}} \geq 1$. Theorem 7.1 asserts that $r_m \geq \dfrac{m-2l+2}{l-1}$ and $\widetilde{r_m} \geq \dfrac{2(m-2l+2)}{l}$.

Proposition 7.4. *(a)* $r_m \geq \min\{r_{m-l+1}+1, \widetilde{r_m}\}$ *(more precisely, either* $r_m = \widetilde{r_m}$*, or* $r_m \geq r_{m-l+1}+1$*);*

(b) $\widetilde{r_m} \geq \widetilde{r_{m-l}} + 2$.

Proof of Proposition 7.4.a also uses an algebraic version (b) of the higher-dimensional analogue of the following result (a).

Proposition 7.5. *(a) Denote by* $X = \binom{[5]}{2}$ *the set of unordered pairs of* 2*-element subsets of* $[5]$*. For any* $i \in [5]$ *and a partition* $[5]-i = \sigma \sqcup \tau$ *into disjoint* 2*-element sets denote*

$$T_{i,\{\sigma,\tau\}} := \big\{\{\alpha,\beta\} \in X \ : \ \alpha \subset \sigma \sqcup i, \ \beta \subset \tau \sqcup i\big\}.$$

Denote by A_i *the sum modulo* 2 *(i. e., the symmetric difference) of sets* $T_{i,\{\sigma,\tau\}}$ *over all non-ordered partitions* $[5]-i = \sigma \sqcup \tau$ *as above. Then*

$$A_i = \big\{\{\alpha,\beta\} \in X \ : \ \alpha \cap \beta = \emptyset\big\}$$

and so is independent of i*.*

(b) Let A *be a symmetric square matrix with* $\mathbb{Z}_2$*-entries whose rows and whose columns correspond to all* l*-element subsets of* $[m]$*. If* A *satisfies the linear dependence property (from the definition of an* $\binom{[m]}{l}$*-matrix), then* $A_{F,i}$ *depends only on* $F \sqcup i$ *not on* (F,i)*.*

Hints and solutions to some problems

See proof of Proposition 1.1 in [Bi20].

1.2. (a) Change the numbers on the main diagonal of M so that the sum of the entries in each row is even. The resulting matrix is degenerate.

(b) Use induction. See Lemma 2.5.b.

1.3. (a) Any matrix formed as a result of putting numbers from $\mathbb{Z}_2$ in the elements on the main diagonal of M can be uniquely represented as the sum $M+D$ where D is a diagonal matrix. By Lemma 3.7.b for every diagonal matrix D with more than k zeros on the main diagonal we have $\operatorname{rk}(M+D) \geq \operatorname{rk} M - \operatorname{rk} D > n - (n-k) = k$.

(b) The algorithm of (b) is constructed using (a) and Lemma 2.5.b. The algorithm given by Lemma 2.5.b has complexity $O(n^4)$. There is an algorithm searching through all diagonal $n \times n$ matrices with $\leq k$ zeroes on the main diagonal with the complexity of

$$O\left(n\binom{n}{0} + n\binom{n}{1} + \ldots + n\binom{n}{k}\right) \overset{(*)}{=} O\left((k+1)n\binom{n}{k}\right) = O\left(n \cdot n^k\right) = O\left(n^{k+1}\right).$$

Here (*) holds because we may assume that $n \geq 2k$. Thus, by Assertion 3.6.b the complexity of the whole algorithm is $O(n^4) + O(n^{k+1}n^2) = O(n^{k+3})$ (since $k \geq 1$).

1.4. (a) Denote by n the number of columns of M and of D. By Lemma 3.7.b we have

$$\begin{aligned} 2\operatorname{rk}(M+D) &= \operatorname{rk}(M+D) + \operatorname{rk}((M+E)+(E+D)) \\ &\geq (\operatorname{rk} M - \operatorname{rk} D) + (\operatorname{rk}(M+E) - \operatorname{rk}(E+D)) \\ &= n - \operatorname{rk} D + \operatorname{rk}(M+E) - (n - \operatorname{rk} D) = \operatorname{rk}(M+E). \end{aligned}$$

(b) Let M_n be the matrix obtained by applying the algorithm of Lemma 2.5.b to the matrix M. Let $k := \operatorname{rk}(M_n + E)$. We have $R(M) = \operatorname{rk}(M+D)$ for some diagonal matrix D. Hence by (a) $k/2 \leq R(M) \leq k$ as required.

The number k can be computed in time $O(n^3)$. Hence the total complexity of the algorithm is $O(n^4) + O(n^3) = O(n^4)$.

2.1. *Answers:* A_1, A_2 and A_3 are degenerate, while A_4 is non-degenerate.

2.2. Hints: (a)-(b) track the maximal non-degenerate submatrix; (c) use induction.

Part (a) is clear.

(b) For a matrix M denote by $\operatorname{row}_{i\to i+j}M$ the matrix obtained from M by replacing the ith row by the sum of the ith row and the jth row. The matrix $\operatorname{col}_{i\to i+j}M$ is defined similarly.

It is clear that to prove part (b) we have to show that the matrices M, $\operatorname{row}_{i\to i+j}M$ and $\operatorname{col}_{i\to i+j}M$ are degenerate or not simultaneously.

Next, observe that $\operatorname{row}_{i\to i+j}\operatorname{row}_{i\to i+j}M = M = \operatorname{col}_{i\to i+j}\operatorname{col}_{i\to i+j}M$. Thus it suffices to prove that if M is degenerate then both $\operatorname{row}_{i\to i+j}M$ and $\operatorname{col}_{i\to i+j}M$ are degenerate.

Assume that the sum of columns $c_1, c_2, \ldots, c_s$ of M equals zero.

Then the sum of the 'same' columns of $\operatorname{row}_{i\to i+j}M$ equals zero.

If $i \notin \{c_1, \ldots, c_s\}$ then the sum of 'the same' columns of $\operatorname{col}_{i\to i+j}M$ equals zero. If $i, j \in \{c_1, \ldots, c_s\}$ then the sum of columns indexed by $\{c_1, \ldots, c_s\} - \{j\}$ of $\operatorname{col}_{i\to i+j}M$ equals zero. If $i \in \{c_1, \ldots, c_s\}$ and $j \notin \{c_1, \ldots, c_s\}$ then the sum of columns indexed by $\{c_1, \ldots, c_s, j\}$ of $\operatorname{col}_{i\to i+j}M$ equals zero.

This completes the proof of (b).

(c) We will show explicitly how to produce a diagonal matrix out of M.

If all entries of M are 0 then M is already diagonal. If M has a non-zero entry then we place this entry in the top-left corner by permuting the row of this entry with the top row, and the column of this entry with the left column. For the obtained matrix add the top row to other rows and the left column to other columns. All entries in the left column and the top row except the the top-left entry become zeros. Delete the top row and the left column of the obtained matrix.

Repeat the procedure inductively for the obtained submatrix. In the end this will produce a diagonal matrix.

(d) By part (c) we can change M into a diagonal matrix using transformations from parts (a, b); also M is degenerate if and only if the new matrix is degenerate. It remains to mention that a diagonal matrix is non-degenerate iff it is the identity matrix.

(f) This follows from (a)-(d).

(g) The algorithm is constructed in the solution of part (c). The algorithm has n major steps, a single major step is described in the second paragraph of (c). Each major step requires at most one permutation of rows, at most one permutation of columns and up to $2n$ additions of rows and columns. Thus the complexity of the whole algorithm is $O(n) + n \cdot O(n^2) = O(n^3)$.

2.3. (a) The formula follows because a matrix from $\mathbb{Z}_2^{2\times 2}$ is degenerate if and only if either it has a zero row, or it has a zero column, or rows are the same and columns are the same (in the latter case all entries are ones).

Alternatively, here are all matrices from $\mathbb{Z}_2^{2\times 2}$ up to permutations of rows and columns:

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&1\\1&1\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}.$$

The first two are non-degenerate, and the other are degenerate. It is easy to verify the formula for each of them.

(d) This follows by (b,c).

Here is an alternative direct proof. Consider $n \times n$ chessboard. A *rook placement* for such a chessboard is a placement of n rooks on that board with the condition that they do not beat each other. A *rook M-placement* for such a chessboard is a rook placement such that all rooks are staying on cells corresponding to unit entries of M. Denote by $\det^* M$ the parity of the amount of rook M-placements. Then (d) can be restated as follows: $\det M = \det^* M$. This follows because

- transformations of 2.2.a, 2.2.b preserve $\det^* M$, and
- $\det M' = \det^* M'$ for a diagonal matrix M'.

2.4. For any degenerate matrix of Problem 2.1 we show how to change entries on the main diagonal to make it non-degenerate; we show the opposite for A_4:

$$A_1 \to \begin{pmatrix}1&0&0\\0&1&0\\0&0&1\end{pmatrix}, \quad A_2, A_3 \to \begin{pmatrix}0&1&1\\1&0&1\\1&1&1\end{pmatrix}, \quad A_4 \to \begin{pmatrix}0&1&1\\0&1&1\\1&0&0\end{pmatrix}.$$

2.5. (a) In the following paragraph we prove by induction on $i \geq 1$ that the determinant $\Delta_i := \det M^{(i)}_{[i]\times[i]}$ of the left upper $i \times i$-corner submatrix of $M^{(i)}$ is equal to 1. Then $\det M^{(n)} = \Delta_n = 1$.

Base $i = 1$ follows because $\Delta_1 = 1 + \delta_0 = 1$. Let us prove the inductive step $i - 1 \to i$. Apply the decomposition formula for the determinant Δ_i by the last row of the corresponding

submatrix of $M^{(i)}$ (Assertion 2.3.c). Since $M^{(i-1)}_{i,i} = M_{i,i} = 0$ and $\Delta_{i-1} = 1$, we have $\Delta_i = \delta_i + (1+\delta_i)\Delta_{i-1} = 1$.

(b) The algorithm is constructed by (a). The algorithm is essentially a computation of the determinants of n square submatrices of sizes $1, 2, \ldots, n$. Hence by Assertion 2.2.g its complexity is $O(1^3 + 2^3 + \ldots + n^3) = O(n \cdot n^3) = O(n^4)$.

3.1. *Answers:* (a1) 0; (a2) 1; (a3), (a4) 3; (b1) 0; (b2), (b3) 1; (b4) 2.

3.2. Hint to (b): find the number of sums of k columns.

Part (a) follows from the definition of $\operatorname{rk} M$.

(b) By definition of rk the number of different sums of columns of M is $2^{\operatorname{rk} M}$. On the other hand the number of such sums does not exceed 2^k. Therefore $2^k \geq 2^{\operatorname{rk} M}$, hence $k \geq \operatorname{rk} M$.

3.3. The proofs of are similar to the proofs of Assertion 2.2.

3.4. Part (a) is clear.

(b) If for a non-zero symmetric matrix M there exists such a permutation of rows and columns, then $\operatorname{rk} M = 1$ by Assertion 3.2.b.

We now take a symmetric matrix M of rank 1. As the required permutation we can take any permutation mapping non-zero rows of M to the first rows. Indeed, take any non-zero rows i, j. If $M_{i,j} = 0$ then there exists a non-zero row k such that $M_{i,k} = 1$. Hence the jth and the kth rows are distinct non-zero rows of the matrix M of rank one. A contradiction. Hence $M_{i,j} = 1$.

(c) Pick a nonzero row and apply the above argument.

3.5. (a) $R\begin{pmatrix}1&0&1\\0&0&1\\0&1&0\end{pmatrix} = 2, \quad R\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} = 1.$

(b) $R\begin{pmatrix}1&0&1\\0&1&1\\0&1&0\end{pmatrix} = 2, \quad R\begin{pmatrix}1&0&1\\0&1&0\\0&0&1\end{pmatrix} = 1.$

3.6. Hint for (a): cf. Assertion 2.2.

(a) The algorithm from the proof of 2.2.c provides a diagonal matrix of the same rank, and has the required complexity. The rank of a diagonal matrix is equal to the number of non-zero entries in it.

(b) We shall construct a set S_k of columns such that

- these columns constitute a non-degenerate submatrix;
- the first k columns of the matrix M are sums of several columns from the set S_k.

If $|S_k| > r$ for some $k = 1, \ldots, n$ then the answer is 'NO'. If for all $k = 1, \ldots, n$ we have $|S_k| \leq r$ then the answer is 'Yes'. The answer is correct because $|S_1| \leq |S_2| \leq \ldots \leq |S_n|$, and because $|S_n| > r$ is equivalent to $\operatorname{rk} M > r$.

Set $S_1 := \emptyset$ if the first column of M is 0 then, and $S_1 := \{1\}$ otherwise.

Let us define S_{k+1} from S_k. We form the set of all sums of columns of M with indices from S_k (it takes $O(n)$ operations because $|S_k| \leq r$). Then we compare the $(k+1)$st column of M with all sums from this set (this will take at most $2^r O(n) = O(n)$ operations). If the $(k+1)$st column of M equals to at least one of the sums then $S_{k+1} := S_k$. Otherwise we set $S_{k+1} := S_k \cup \{k+1\}$.

It is easy to verify that the total complexity of the algorithm is $O(n^2)$.

3.7. Part (b) follows from (a) because

$$\operatorname{rk} M = \operatorname{rk}(M + D + D) \leq \operatorname{rk}(M + D) + \operatorname{rk} D \quad \Rightarrow \quad \operatorname{rk}(M + D) \geq \operatorname{rk} M - \operatorname{rk} D.$$

We now prove (a). Choose columns from Assertion 3.2.a for M and for D. Then every column of $M+D$ is the sum of some of chosen $\operatorname{rk} M + \operatorname{rk} D$ columns. By Assertion 3.2.b $\operatorname{rk}(M+D) \le \operatorname{rk} M + \operatorname{rk} D$.

3.8. The statement and the proof of Assertion 3.8 are similar to the statement and the proof of Theorem 1.3.b.

3.9. Answer: no. If M is a 3×3-matrix given next and $k=1$ then the statement is false.

$$\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

3.10. *Answers:* (a) 1; (b) $(2^n-1)^2$; (c) $(2^n-1)^2(2^n-2)^2/6$.

(a) There exists only one matrix of rank 0, the matrix all whose entries are zeroes.

(b) For the matrix of rank 1 all columns containing a non-zero entry are the same. Hence such matrices are in 1–1 correspondence with ordered pairs formed by

- a non-empty subset of the set of columns ('non-zero columns'), and
- a nonzero vector in $v \in \mathbb{Z}_2^n$ ('column vector').

Therefore there are $(2^n-1)^2$ such matrices.

(c) Fix a matrix M of rank 2. Then there exists a pair (v,w) of columns of M forming a non-degenerate matrix. Any other column is either 0 or v, or w, or $v+w$ (see Assertion 3.2). This set $S = S_M$ of four vectors does not depend on a choice of the two columns v, w; we call it the *column span* of M. (This is a 2-dimensional vector subspace of $\mathbb{Z}_2^n$.)

Each column span is defined by any ordered pair of non-zero vectors in it. Each column span contains exactly 6 such ordered pairs. Hence there are $(2^n-1)(2^n-2)/6$ column spans. In the following paragraph we prove that there are exactly $(2^n-1)(2^n-2)$ matrices of rank 2 for a given column span. Hence there are $(2^n-1)^2(2^n-2)^2/6$ matrices of rank 2.

First proof. To a matrix M there correspond the set X of columns of M equal to v or to $v+w$, and the set Y of columns of M equal w or $v+w$. Since $\operatorname{rk} M = 2$, both sets are non-empty and $X \ne Y$. Moreover, matrix M can be reconstructed from X, Y. There are $(2^n-1)(2^n-2)$ pairs (X,Y) of distinct non-empty subsets.

Second proof. For a given 4-element set $S = \{0, v, w, v+w\}$, regard a matrix M with the column span S as a map ϕ_M from the set $[n]$ of columns to S. We have $\operatorname{rk} M = 2$ if and only if

(*) the image of ϕ_M contain at least two of vectors $v, w, v+w$.

There are 4^n maps $[n] \to S$. There are 2^n maps $[n] \to \{0, v\}$. The same holds for $\{0, v\}$ replaced either by $\{0, w\}$ or by $\{0, v+w\}$. There is only one map $[n] \to \{0\}$. Hence there are exactly $4^n - 3\cdot 2^n + 2 = (2^n-1)(2^n-2)$ maps satisfying the condition (*).

Remark. More generally, the number of matrices of rank k in $\mathbb{Z}_2^{m\times n}$ is equal to

$$\frac{2^{k(k-1)/2}\Pi_{i=0}^{k-1}(2^{m-i}-1)\Pi_{i=0}^{k-1}(2^{n-i}-1)}{\Pi_{i=0}^{k-1}(2^{k-i}-1)}.$$

See theorem 7.1.5 in [ACM29, p. 299] (this theorem is even more general; for our case of matrices over $\mathbb{Z}_2$ take $q=2$, $\mathrm{GF}(2) = \mathbb{Z}_2$).

4.1. (a1-a3) A beautiful realization of the graph K_5 on the torus is shown in Figure 4, left. Realizations of K_6 and K_7 are analogous, see Figure 4, middle.

Another solutions (whose idea works for (c,d)). Draw the graph K_5 in the plane with *one* self-intersection point. In a small neighborhood of the point, attach a handle and lift one of the edges 'bridgelike' over the other edge to the handle, see Figure 5, left.

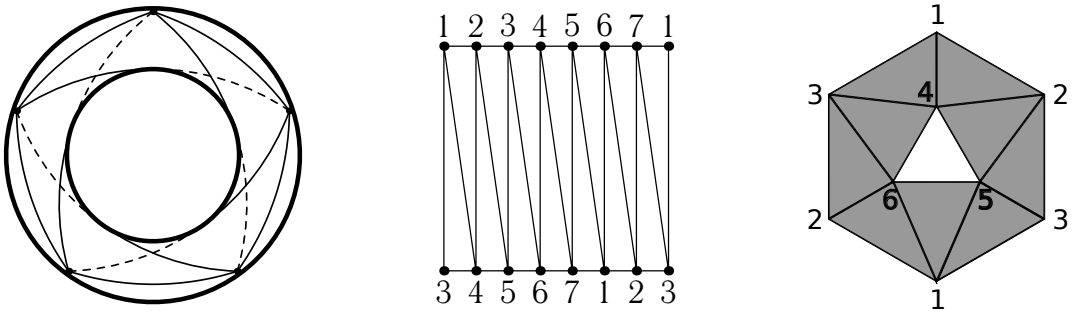


Figure 4: Realization of nonplanar graphs

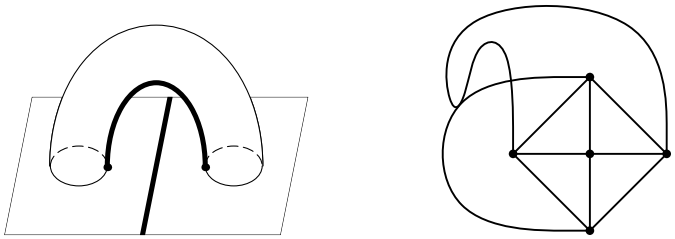


Figure 5: Left: resolving intersection by adding a handle.
Right: a 'non-general position even drawing' of K_5 in the plane

(b2) See Figure. 4, right.

4.2. See Fig. 5, right.

5.1. (b) Induction on m. The base $m \le 4$ is clear. By Assertion 5.7.b and induction hypothesis we have

$$\widetilde{r_m} \ge \widetilde{r_{m-5}} + 2 \ge \frac{2(m-5-4)}{5} + 2 = \frac{2(m-4)}{5}.$$

(a) Induction on m. The base $m \le 4$ is clear. By Assertion 5.7.a, Theorem 5.1.b and induction hypothesis we have

$$r_m \ge \min\{r_{m-3}+1, \widetilde{r_m}\} \ge \min\left\{\frac{m-3-4}{3}+1, \frac{2(m-4)}{5}\right\} = \frac{m-4}{3}.$$

5.3. Denote by A^f the $\binom{[m]}{3}$-matrix constructed via an embedding $f\colon K_m \to S$, see the beginning of Section 5.

(a) Consider the K_4-subgraph of K_5 with vertices 1, 2, 3, 4 together with its embedding to the torus defined by Figure 3, right side. Then A^f is a non-trivial $\binom{[m]}{3}$-matrix.

(b) Let f be the embedding of K_5 into the torus defined by the right side of Figure 3. Then A^f has the required property.

(c) By Assertion 4.1.d there exists an embedding $f\colon K_m \to S$ where S is a sphere with several handles. Then A^f has the required property.

(a', b', c') The matrices A^f from (a, b, c) respectively satisfy the needed conditions.

Parts (d, e, f) follow from Assertion 5.6.a, b.

5.4. See proof of Assertion 7.2 below.

5.5. (a, b) See proof of Assertions 7.3.a,b below.

5.6. (a) Recall that if $m \ge 5$ then every $\binom{[m]}{3}$-matrix is not a zero matrix. This implies that $r_5, r_6 \ge 1$. Let f be an embedding defined by Assertion 4.1.b1, b2. It follows from Theorem 4.4 that $\operatorname{rk} A^f \le 1$. Hence $r_5 = r_6 = 1$.

(b) Assertion 3.4.c implies that $\widetilde{r_5}, \widetilde{r_6}, \widetilde{r_7} \geq 2$. We have $\operatorname{rk} A^f = 2$ for f defined by Assertion 4.1.a1, a2, a3 and hence $\widetilde{r_5} = \widetilde{r_6} = \widetilde{r_7} = 2$.

(c) Let A be an $\binom{[m]}{3}$-matrix and let B be an $\binom{[m-1]}{3}$-submatrix of A introduced in Assertion 5.4. We have $\operatorname{rk} B \leq \operatorname{rk} A$ and therefore $r_m \geq r_{m-1}$.

If A is even then B is even and therefore $\widetilde{r_m} \geq \widetilde{r_{m-1}}$.

5.7. (a) (Take $l = 3$.) Take an $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = r_m$. If A is even, then $r_m = \widetilde{r_m}$, so we are done. Otherwise there is an l-element subset $X \subset [m]$ such that $A_{X,X} = 1$. Let B be the 'restriction' of A to l-element subsets of $[m] - X$.

Then

$$r_m = \operatorname{rk} A \geq \operatorname{rk} B + 1 \geq r_{m-l} + 1, \quad \text{where}$$

- the first inequality follows by Assertion 5.5.a;
- the second inequality holds because B is a $\binom{[m]-X}{l}$-matrix by Assertion 5.4.

(b) (Take $l = 3$.) Take an even $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = \widetilde{r_m}$. By the non-triviality $A \neq 0$. Hence there are l-element subsets $X, Y \subset [m]$ such that $A_{X,Y} = 1$. Let C be the 'restriction' of A to l-element subsets of $[m] - X - Y$.

Then

$$\widetilde{r_m} = \operatorname{rk} A \geq \operatorname{rk} C + 2 \geq \widetilde{r_{m-2l+1}} + 2, \quad \text{where}$$

- the first inequality follows by Assertion 5.5.b;
- the second inequality holds because C is a $\binom{[m]-X-Y}{l}$-matrix by Assertion 5.4, and because $A_{X,Y} = 1$, so by the triviality $X \cap Y \neq \emptyset$, hence $|[m] - X - Y| \geq m - 2l + 1$.

6.7. (a) $\lambda_{X,P} = X \cdot_A P$.

6.8. (a) $\lambda_{X,Y,P} = X \cdot_A P$, $\lambda_{Y,X,P} = Y \cdot_A P$.

7.2. (For 5.4 take $l = 3$.) It is obvious that all the conditions for the mentioned submatrix are satisfied.

7.3. (a) (For 5.5.a take $l = 3$.) Let B' be the 'restriction' of A to X and to l-element subsets of $[m] - X$. Then

$$\operatorname{rk} A \geq \operatorname{rk} B' = \operatorname{rk} B + 1,$$

where equality holds because by the triviality $B'_{X,Z} = 0$ for any $Z \subset [m] - X$.

(b) (For 5.5.b take $l = 3$.) Let C' be the 'restriction' of A to X, Y and l-element subsets of $[m] - X - Y$. Then

$$\operatorname{rk} A \geq \operatorname{rk} C' = \operatorname{rk} C + 2,$$

where equality holds because by the triviality $C'_{X,Z} = C'_{Y,Z} = 0$ for any $Z \subset [m] - X - Y$.

(b') Take a basis of $\mathbb{Z}_2^{\binom{m}{l}}$ corresponding to l-element subsets of $[m]$. Define a bilinear form A on $\mathbb{Z}_2^{\binom{m}{l}}$ by setting $A(P, Q) := A_{P,Q}$ for basic vectors P, Q. Take any l-element set $P \subset [m]$. Let

$$\overline{P} = \overline{P}(X, Y) := P + A_{X,P}Y + A_{Y,P}X.$$

Recall that

$$A_{X,Y} = A_{Y,X} = 1 \quad \text{and} \quad A_{X,X} = A_{Y,Y} = 0. \tag{*}$$

Hence

$$A(\overline{P}, X) = A(\overline{P}, Y) = 0 \tag{**}$$

(i. e., $\overline{P}$ is the orthogonal projection of P to the orthogonal complement of $\langle X, Y\rangle$ with respect to A). By the triviality, for $P \subset [m] - X$ we have $\overline{P} = P + A_{Y,P}X$. Hence for every l-element sets $P, Q \subset [m] - X$ we have

$$A(\overline{P}, \overline{Q}) = A_{P,Q} + 0 + 0 + 0 = B_{P,Q}. \tag{***}$$

(I. e., B is the Gramian matrix with respect to A of the 'projections' $\overline{P}$ of l-element sets $P \subset [m]-X$.) Let B' be the Gramian matrix with respect to A of X, Y and the 'projections' $\overline{R}$ of l-element sets $R \subset [m]-X$. I. e., $B'_{P,Q} = A(\widehat{P},\widehat{Q})$, where $\widehat{P} = P$ if $P \in \{X,Y\}$, and $\widehat{P} = \overline{P}$ otherwise ($\widehat{Q}$ is defined analogously). Then

- $B'_{X,Y} = B'_{Y,X} = 1$, $B'_{X,X} = B'_{Y,Y} = 0$ (by (*)),
- $B'_{X,P} = B'_{P,X} = B'_{Y,P} = B'_{P,Y} = 0$ for $P \neq X, Y$ (by (**)), and
- $B'_{P,Q} = B_{P,Q}$ for $P, Q \subset [m]-X$ (by (***)).

Hence $\operatorname{rk} B + 2 = \operatorname{rk} B' \leq \operatorname{rk} A$.

(a') In this paragraph we prove that $\operatorname{rk} D < \operatorname{rk} A$. Take a basis of $\mathbb{Z}_2^{\binom{m}{l}}$ corresponding to l-element subsets of $[m]$. Define a bilinear form A on $\mathbb{Z}_2^{\binom{m}{l}}$ by setting $A(P,Q) := A_{P,Q}$ for basic vectors P, Q. Let P_X be the orthogonal projection of P to the orthogonal complement of X (with respect to A), i. e., $P_X := P + A_{P,X}X$. We have

$$A(P_X, Q_X) = A(P,Q) + A(A_{P,X}X, Q) + A(P, A_{Q,X}X) + A(A_{P,X}X, A_{Q,X}X) =$$
$$= A_{P,Q} + A_{P,X}A_{X,Q} + A_{P,X}A_{Q,X} + A_{P,X}A_{Q,X}A_{X,X} = A_{P,Q} + A_{P,X}A_{Q,X} = D_{P,Q}.$$

Then D is the Gramian matrix (with respect to A) of the projections of subsets of $[m-l+1]$. Let D' be the Gramian matrix (with respect to A) of X and the projections of subsets of $[m-l+1]$. We have $D_{P,Q} = D'_{P,Q}$ for all subsets $P, Q \subset [m-l+1]$. Furthermore, $D'_{X,P} = D'_{P,X} = 0$ for any basic vector $P \neq X$ and $D'_{X,X} = A_{X,X} = 1$. Thus $\operatorname{rk} D = \operatorname{rk} D' - 1 < \operatorname{rk} A$.

In this paragraph we prove that D satisfies the triviality property. If $P \cap Q = \emptyset$, then either $P \cap X = \emptyset$, or $Q \cap X = \emptyset$. Hence $D_{P,Q} = A_{P,Q} + A_{P,X}A_{Q,X} = 0 + 0 = 0$.

In this paragraph we prove that D satisfies the linear dependence property. For each $(l+1)$-element and l-element subsets $F, P \subset [m-l+1]$ we have

$$\sum_{i \in F} D_{F-i,P} = \sum_{i \in F} A_{F-i,P} + A_{P,X} \sum_{i \in F} A_{F-i,X} = 0.$$

In this paragraph we prove that D satisfies the non-triviality property. By Proposition 7.5.b for D, we may assume that $i \neq m-l+1$. Then for each summand $D_{i \sqcup \sigma, i \sqcup \tau}$ of $D_{F,i}$ at least one of the sets $i \sqcup \sigma, i \sqcup \tau$ does not contain $m-l+1$ and hence does not intersect X. Hence $D_{i \sqcup \sigma, i \sqcup \tau} = A_{i \sqcup \sigma, i \sqcup \tau} + A_{i \sqcup \sigma, X}A_{i \sqcup \tau, X} = A_{i \sqcup \sigma, i \sqcup \tau}$. Thus $D_{F,i} = A_{F,i} = 1$.

7.4. (a) Take an $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = r_m$. If A is even, then $r_m = \widetilde{r_m}$, so we are done. Otherwise there is an l-element subset $X \subset [m]$ such that $A_{X,X} = 1$. Without loss of generality $X = \{m-l+1, m-l+2, \ldots, m\}$. Then by Assertion 7.3.a'

$$r_m = \operatorname{rk} A \geq \operatorname{rk} D + 1 \geq r_{m-l+1} + 1, \quad \text{where}$$

- D is the matrix defined in Assertion 7.3.a';
- the first inequality follows from Assertion 7.3.a';
- the second inequality holds because D is an $\binom{[m-l+1]}{l}$-matrix by Assertion 7.3.a'.

(b) Take an even $\binom{[m]}{l}$-matrix A such that $\operatorname{rk} A = \widetilde{r_m}$. By the non-triviality $A \neq 0$. Let X, Y, B be defined as in Assertion 7.3.b'. Then

$$\widetilde{r_m} = \operatorname{rk} A \geq \operatorname{rk} B + 2 \geq r_{m-l} + 2, \quad \text{where}$$

- the first inequality follows from Assertion 7.3.b';
- the second inequality holds because B is an even $\binom{[m]-X}{l}$-matrix by Assertion 7.2.

7.5. (a) It suffices to check that for each pair $\{\alpha,\beta\}$ the number of sets $T_{i,\{\sigma,\tau\}}$ containing $\{\alpha,\beta\}$ is odd if and only if $\alpha\cap\beta=\emptyset$ (hence this parity not depend on i). Clearly, $|\alpha\cap\beta|\le 2$.

Assume $|\alpha\cap\beta|=2$. Then $\{\alpha,\beta\}\notin T_{i,\{\sigma,\tau\}}$ for all i,σ,τ and hence $\{\alpha,\beta\}\notin A_i$ for all $i\in[5]$.

Assume $|\alpha\cap\beta|=1$. It suffices to consider the case $\alpha=\{1,2\}$, $\beta=\{1,3\}$. Then $\{\alpha,\beta\}\in T_{i,\{\sigma,\tau\}}$ iff $i=1$ and $\{\sigma,\tau\}$ is either $\big\{\{2,4\},\{3,5\}\big\}$ or $\big\{\{2,5\},\{3,4\}\big\}$ Therefore $\{\alpha,\beta\}\notin A_i$ for all $i\in[5]$.

Assume $|\alpha\cap\beta|=0$. It suffices to consider the case $\alpha=\{1,2\}$, $\beta=\{3,4\}$. Then $\{\alpha,\beta\}\in T_{i,\{\sigma,\tau\}}$ iff either

- $i=1$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{1,3,4\}\big\}$, or
- $i=2$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{2,3,4\}\big\}$, or
- $i=3$ and $\{\sigma,\tau\}=\big\{\{1,2,3\},\{3,4,5\}\big\}$, or
- $i=4$ and $\{\sigma,\tau\}=\big\{\{1,2,4\},\{3,4,5\}\big\}$, or
- $i=5$ and $\{\sigma,\tau\}=\big\{\{1,2,5\},\{3,4,5\}\big\}$.

Therefore $\{\alpha,\beta\}\in A_i$ for every $i\in[5]$.

(b) It suffices to prove that $A_{G\sqcup i,j}=A_{G\sqcup j,i}$ for each $i,j\in[m]$ and $(2l-3)$-element subset $G\subset[m]-i-j$. Denote $\overline{\sigma}:=\{i,j\}\sqcup\sigma$. Then

$$A_{G\sqcup j,i}+A_{G\sqcup i,j}\overset{(1)}{=}\sum_{\{(\sigma,\tau)\,:\,G=\sigma\sqcup\tau,\ |\sigma|=l-2\}}(A_{\overline{\sigma},i\sqcup\tau}+A_{\overline{\sigma},j\sqcup\tau})\overset{(2)}{=}$$

$$=\sum_{\{(\sigma,\tau)\,:\,G=\sigma\sqcup\tau,\ |\sigma|=l-2\}}\ \sum_{t\in\tau}A_{\overline{\sigma},\overline{\tau-t}}\overset{(3)}{=}\sum_{t\in G}\ \sum_{\{(\sigma,\nu)\,:\,G-t=\sigma\sqcup\nu,\ |\sigma|=l-2\}}A_{\overline{\sigma},\overline{\nu}}\overset{(4)}{=}0,\quad\text{where}$$

- equality (1) holds because $A_{G\sqcup j,i}$ is equal to the sum of the first summands $A_{\overline{\sigma},i\sqcup\tau}$, and $A_{G\sqcup i,j}$ is equal to the sum of the second summands $A_{\overline{\sigma},j\sqcup\tau}$;
- equality (2) holds by the linear dependence for $F=\overline{\tau}$, $P=\overline{\sigma}$;
- equality (3) is obtained by changes of the order of summation and of variable $\nu=\tau-t$;
- equality (4) holds because ordered decompositions (σ,ν) of $G-t$ into $(l-2)$-element subsets σ,ν split into pairs $\{(\sigma,\nu),(\nu,\sigma)\}$ and $A_{\overline{\sigma},\overline{\nu}}+A_{\overline{\nu},\overline{\sigma}}=0$.

References

[ACM29] *D. Hachenberger, D. Jungnickel.* Topics in Galois Fields (2020).

[Bi20] * *A. Bikeev.* Realizability of discs with ribbons on the Möbius strip. Mat. Prosveschenie, 28 (2021); erratum to appear. arXiv:2010.15833.

[Bi21] *A. I. Bikeev,* Criteria for integer and modulo 2 embeddability of graphs to surfaces, arXiv:2012.12070v2.

[DS22] *S. Dzhenzher and A. Skopenkov,* To the Kühnel conjecture on embeddability of k-complexes into $2k$-manifolds, arXiv:2208.04188.

[FK19] *R. Fulek, J. Kynčl,* $\mathbb{Z}_2$-genus of graphs and minimum rank of partial symmetric matrices, 35th Intern. Symp. on Comp. Geom. (SoCG 2019), Article No. 39; pp. 39:1–39:16, https://drops.dagstuhl.de/opus/volltexte/2019/10443/pdf/LIPIcs-SoCG-2019-39.pdf. We refer to numbering in arXiv version: arXiv:1903.08637.

[Ko21] *E. Kogan.* On the rank of $\mathbb{Z}_2$-matrices with free entries on the diagonal, arXiv:2104.10668.

[KS21] * *E. Kogan and A. Skopenkov.* A short exposition of the Patak-Tancer theorem on non-embeddability of k-complexes in $2k$-manifolds, arXiv:2106.14010.

[KS21e] *E. Kogan and A. Skopenkov.* Embeddings of k-complexes in $2k$-manifolds and minimum rank of partial symmetric matrices, arXiv:2112.06636.

[MC] * https://en.wikipedia.org/wiki/Matrix_completion#Low_rank_matrix_completion

[NKS] * *L. T. Nguyen, J. Kim, B. Shim.* Low-rank matrix completion: a contemporary survey. arXiv:1907.11705.

[PT19] *P. Paták and M. Tancer.* Embeddings of k-complexes into $2k$-manifolds. arXiv:1904.02404.

[Sk14] * *A. Skopenkov,* Realizability of hypergraphs and Ramsey link theory, arXiv:1402.0658.

[Sk20] * *A. Skopenkov,* Algebraic Topology From Geometric Viewpoint (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.

Books, surveys and expository papers in this list are marked by the stars.

Движение точек

Давид Бродский

Проект представляют: Давид Бродский, Алексей Заславский
Олег Заславский, Иван Фролов и Фёдор Нилов

Движение — это жизнь,
а жизнь — это движение!

Аристотель

1 Проективное движение

Все утверждения, сформулированные в этом параграфе в качестве лемм и теорем можно использовать без доказательства. В основном это стандартные утверждения проективной геометрии — желающие могут самостоятельно осознать их истинность.

Определение 1.1. Проективная плоскость. *Проективной плоскостью $\mathbb{RP}^2$ мы будем называть обычную плоскость, дополненную бесконечно удаленными точками, в каждой из которых пересекается свой класс параллельных прямых. Таким образом, на каждой прямой появляется новая бесконечно удаленная точка, общая для всех параллельных между собой прямых. Все бесконечно удаленные точки образуют бесконечно удаленную прямую. Прямая, дополненная бесконечно удаленной точкой, называется проективной.*

Определение 1.2. Двойное отношение четверки точек на проективной прямой. *Пусть точки A, B, C, D лежат на проективной прямой ℓ. Двойным отношением точек $(A, B; C, D)$ на прямой ℓ будем называть величину*

$$\frac{\overrightarrow{CA}}{\overrightarrow{CB}} : \frac{\overrightarrow{DA}}{\overrightarrow{DB}}$$

Будем считать, что бесконечно удаленная точка делит любой отрезок в отношении $1:1$.

Определение 1.3. Пучок прямых. *Пучком прямых $\mathcal{L}_A$ точки A будем называть множество всех прямых, проходящих через точку A.*

Отметим, что множество всех прямых одного направления образуют пучок бесконечно удаленной точки.

Определение 1.4. Двойное отношение четверки прямых одного пучка. *Пусть прямые a, b, c, d проходят через точку O (множество прямых, проходящих через точку O, называется пучком). Выберем произвольным образом на этих прямых направляющие векторы $\overrightarrow{v}_a$, $\overrightarrow{v}_b$, $\overrightarrow{v}_c$, $\overrightarrow{v}_d$. Двойным отношением прямых $(a, b; c, d)$ будем называть величину*

$$\frac{\sin\angle(\overrightarrow{v}_c, \overrightarrow{v}_a)}{\sin\angle(\overrightarrow{v}_c, \overrightarrow{v}_b)} : \frac{\sin\angle(\overrightarrow{v}_d, \overrightarrow{v}_a)}{\sin\angle(\overrightarrow{v}_d, \overrightarrow{v}_b)}$$

Замечание: *Вообще говоря, знак $\sin\angle(\overrightarrow{v}_x, \overrightarrow{v}_y)$ не определяется прямыми x и y однозначно, так как направляющий вектор можно выбрать двумя способами. Однако, если поменять направление одного из векторов, то знак инвертируется сразу у двух синусов, и значение двойного отношения не изменится.*

Определение 1.5. Двойное отношение точек на окружности. *Пусть точки A, B, C, D лежат на окружности Ω. Отметим еще одну точку O* **на окружности**. *Двойным отношением на окружности Ω точек $(A, B; C, D)$ будем называть двойное отношение прямых $(OA, OB; OC, OD)$. Корректность определения следует из того, что величина вписанного угла постоянна.*

Лемма 1.1. *Пусть точки A, B, C, D лежат на прямой ℓ, точка O вне этой прямой. Тогда*

$$(A, B; C, D) = (OA, OB; OC, OD).$$

1. Убедитесь, что если завести на плоскости комплексные координаты, то двойное отношение четырех точек на прямой или окружности с координатами a, b, c, d считается как $\frac{c-a}{c-b} : \frac{d-a}{d-b}$.

В дальнейшем мы определим двойное отношение четырех точек на произвольной конике. Для них результат последней задачи **НЕ ВЕРЕН**.

Определение 1.6. Гомография. *Будем называть отображение $\mathcal{F}$ проективным (или гомографией), если*

$$(\mathcal{F}(A), \mathcal{F}(B); \mathcal{F}(C), \mathcal{F}(D)) = (A, B; C, D).$$

Отображение может действовать между прямыми, пучками и окружностями (кониками).

Лемма 1.2. *Пусть $A, B, C \in \ell, k \in \mathbb{R}$, тогда существует единственная точка $D \in \ell$ такая, что $(A, B, C, D) = k$.*

Теорема 1.1. *Любую гомографию прямых можно разложить в композицию нескольких центральных проекций и параллельных переносов.*

Определение 1.7. Проективное движение. *Зафиксируем некоторую проективную прямую $\mathcal{T}$. Будем говорить, что переменная точка X движется по проективной прямой или окружности ℓ проективно, если существует проективное отображение $\mathcal{F}\colon \mathcal{T} \to \ell$ такое, что $X = \mathcal{F}(t \in \mathcal{T})$. Прямая $\mathcal{T}$ играет роль параметра времени.*

Давайте поясним простыми словами, что в этом определении имеется в виду. Что означает, что точка X движется с течением времени? Формально это значит, что для каждого момента t существует положение точки X на плоскости, соответствующее этому моменту. Такое соответствие может быть выражено функцией $\mathcal{F}(t)$, которая по сути действует из координатной прямой в плоскость. Однако нам иногда будет удобно подставлять «бесконечное» время, и, для того чтобы формализовать эту идею, вместо обычной прямой времени мы будем брать проективную. Так вот проективное движение с течением времени это любое движение точки по прямой или окружности, при котором выполняется странное условие на сохранение двойных отношений. То есть, если взять любые четыре момента времени (как точки на проективной прямой), то их двойное отношение должно быть равно двойному отношению четырех положений точки X, соответствующих этим моментам времени.

Аналогично определим прямую, проективно вращающуюся в пучке:

Определение 1.8. Проективно вращающаяся прямая. *Будем говорить, что переменная прямая ℓ вращается в пучке $\mathcal{L}$ проективно, если существует проективное отображение $\mathcal{F}\colon \mathcal{T} \to \mathcal{L}$ такое, что $\ell = \mathcal{F}(t \in \mathcal{T})$.*

Договоримся о некоторых обозначениях специальных гомографий, которые в дальнейшем будем использовать.

- $\ell \xrightarrow{S} \mathcal{L}_S$ проекция с центром в точке S, отображающая прямую ℓ в пучок прямых $\mathcal{L}_S$.
- $\mathcal{R}_S^{\psi}$ — поворот с центром в точке S против часовой стрелки на угол ψ.
- $\mathcal{H}_S^k$ — гомотетия с центром в точке S и коэффициентом k.

Покажем, как проективное движение помогает решать задачи.

Пример 1.1. *Пусть A_1 — точка касания вписанной окружности треугольника ABC со стороной BC, D — произвольная точка на BC. Обозначим за I_B и I_C центры вписанных окружностей $\Delta ABD, \Delta ACD$ соответственно. Докажите, что $\angle I_B A_1 I_C = 90^\circ$*

Доказательство. Разобьем решение на несколько типовых шагов.

1. Зафиксируем $\triangle ABC$ и будем проективно двигать точку I_B по биссектрисе $\angle ABC$.
2. Построим гомографию $\mathcal{F}\colon BI \to BI$, тождественность которой равносильна задаче.

   Оформим «цепочку» гомографий в виде таблички, за ℓ_b, ℓ_c обозначены биссектрисы $\angle B$ и $\angle C$ соответственно:

   $$\begin{array}{ccccccccccc} \ell_b & \xrightarrow{A} & \mathcal{L}_A & \xrightarrow{\mathcal{R}_A^{\frac{\alpha}{2}}} & \mathcal{L}_A & \xrightarrow{A} & \ell_c & \xrightarrow{A_1} & \mathcal{L}_{A_1} & \xrightarrow{\mathcal{R}_{A_1}^{\frac{\pi}{2}}} & \mathcal{L}_{A_1} & \xrightarrow{A_1} & \ell_b \\ I_B & & AI_B & & AI_C & & I_C & & A_1I_C & & A_1I'_B & & I'_B \end{array}$$

   В верхней строке указаны прямые и пучки, переводящиеся друг в друга гомографиями, в нижней — объекты, которые по ним движутся. Очевидно, что задача равносильна проверке того, что $I_B = I'_B$.
3. Проверим, что задача верна в каких-нибудь трех положениях точки I_B. Положения обычно удобно выбирать вырожденные. В этой задаче мы рассмотрим $I_B = B, I_B = I, I_B = P$, где P центр вписанной окружности треугольника ABA_1. В каждом из них задача очевидна.

Поскольку гомография однозначно восстанавливается по образам трех точек, построенное отображение из прямой ℓ_1 в себя тождественно, поэтому задача верна и при любом другом положении точки I_B. □

Давайте потренируемся решать задачи, используя проективное движение. Во многих задачах полезно помнить, что направления суть точки бесконечно удаленной прямой.

2. Прямая ℓ проективно вращается вокруг фиксированной точки P. Точка $S \neq P$ — фиксирована. Докажите, что основание перпендикуляра из точки S на ℓ движется проективно. Какова будет траектория движения этой точки?

3. Внешние биссектрисы BB_1 и CC_1 треугольника ABC пересекаются в точке I_A. Прямая ℓ, проходящая через I_A, пересекает прямые AB и AC в точках X и Y соответственно. Докажите, что прямые, симметричные прямым BY и CX относительно BB_1 и CC_1, пересекаются на B_1C_1.

4. Дан треугольник ABC и точки B_1, C_1 на сторонах AC, AB такие, что прямые BB_1, CC_1 пересекаются на высоте треугольника AA_1. Докажите, что прямые A_1B_1 и A_1C_1 симметричны относительно AA_1.

5. На чевианах AA_1, BB_1, CC_1 (то есть, пересекающихся в одной точке) треугольника ABC выбраны точки A_2, B_2 и C_2 соответственно. Положим $A_3 = BC_2 \cap B_2C$. Точки B_3 и C_3 определяются аналогично. Докажите, что прямые AA_3, BB_3 и CC_3 пересекаются в одной точке.

6. Дан ромб $ABCD$ с острым углом B. Точка O — центр описанной окружности треугольника ABC. На продолжении луча OC за точку C выбрана точка P. Прямая PD пересекается с прямой, проходящей через точку O параллельно стороне AB, в точке Q. Докажите, что $\angle AQO = \angle PBC$.

7. Остроугольный треугольник ABC вписан в окружность Ω и описан около окружности ω. Точка P выбирается на отрезке, соединяющим центры Ω и ω. Обозначим за A', B' и C' вторые пересечения прямых AP, BP и CP с Ω. Докажите, что внутренние биссектрисы $\angle BA'C, \angle CB'A$ и $\angle AC'B$ пересекаются на линии центров Ω и ω.

8. Четырехугольник $ABCD$ описан около окружности с центром I, на прямых AI и CI выбраны точки P и Q соответственно так, что угол $\angle PBQ = \frac{1}{2}\angle ABC$. Докажите, что угол $\angle PDQ = \frac{1}{2}\angle ADC$.

9. Обозначим за S проекцию ортоцентра треугольника ABC на его медиану AM. Окружность ω проходит через точки A и S и пересекает отрезки AB и AC в точках Q и P соответственно. Докажите, что отрезки BP и CQ пересекаются на ω.

10. **(a)** Пусть f — гомография проективной прямой ℓ в себя. Параметризуем конечные точки прямой переменной x. Докажите, что отображение f *дробно-линейно*, то есть $f(x) = \dfrac{ax+b}{cx+d}$, где числа a, b, c и d фиксированы. **(b)** Пусть f — гомография прямых ℓ_1 и ℓ_2. Заведем на конечной части плоскости декартовы координаты. Докажите, что $f(x,y) = \left(\dfrac{a_1x+b_1y+c_1}{dx+ey+f}, \dfrac{a_2x+b_2y+c_2}{dx+ey+f}\right)$, где числа $a_1, a_2, b_1, b_2, c_1, c_2, d, e, f$ — фиксированы. **(c)** Докажите, что любое отображение плоскости $\mathbb{R}^2$ такого вида, который описан в пункте (b) может быть однозначно продолжено до проективного преобразования проективной плоскости.

11. Отображение f из комплексной прямой $\mathbb{C}$ в себя задается в декартовых координатах как $f(z) = \dfrac{P(z)}{Q(z)}$, где P и Q — многочлены. Пусть дополнительно известно, что f биективно. Докажите, что f сохраняет двойные отношения любой четверки комплексных чисел.

2 Проективное движение +

Удивительным образом оказывается, что инверсия, суженная на окружность или прямую, также сохраняет двойные отношения!

Теорема 2.1. *Пусть при инверсии $\mathcal{I}$ окружность или прямая Ω переходит в окружность или прямую $\widetilde{\Omega}$. Тогда для любых четырех точек $A, B, C, D \in \Omega$ верно $(A, B; C, D) = (\mathcal{I}(A), \mathcal{I}(B); \mathcal{I}(C), \mathcal{I}(D))$.*

Доказательство. Ранее было доказано, что двойное отношение четвёрки точек на прямой или окружности равно двойному отношению комплексных координат этих точек. Воспользуемся этим.

Введём комплексные координаты так, что окружность, относительно которой строится инверсия $\mathcal{I}$, задаётся уравнением $z\overline{z} = 1$. Образ $\mathcal{I}(z)$ произвольной точки z плоскости будет $\mathcal{I}(z) = \dfrac{1}{\overline{z}}$.

Обозначим за a, b, c и d комплексные координаты точек и напишем:

$$(a^*, b^*; c^*, d^*) = \left(\frac{1}{\overline{a}}, \frac{1}{\overline{b}}; \frac{1}{\overline{c}}, \frac{1}{\overline{d}}\right) = \frac{\dfrac{1}{\overline{c}} - \dfrac{1}{\overline{a}}}{\dfrac{1}{\overline{c}} - \dfrac{1}{\overline{b}}} : \frac{\dfrac{1}{\overline{d}} - \dfrac{1}{\overline{a}}}{\dfrac{1}{\overline{d}} - \dfrac{1}{\overline{b}}} =$$

$$= \frac{\overline{c} - \overline{a}}{\overline{c} - \overline{b}} : \frac{\overline{d} - \overline{a}}{\overline{d} - \overline{b}} = \overline{\frac{c - a}{c - b} : \frac{d - a}{d - b}} = \frac{c - a}{c - b} : \frac{d - a}{d - b} = (a, b; c, d).$$

□

Теорема позволяет сделать следующие крайне полезное наблюдение:

12. Проекция окружности на себя. a) Пусть Ω — окружность, S — произвольная точка плоскости, не лежащая на окружности. Каждой точке $X \in \Omega$ сопоставим вторую точку $\mathcal{F}(X)$ пересечения прямой SX с Ω. Тогда отображение $\mathcal{F}\colon \Omega \to \Omega$ проективно. **b)** Докажите, что отображение, сопоставляющие точке X прямую $SX \in \mathcal{L}$ НЕ проективно.

13. Перебрасывание окружности на касательную. Пусть точка X движется по прямой ℓ, которая касается окружности Ω. Обозначим основание второй касательной из X к Ω за $Y = \mathcal{F}(X)$. Тогда отображение $\mathcal{F}\colon \ell \to \Omega$ проективно.

14. Перебрасывание окружности на себя через прямую. a) Точка X лежит на окружности Ω, ℓ — фиксированная прямая, не касающаяся Ω. Пусть касательная к Ω, восстановленная в X, пересекает ℓ в точке Z, $Y = \mathcal{F}(X)$ — основание второй касательной из Z к Ω. Тогда отображение $\mathcal{F}\colon \Omega \to \Omega$ проективно. **b)** Докажите, что отображение, сопоставляющие точке X точку $Z \in \ell$ НЕ проективно.

Доказанные выше леммы часто помогают решать задачи проективным движением.

15. Пусть γ_A, γ_B, γ_C — вневписанные окружности треугольника ABC, касающиеся сторон BC, CA, AB соответственно. Обозначим через ℓ_A общую внешнюю касательную окружностей γ_B и γ_C, отличную от BC. Аналогично определим прямые ℓ_B, ℓ_C. Из точки P, лежащей на ℓ_A, проведем отличную от ℓ_A касательную к γ_B и найдем точку X ее пересечения с ℓ_C. Аналогично найдем точку Y пересечения касательной из P к γ_C с ℓ_B. Докажите, что прямая XY касается γ_A.

16. Остроугольный треугольник ABC с ортоцентром H вписан в окружность ω с центром O. Прямая l проходит через H и пересекает меньшие дуги AB и AC в точках P и Q соответственно. Пусть AA' — диаметр окружности ω. Прямые $A'P$ и $A'Q$ пересекают BC в точках K и L соответственно. Докажите, что точки O, K, L и A' лежат на одной окружности.

17. Пусть S — проекция центра I окружности на диагональ AC описанного около нее четырехугольника $ABCD$. Докажите, что $\angle BSA = \angle DSA$.

18. Пятиугольник $ABCDE$ описан около окружности ω. Пары лучей EA и CB, AE и CD, AB и DC, BC и ED пересекаются в точах P, Q, X, Y соответственно. Окружность ω касается AE в точке R. Оказалось, что $XY \parallel AE$. Пусть окружности $(AXQ), (PYE)$ пересекаются в точках S, T. Докажите, что точки S, T, R лежат на одной прямой.

19. Прямая ℓ проходит через центр O описанной около треугольника ABC окружности, пересекая стороны AB, AC треугольника в точках P, Q. Докажите, что одна из точек пересечения окружностей, построенных на отрезках BQ, CP как на диаметрах, лежит на окружности девяти точек треугольника ABC, а вторая — на описанной около него окружности.

20. 2023 прямые пересекаются в одной точке. В каждый из 4026-и углов вписано по окружности; окружности касаются друг друга по циклу. На сторонах углов отмечено по точке. Известно, что для всех углов, кроме одного, отрезок, соединяющий отмеченные точки на сторонах, касается вписанной в угол окружности. Докажите, что для оставшегося угла это также верно.

21. Зафиксируем стороны AB и AC треугольника ABC, а также вписанную в него окружность ω. Докажите, что точка касания ω с отрезком BC проективно зависит от точки Фейербаха этого треугольника.

Теорема 2.2. Частный случай теоремы Понселе, можно использовать без доказательства. *Треугольник ABC вписан в окружность Ω и описан около окружности ω (возможно, внешним образом). Пусть точка A' также лежит на Ω, касательные из нее к ω вторично пересекают Ω в точках B' и C'. Тогда прямая $B'C'$ касается ω.*

Давайте заметим, что в данной конфигурации имеется пара биективно зависящих друг от друга точек: каждой точке A описанной окружности соответствует точка касания стороны BC со вписанной окружностью. Возникает подозрение, что подобное отображение с описанной окружности на вписанную также проективно.

Лемма 2.1. Гомографии конфигурации Понселе. *Пусть треугольник ABC вращается по Понселе с сохранением вписанной окружности. Тогда точка A_1 — касание отрезка BC со вписанной окружностью, точки S_A и T_A — середины дуг, стягивающих хорду BC, точка I_A — центр вневписанной окружности, касающейся отрезка BC; все перечисленные точки проективно зависят от точки A.*

Отображение, переводящую точку A в точку A_1, будем называть *гомографией Понселе* и обозначать ее $\mathcal{P}$.

Доказательство. Обозначим через I и O центры вписанной и описанной окружностей треугольника ABC соответственно. Заметим, что

- Середина S_A дуги BC есть образ точки A при проекции описанной окружности на себя с центром в точке I.
- Точка T_A диаметрально противоположна точке S_A.
- Точка A_1 — образ точки S_A при положительной гомотетии, переводящей описанную окружность во вписанную.
- В силу леммы о трезубце точка I_A — образ середины S_A дуги BC при гомотетии с центром в точке I и коэффициентом 2.

Явно предъявлены гомографии, по точке A строящие точки S_A, T_A, A_1, I_A, а значит они действительно проективно зависят от A. □

Обычно гомографии Понселе очень хорошо работают вместе на пару с методом полиномиального движения точек, который обобщает проективное движение. Но некоторые трудные задачи удается решить лишь уже известным нам аппаратом.

22. Выпуклый шестиугольник $AQCPBR$ вписан в окружность Ω, и при этом треугольники ABC и PQR описаны около одной и той же окружности γ. Прямая ℓ, параллельная прямой BC и не совпадающая с ней, касается γ. Пусть P_1 — точка пересечения прямой ℓ и отрезка QR. Докажите, что $\angle PAB = \angle P_1AC$.

23. Треугольники ABC и DEF описаны около окружности ω и вписаны в окружность γ. Обозначим за K и L точки касания отрезков BC и EF с окружностью ω. Положим N и M — вторые пересечения AL и DK с γ соответственно. Докажите, что прямые AM, EF, BC, ND пересекаются в одной точке.

24. Пусть оказалось, что в конфигурации Понселе вершины A и B вращающегося треугольника зависят друг от друга проективно. Докажите, что вращающийся треугольник — правильный.

Возможно, последняя задача пока покажется вам сложной. Предлагаем вернутся к ней после того, как Вы разберетесь с *принципом относительности*.

Хорошо известно, что теорема Понселе верна не только для треугольника, но и для любого n-угольника. В связи с этим возникает такой естественный вопрос:

25. Пусть многоугольник $A_1A_2\dots A_{2k+1}$ вращается по Понселе. Верно ли, что точка A_{k+1} проективно зависит от точки касания звена A_1A_{2k+1} со вписанной окружностью?

Нам не известно элементарное доказательство этого утверждения.

3 Коники

Определение 3.1. Коника. *Невырожденной коникой мы будем называть образ окружности после проективного преобразования. Вырожденной коникой называется пара прямых или прямая.*

Можно без доказательства пользоваться тем, что любая невырожденная коника это окружность, эллипс, парабола или гипербола; а также тем, что любая коника является множеством точек (x, y), удовлетворяющих уравнению $ax^2+by^2+cxy+dx+ey+f = 0$, где a, b, c, d, e, f — фиксированные вещественные числа.

Без доказательства разрешается использовать следующее утверждение:

Теорема 3.1. *Через любые пять точек, никакие три из которых не лежат на одной прямой, можно провести невырожденную конику, причем единственным образом.*

Определение 3.2. Двойное отношение четырех точек на конике. *Пусть A, B, C, D — точки на конике Ω, а S — еще одна точка на ней же. Будем называть двойным отношением четверки точек $(A, B; C, D)$ на конике двойное отношение четверки прямых $(SA, SB; SC, SD)$.*

26. Докажите, что это определение двойного отношения корректно.

27. На конике $\mathcal{C}$ нашлись три точки A, B и C, лежащие на одной прямой. Докажите, что $\mathcal{C}$ — вырожденная.

28. a) Прямые a_t и b_t проективно вращаются вокруг точек A и B соответственно. Докажите, что точка пересечения прямых a_t и b_t проективно движется по некоторой конике (возможно, вырожденной) b) Точки A_t и B_t проективно движутся по прямым a и b соответственно. Докажите, что прямая A_tB_t огибает некоторую конику (или все время проходит через фиксированную точку).

При каких условиях в предыдущей задаче коника получается вырожденной?

29. Точки A_t и B_t движутся по прямой с постоянными скоростями. Какую конику огибает соединяющая их прямая?

Коники зачастую оказываются геометрическим местом точек различных объектов.

30. Даны окружность и прямая, пересекающиеся в точках A и B. Найдите ГМТ точек, для которых касательная к окружности равна расстоянию до прямой.

31. На сторонах остроугольного треугольника ABC как на основаниях строятся подобные равнобедренные треугольники BA_1C, CB_1A, AC_1B (либо все внутрь, либо все наружу). Докажите, что прямые AA_1, BB_1, CC_1 пересекаются в одной точке, и найдите их ГМТ.

Иногда применение коник оказывается полезным в задачах, напрямую с ними не связанными.

32. В остроугольном неравнобедренном треугольнике ABC отмечены изогонально сопряжённые точки P и Q. Точка W — середина дуги BAC окружности (ABC). Прямые WP и WQ второй

раз пересекают окружность (ABC) в точках X и Y соответственно. Через точки P и Q проведены прямые, параллельные прямой AW; эти прямые пересекают стороны AB, AC в точках P_B, P_C, Q_B, Q_C. Докажите, что точки X, Y, P_B, P_C, Q_B, Q_C лежат на одной окружности.

33. Окружность, вписанная в неравнобедренный треугольник ABC, касается его сторон BC, CA и AB в точках A_1, B_1 и C_1 соответственно. Три мухи ползли по прямым AA_1, BB_1 и CC_1 с постоянными скоростями так, что в какой-то момент они находились в точках A, B и C, а в другой момент были в точках A_1, B_1 и C_1. В некоторый момент времени все три мухи находились на прямой p_1, а в некоторый другой момент — на прямой p_2. Докажите, что $p_1 \perp p_2$.

34. На сторонах AD, CD четырехугольника $ABCD$ выбраны точки P, Q так, что $\angle ABP = \angle CBQ$. Обозначим за S точку пересечения CP с AQ. Докажите, что $\angle PBS = \angle QBD$.

35. Рассмотрим произвольный треугольник ABC с центром I вписанной окружности. Прямая ℓ пересекает прямые AI, BI и CI соответственно в точках D, E, F, отличных от A, B, C и I. Серединные перпендикуляры к отрезкам AD, BE и CF образуют треугольник Δ с описанной окружностью ω. Докажите, что окружности ω и (ABC) касаются.

4 Полиномиальное движение

Определение 4.1. Проективная плоскость. *Проективной плоскостью называется множество всех прямых в пространстве, проходящих через фиксированную точку O, а эти прямые называются точками проективной плоскости.*

На каждой прямой в $\mathbb{R}^3$, проходящей через начало координат, можно выбрать любую точку (x, y, z), отличную от начала координат. Таким образом, все ненулевые тройки $[x : y : z]$ с точностью до пропорциональности кодируют точки проективной плоскости и называются *однородными координатами на плоскости*. Это определение естественно согласуется с данным ранее интуитивным: если зафиксировать в пространстве обычную плоскость $\alpha | z = 1$, не содержащую точку O, то каждой ее точке A сопоставляется прямая OA, а каждой бесконечно удаленной точке некоторого направления сопоставляется прямая, проходящая через точку O параллельно α соответствующего направления. Тройка $[0 : 0 : 0]$ не задает никакую точку проективной плоскости.

Заметим, что оси OX и OY трехмерных координат параллельны плоскости α, а ось OZ перпендикулярна ей. Спроецировав OX и OY на α, получим стандартную систему координат в этой плоскости. Точка с координатами (x, y) в этих координатах имеет однородные координаты $[x : y : 1]$. Бесконечно удаленные точки проективной плоскости имеют однородные координаты $[x : y : 0]$

Пусть p и q — две различные точки проективной плоскости α. Посмотрим на плоскость, проходящую через точки p, q и O, — она задается уравнением $ax+by+cz = 0$, где a, b и c — фиксированные числа, выбранные с точностью до пропорциональности. Однородными координатами прямой pq мы будем называть тройку чисел $[a : b : c]$ с точностью до пропорциональности. Тройка $[0 : 0 : 0]$ не задает никакую прямую.

Легко видеть, что точка $[x_0 : y_0 : z_0]$ лежит на прямой $[a : b : c]$ тогда и только тогда, когда $ax_0 + bx_0 + cz_0 = 0$, откуда прямой подстановкой следует следующее утверждение:

Лемма 4.1. *Коэффициент прямой, проходящей через точки с координатами $[x_1 : y_1 : z_1]$ и $[x_2 : y_2 : z_2]$, можно записать как*

$$[y_1z_2 - z_1y_2 : z_1x_2 - x_1z_2 : x_1y_2 - y_1x_2]$$

а координату точки пересечения двух прямых $[a_1 : b_1 : c_1]$ и $[a_2 : b_2 : c_2]$

$$[b_1c_2 - c_1b_2 : c_1a_2 - a_1c_2 : a_1b_2 - b_1a_2]$$

Аналогичным образом можно определить однородные координаты на проективной прямой, кодируя ее точки парами чисел $[x : y]$ с точностью до пропорциональности. Поскольку время — это точка проективной прямой, ее можно рассматривать как пару чисел $[t_1 : t_2]$.

Раннее мы рассматривали отображения из проективной прямой в проективную плоскость (а конкретно, в прямые и коники на ней), сохраняющие двойные отношения. Сейчас мы расширим наш арсенал *полиномиальными отображениями*, то есть такими функциями $\mathcal{F}\colon \mathbb{RP}^1 \to \mathbb{RP}^2$, которые на вход берут пару чисел t_1, t_2, а на выходе выдают тройку многочленов $P(t_1, t_2), Q(t_1, t_2)$ и $R(t_1, t_2)$, отвечающие тройке однородных координат точки на проективной плоскости.

Очевидно, что на многочлены P, Q и R нужно наложить некоторые условия, чтобы указанное отображение корректно отображало точки проективной прямой-времени в проективную плоскость.

Многочлены должны быть однородными ($t_1^2+2t_1t_2$ подходит, а $t^3+2t_1t_2$ — нет) и одинаковой степени, чтобы можно было пропорционально заменять координаты. Также мы не хотим, чтобы для каких-то t_1, t_2 все три многочлена разом обращались в ноль, для этого потребуем их взаимную простоту.

Определение 4.2. Степенная зависимость. *Будем говорить, что степень зависимости точки X от времени равна k, если однородные координаты точки X можно записать как $[P_1(t_1,t_2) : P_2(t_1,t_2) : P_3(t_1,t_2)]$, где P_i — однородные полиномы степени k от времени, которые взаимно просты в совокупности. Аналогично определим степени зависимости прямых.*

Легко понять, что такое определение корректно.

Лемма 4.2. О сложении степеней. *Пусть точки X и Y движутся со степенями a и b соответственно. Тогда степень прямой XY не выше, чем $a+b$.*

Доказательство. Обозначим однородные координаты точек за $[x_1 : x_2 : x_3]$ и $[y_1 : y_2 : y_3]$ соответственно, тогда координаты прямой XY задаются как $[x_2y_3 - x_3y_2 : x_3y_1 - x_1y_3 : x_1y_2 - y_1x_2]$. Если x_i — это многочлены степени не выше, чем a, а y_i — не выше чем b, то указанные выражения — полиномы степени не выше, чем $a+b$. Отметим, что оценка может быть не точна только в том случае, когда получившаяся тройка многочленов не взаимно проста в совокупности. □

Лемма 4.3. *Пусть точка X степени 1 движется по прямой, не проходящей через точку S. Тогда степень прямой SX также равна 1.*

Доказательство. Из леммы о сложении степеней следует, что степень прямой SX не выше, чем $0+1$. Так как прямая не неподвижна, то оценка точна. □

В следующей главе мы докажем более общую теорему: если точка X степени a движется по произвольной траектории, не проходящей через точку S, то степень прямой SX равна степени точки X.

Теорема 4.1. *Степень зависимости точки X, проективно едущей по прямой, равна 1. Степень проективно вращающейся в пучке прямой также равна* 1.

Доказательство. Для начала покажем, что любое проективное отображение из прямой в прямую можно разложить в композицию параллельных переносов и центральных проекций.

Пусть точки A, B и C прямой ℓ_1 переходят в точки A_1, B_1 и C_1 прямой ℓ_2. Если $\ell_1 \parallel \ell_2$, то спроецируем ℓ_1 на любую не параллельную им прямую и будем решать задачу для пары не параллельных прямых. Сделаем параллельный перенос прямой ℓ_1, переводящий точку A в точку A_1, точки B и C перешли при нем в B' и C'. Обозначим за S пересечение B_1B' и C_1C' (возможно, бесконечно удаленное). Проекция с центром в точке S, переводящая ℓ_1' в ℓ_2, реализует искомую гомографию.

Очевидно, что параллельный перенос не меняет степень зависимости, поэтому нужно проверить, что центральная проекция проективно движущейся по прямой точки не меняет степень зависимости — это следует из предыдущей леммы. □

Теорема 4.2. *Проективные преобразования плоскости линейно меняют однородные координаты.*

Лемма 4.4. Об удвоении степени на конике. *Точка X, проективно бегающая по окружности (конике), имеет степень зависимости* 2.

Доказательство. Отметим на окружности две фиксированные точки A, B, тогда прямые $a = AX$ и $b = BX$ вращаются проективно, следовательно точка X определяется как пересечение двух прямых со степенями зависимости 1, тогда по лемме о сложении степеней получаем требуемое. □

Замечание: Легко понять, верна и двойственная лемма: Пусть прямая ℓ вращается вокруг окружности (коники) так, что точка касания имеет степень движется проективно. Тогда степень ℓ оценивается как 2.

Теорема 4.3. *Чтобы проверить, что точка степени k всегда совпадает с точкой степени l, достаточно проверить $k + l + 1$ положение.*

Доказательство. Заметим, что совпадение точек в момент времени $[t_1 : t_2]$ равносильно тому, что отношения многочленов от t_1, t_2, задающих координаты точек, равны:

$$\begin{cases} \dfrac{P_x(t_1,t_2)}{P_y(t_1,t_2)} = \dfrac{Q_x(t_1,t_2)}{Q_y(t_1,t_2)} \\ \dfrac{P_y(t_1,t_2)}{P_z(t_1,t_2)} = \dfrac{Q_y(t_1,t_2)}{Q_z(t_1,t_2)} \\ \dfrac{P_z(t_1,t_2)}{P_x(t_1,t_2)} = \dfrac{Q_z(t_1,t_2)}{Q_x(t_1,t_2)} \end{cases}$$

Что равносильно (если соответствующая пара знаменателей не обращается в ноль):

$$\begin{cases} P_x(t_1,t_2)Q_y(t_1,t_2) = P_y(t_1,t_2)Q_x(t_1,t_2) \\ P_x(t_1,t_2)Q_z(t_1,t_2) = P_z(t_1,t_2)Q_x(t_1,t_2) \end{cases}$$

А для того, чтобы проверить тождественное совпадение однородных многочленов от двух переменных степени не выше чем $k+l$, достаточно проверить $k+l+1$ не пропорциональное положение. Действительно: если многочлен обнуляется в точках (x_i, y_i) при $y_i \neq 0$, то разделив $P(t_1, t_2)$ на t_2^d где d — степень многочлена, получим полином от одной переменной $\dfrac{t_1}{t_2}$, количество корней которого больше его степени, поэтому он тождественно равен нулю. Если же один из поданных нам моментов времени $[t : 0]$, то можно вынести t_2 как общий множитель и применить к оставшемуся предыдущее рассуждение. □

Аналогично, для проверки инцидентности прямой степени k и точки степени l также достаточно проверять $k + l + 1$ положение.

Сформулированный набор лемм является «базовым» и уже помогает решать множество не простых задач. Убедимся в этом на примере:

Пример 4.1. *На прямой BC неравнобедренного треугольника ABC выбраны точки P и Q так, что $BP = CQ$. Пусть ω — вписанная окружность треугольника, ω_A — вневписанная, касающаяся отрезка BC. S и T на окружностях ω и ω_A соответственно таковы, что PS касается ω, а QT касается ω_A. AS и AT пересекают BC в X и Y соответственно. Доказать, что $BX = CY$.*

1. Введем на плоскости однородную систему координат и время. Будем двигать точку P проективно по прямой BC. Будем обозначать степень зависимости точки за d.

2. Точка S проективно зависит от P и движется по окружности, поэтому, согласно лемме об удвоении степени точки на конике, $d(S) \leq 2$.

3. По лемме о сложении степеней $d(AS) \leq d(S) + d(A) \leq 2 + 0 = 2$

4. В силу той же леммы $d(X) \leq d(BC) + d(AS) \leq 0 + 2 = 2$. Аналогично $d(Y) \leq 2$, так как P и Q симметричны относительно M середины BC, то есть, проективно зависимы.

5. Обозначим $Y' = \mathcal{S}_M(X)$. Очевидно, $d(Y') = d(X) \leq 2$, значит, мы хотим доказать, что две точки со степенями зависимости не более чем 2 совпадают, для этого достаточно проверить $2 + 2 + 1 = 5$ положений.

6. Положения $P = C, P = B, P = A_1$ — точка касания вписанной окружности, $P = M$ – середина $BC, P = \infty$ очевидны.

При решении задач полезно понимать, как корректно обрабатывать вырожденные случаи. Пусть в какой-то момент мы хотим провести прямую через две совпадающие точки: из формул следует, что координаты этой прямой будут $[0 : 0 : 0]$ (то есть, у трех многочленов, задающих координаты прямой, будет общий множитель), что автоматически гарантирует обнуление всех последующих однородных многочленов; поэтому можно считать, что во всех вырожденных случаях условие задачи автоматически выполнено. Однако при таком подходе нужно действовать аккуратно. Разберем такой пример: точка X проективно движется по конике, точка S фиксирована на ней. Пусть требуется доказать, что некоторая точка Y степени 1 всегда лежит на прямой SX. Мы хотим правильно интерпретировать прямую SX, когда $S = X$. Если мы оцениваем степень прямой SX по лемме о сложении степеней, то ее степень не выше 2, и, при $X = S$, прямая SX «нулевая», что дает нам бесплатное положение (эффект того, что мы изначально не точно оценили степень). После этого, для решения задачи нам нужно найти еще три положения. Если же мы думаем про SX как про прямую, проективно вращающуюся в пучке точки S, то нам изначально нужно проверять три положения, но при $X = S$ прямую SX, конечно, надо интерпретировать как касательную, а не как «нулевую».

Попробуйте попрактиковаться с теорией, решив несколько упражнений.

36. Точки A и B движутся с постоянными скоростями по двум прямым. Докажите, что направление прямой AB проективно.

37. Три точки движутся проективно. Сколько положений достаточно проверить, чтобы убедиться, что они всегда лежат на одной прямой? Тот же вопрос для трех проективно вращающихся прямых.

38. Точки X и Y движутся со степенями a и b. Докажите, что середина отрезка, их соединяющего, движется со степенью не выше, чем $a + b$.

39. На окружности ω фиксирована точка P и движется точка A степени a. Точка B выбирается так, что дуга PB в два раза больше дуги PA (если считать против ч.с.). Докажите, что степень B не выше $2a$.

40. Полярное преобразование не меняет степень зависимости.

Теперь перейдем к решению задач.

41. Выпуклый шестиугольник $ABCDEF$ вписан в окружность. Треугольники ACE и BDF в пересечении образуют шестиугольник. Докажите, что главные диагонали этого шестиугольника пересекаются в одной точке.

42. Через ортоцентр остроугольного треугольника провели две перпендикулярные прямые. Докажите, что середины отрезков, которые эти прямые высекают на сторонах или продолжениях сторон треугольника, лежат на одной прямой.

43. Дан треугольник ABC и три точки P, Q, R, лежащие на одной прямой. Прямые AP, BP и CP пересекают описанную окружность треугольника ABC в точках A', B' и C'. Прямые $A'Q$, $B'Q$ и $C'Q$ пересекают ту же окружность в точках A'', B'' и C''. Прямые $A''R$, $B''R$, $C''R$ пересекают ту же окружность в точках A''', B''' и C'''. Доказать, что прямые AA''', BB''', CC''' пересекаются в одной точке, лежащей на прямой, проходящей через точки P, Q и R.

44. На описанной окружности треугольника ABC отмечена точка X. Прямые BX и CX пересекают высоты CC_1 и BB_1 в точках P, Q соответственно. Докажите, что середина отрезка PQ лежит на прямой B_1C_1.

45. В остроугольном треугольнике ABC, вписанном в окружность Ω с центром O, проведена высота AH_A. Прямые ℓ_A, ℓ_B, ℓ_C касаются окружности Ω в точках A, B, C соответственно. Точка S — ортоцентр треугольника, образованного прямыми ℓ_A, ℓ_B, ℓ_C. Докажите, что прямые OH_A и SH_A симметричны относительно прямой BC.

46. Вневписанная окружность треугольника ABC имеет центр I_A, касается отрезка BC в точке A_1 и касается прямых AB, AC в точках C_1, B_1 соответственно. На прямой I_AC_1 выбрана точка P так, что $AP \perp BI_A$. На прямой I_AB_1 выбрана точка Q так, что $AQ \perp CI_A$. Докажите, что точки P, Q, A_1 лежат на одной прямой.

47. На прямой Эйлера неравнобедренного треугольника ABC отмечена точка X, лежащая внутри треугольника; точка O — центр окружности (ABC). Прямые AX, BX, CX пересекают соответственные стороны треугольника ABC, в точках A_1, B_1, C_1. Докажите, что окружности (AOA_1), (BOB_1), (COC_1) имеют две общие точки.

48. Дан треугольник ABC с ортоцентром H. На описанной около треугольника окружности выбираются точки A_1, B_1 и C_1 так, что прямые AA_1, BB_1 и CC_1 конкуррентны. Обозначим за A_2, B_2 и C_2 точки, симметричные A_1, B_1 и C_1 относительно середин соответствующих сторон треугольника. Докажите, что точки A_2, B_2, C_2 и H лежат на одной окружности.

49. Дан треугольник ABC с ортоцентром H. На описанной около треугольника окружности выбираются точки A_1, B_1 и C_1 так, что прямые AA_1, BB_1 и CC_1 конкуррентны. Обозначим за A_2, B_2 и C_2 точки, симметричные A_1, B_1 и C_1 относительно соответствующих сторон треугольника. Докажите, что точки A_2, B_2, C_2 и H лежат на одной окружности.

50. Теорема Торнера. Пусть точки P, Q инверсны относительно окружности ABC, P_C симметрична P относительно AB, P_CQ пересекает AB в точке C'. Аналогично определяются точки A', B'. Тогда A', B', C' лежат на одной прямой.

51. Выпуклый четырехугольник $ABCD$ таков, что $\angle B = \angle D$. Докажите, что середина диагонали BD лежит на общей внутренней касательной к окружностям, вписанным в треугольники ABC

и ACD.

52. Дан треугольник ABC. Обозначим за A_1 пересечение средней линии, параллельной BC, с прямой, соединяющей основания высот на стороны AB, AC. Аналогично определим точки B_1, C_1. Докажите, что ортоцентр треугольника $A_1B_1C_1$ лежит на прямой Эйлера треугольника ABC.

53. Диагонали вписанного в окружность в ω четырехугольника $ABCD$ пересекаются в точке P. Обозначим за I_A, I_B, I_C и I_D центры окружностей, вписанных в треугольники APB, BPC, CPD и DPA соответственно. Пусть S_A, S_B, S_C и S_D середины «меньших» дуг AB, BC, CD и DA окружности ω. Докажите, что прямые I_AS_A, I_BS_B, I_CS_C и I_DS_D пересекаются в одной точке.

5 Полиномиальное движение +

В этой главе собрано три сюжета, которые можно изучать почти независимо друг от друга: обобщения ранее доказанных теорем, принцип относительности, и комбинирование теоремы Понселе с движением.

Для того, чтобы доказывать более продвинутые теоремы, связанные с полиномиальным движением, нам понадобится более мощный арсенал, чем вещественные числа. Все определения и теоремы предыдущей главы работают и для комплексных чисел. Вместо проективной прямой $\mathbb{RP}^1$ мы будем рассматривать $\mathbb{CP}^1$ — множество прямых, проходящих через $(0,0)$ в $\mathbb{C}^2$. Однородные координаты на проективной комплексной прямой это пары чисел $[z_1 : z_2]$, выбирающиеся с точностью до пропорциональности. То же и с комплексной проективной плоскостью $\mathbb{CP}^2$ и ее однородными координатами, пучками и т.д. Отметим, что многие результаты предыдущих глав также верны и для комплексных чисел. Комплексную единичную окружность на $\mathbb{C}^2$ нужно мыслить как множество решений уравнения $x^2+y^2=1$ в комплексных числах, а на $\mathbb{CP}^2$ как множество точек $[x : y : z]$, для которых $x^2+y^2=z^2$. Любая невырожденная коника получается из окружности проективным преобразованием (переводящем прямые в прямые) и может быть задана множеством нулей однородного неприводимого полинома $P(x,y,z)=0$.

54. Докажите, что комплексная прямая и невырожденная комплексная коника имеют не более двух общих точек. Могут ли они не пересекаться?

Комплексные числа лучше вещественных тем, что любой непостоянный полином $f(x)$ имеет корень (этим можно пользоваться без доказательств). Более того, любая кривая степени n на $\mathbb{CP}^2$ (то есть, множество нулей однородного полинома степени n) пересекается с кривой степени m по mn точкам с учетом кратности. Это утверждение называется обобщенной теоремой Безу. В этой главе теорема Безу нам не понадобится — мы будем использовать лишь такой его частный случай:

55. а) Докажите, что однородный непостоянный многочлен $f(t_1,t_2)$ делится на некоторый линейный однородный многочлен at_1+bt_2 **б)**. Докажите, что любой однородный многочлен $f(t_1,t_2)$ единственным образом (с точностью до перестановок и умножения на константы) раскладывается в произведение $p_1^{\alpha_1}p_2^{\alpha_2}...p_n^{\alpha_n}$, где p_i — однородные линейные полиномы от двух переменных.

Не вооруженным взглядом видно, что последняя задача — аналог основной теоремы арифметики.

Лемма 5.1. ***Комплексная лемма о сложении степеней.*** *Пусть точки X и Y движутся со степенями a и b соответственно. Тогда степень прямой XY не выше чем $a+b$, причем если точки X и Y в любой момент времени различны, то эта оценка точная.*

Доказательство. Обозначим однородные координаты точек за $[x_1 : x_2 : x_3]$ и $[y_1 : y_2 : y_3]$ соответственно, тогда координаты прямой XY задаются как $[x_2y_3-x_3y_2 : x_3y_1-x_1y_3 : x_1y_2-y_1x_2]$. Если x_i — это многочлены степени не выше, чем a, а y_i — не выше чем b, то указанные выражения — полиномы степени не выше, чем $a+b$. Если оценка не точна, то у трех получившихся многочленов есть общий непостоянный множитель $d(t_1,t_2)$. Выберем у d любой линейный делитель $p=at_1+bt_2$. Тогда в момент времени $[b : -a]$ прямая XY была нулевая, то есть точки X и Y совпадали, противоречие. □

Лемма 5.2. *Пусть точка X степени a движется по прямой, не проходящей через точку S. Тогда степень прямой SX также равна a.*

Доказательство. Следует из предыдущего утверждения. □

Суммируя все вышеперечисленное получаем:

Теорема 5.1. *Пусть f — гомография прямых или пучков. Тогда f не меняет степень зависимости.*

Осталось разобраться с гомографиями, задействующими коники. Мы уже доказали, что при перебрасывании точки на конику ее степень удваивается. Верно и обратное.

Теорема 5.2. ***(О сбрасывании точки с коники).*** *Точка X степени k движется по конике, точка S фиксирована на ней. Тогда степень прямой SX равна $\frac{k}{2}$, в частности, k — четно.*

Эту теорему, разбитую на задачи, Вы докажете (или нет) самостоятельно (все объекты в них предполагаются комплексными).

56. Дана коника ω. Выберем произвольную точку S ВНЕ коники и прямую ℓ, не содержащую S. Пусть f — проекция коники из точки S на прямую ℓ. Докажите, что у всех точек прямой по два прообраза, кроме, быть может, конечного числа.

57. Точка X полиномиально движется по конике ω. Выберем НА ω произвольную точку T и рассмотрим проекцию ω из T на прямую $z = 0$. Пусть образ точки X при этой проекции — это X'. Таким образом, мы построили отображение g из комплексной прямой-времени в прямую $z = 0$. **a)** Докажите, что существует такое число k, что у всех точек прямой $z = 0$ кроме, быть может, конечного числа ровно k прообразов при отображении g. **b)** Докажите, что точка X посетила почти все точки ω ровно k раз.

58. Обозначим за X'' образ точки X при отображении f из пред-предыдущей задачи. Посчитайте двумя способами, сколько раз точка X'' посетила общую точку прямой ℓ и выведите отсюда утверждение теоремы.

Начнем следующий сюжет с некоторого мотивирующего примера. Предположим, что вершины некоторого треугольника движутся со степенями a, b и c соответственно. Как можно оценить степень центра описанной около него окружности? Несложные вычисления показывают, что степень середины отрезка, соединяющего точки со степенями a и b, движется со степенью не выше, чем $a + b$. Направление прямой, соединяющей вершины степеней a и b, также имеет степень не выше, $a + b$, поэтому серединный перпендикуляр к соответствующей стороне треугольника имеет степень не выше, чем $(a+b)+(a+b) = 2(a+b)$ (согласно лемме о сложении степеней). Аналогично, серединный перпендикуляр к стороне треугольника с вершинами степени a и c имеет степень не выше, чем $2(a+c)$. Пересекая эти серединные перпендикуляры и вновь применяя принцип сложения степеней, получим, что центр окружности движется со степенью не большей, чем $4a + 2b + 2c$.

Это оценка заставляет задуматься: получившееся выражение не симметрично по степеням вершин треугольника, что странно. Вероятно, это должно означать, что предъявленная нами оценка не точна. Более того, появляется разумное подозрение, что реально можно оценить степень просто как $2(a + b + c)$. Давайте заведем инструмент, который позволит нам доказать нашу гипотезу.

Определение 5.1. Полиномиальная подстановка. *Предположим, что на проективной плоскости зафиксированы произвольные подмножества $P_1, P_2, ...P_n$ и для любого набора точек $p_1 \in$*

$P_1, p_2 \in P_2 ..., p_n \in P_n$ определена точка $[p_{0_x} : p_{0_y} : p_{0_z}] = \mathcal{R}(p_1, p_2, ..., p_n)$, причем существуют однородные многочлены R_x, R_y, R_z от $3n$ переменных такие, что $p_{0_x} = R_x(p_{1_x}, p_{1_y} ... p_{n_z})$ и аналогично для p_{0_y} и p_{0_z}. Более того потребуем, чтобы многочлены $\mathcal{R}_x, \mathcal{R}_y$ и $\mathcal{R}_z$ были однородными многочленами одинаковой степени отдельно по координатам каждой из точек p_i. Такое $\mathcal{R}$ будем называть полиномиальной подстановкой от n переменных.

Определение 5.2. Относительная степень зависимости. *Пусть $\mathcal{R}$ — некоторая полиномиальная подстановка от двух переменных, точки q_1 и q_2 движутся с некоторыми степенями зависимости, также $q = \mathcal{R}(q_1, q_2)$. Пусть r_1 наименьшее такое натуральное число, что для любого фиксированного момента времени $[\tau_1 : \tau_2]$ степень зависимости точки $\mathcal{R}(q_1, q_2(\tau_1, \tau_2))$ не выше, чем r_1 (при разных фиксированных $[\tau_1 : \tau_2]$ степень может быть разной). Такое r_1 мы будем называть относительно степенью точки q от точки q_1.*

Аналогично определяются относительные степени точки, зависящей более, чем от двух. Нужно фиксировать все точки q_i и смотреть на степень зависимости точки q, когда она зависит только от одной переменной точки.

59. Принцип относительности. Пусть точки $q_1, q_2 ..., q_n$ движутся полиномиально, и относительные степени точки $q = \mathcal{R}(q_{1_t}, q_{2_t}, ...q_{n_t})$ равны $r_1, r_2, ...r_n$ для некоторой полиномиальной подстановки $\mathcal{R}$. Тогда степень зависимости точки q не выше, чем $r_1 + r_2 + ... + r_n$.

60. Пусть вершины треугольника двигаются со степенями a, b и c соответственно, тогда центр описанной около этого треугольника окружности и его ортоцентр оба имеют степень зависимости не больше, чем $2(a + b + c)$.

61. Точки A и B движутся по конике ω проективно. **a)** Докажите, что прямая AB огибает некоторую конику γ. **b)** Докажите, что коники ω и γ касаются в двух точках на $\mathbb{CP}^2$ (то есть, точки касания могут иметь комплексные координаты). **c)** Докажите, что в конфигурации Понселе соседние вершины треугольника зависят друг от друга проективно тогда и только тогда, когда вращающийся треугольник — правильный.

62. Точки A и B едут по одной и той же конике проективно. Докажите, что пересечение касательных к конике в точках A и B проективно движется по некоторой конике.

63. Пусть точка A движется по конике со степенью $2a$, точка B движется по произвольной траектории со степенью b. Обозначим за C второе пересечение прямой AB с коникой. Тогда степень зависимости точки C не выше чем $2a + 2b$.

64. Точки движутся со степенями a, b, c и d. Докажите, что для того, чтобы проверить то, что они лежат на одной окружности, достаточно $2(a + b + c + d) + 1$ положение.

Часто оказывается эффективным применение поризма Понселе не только ко вписанной и описанной окружности треугольника, но и ко вневписанной и описанной. При такой конфигурации есть шесть вырожденных положений: параметризуем динамику касательной ℓ, вращающейся вокруг вневписанной окружности; можно выбрать два положения, когда ℓ касается описанной и вневписанной окружности, два положения, когда ℓ проходит через общие точки окружностей, а также два положения, когда получающиеся треугольник равнобедренный.

65. Обозначим за Ω и ω описанную и вневписанную окружности треугольника ABC. Пусть они

пересекаются в точках X и Y. Общие внешние касательные Ω и ω касаются Ω в U и V. Докажите, что касательные к ω в X и Y проходят через U и V.

66. Обозначим за ω вневписанную окружность треугольника ABC, касающуюся отрезка BC. Общие внешние касательные к ω и (ABC) касаются (ABC) в точках X и Y. Докажите, что прямая XY проходит через основания биссектрис, проведенных из вершин B и C.

67. Вневписанная окружность ω треугольника ABC касается отрезка BC в точке A_1 и пересекает описанную окружность (ABC) в точках X и Y. Касательные к ω в точках X и Y пересекаются в точке Z. Обозначим за S середину дуги BAC. Докажите, что прямые SA_1 и AZ пересекаются на (ABC).

68. Вневписанная окружность ω треугольника ABC касается отрезка BC в точке D и пересекает описанную окружность (ABC) в точках K и L. Обозначим за E основание высоты треугольника из вершины A. Докажите, что на прямых KD и LD найдутся такие точки V и N, что четырехугольник $EVAN$ — ромб.

69. Прямая ℓ степени d вращается вокруг точки O. Зафиксируем два различных вектора $\overrightarrow{OA}$ и $\overrightarrow{OB}$, с началом в точке O. Докажите, что $\dfrac{\sin\angle(\ell,\overrightarrow{OA})}{\sin\angle(\ell,\overrightarrow{OB})} = \dfrac{P(t_1,t_2)}{Q(t_1,t_2)}$, где $P(t_1,t_2)$ и $Q(t_1,t_2)$ — однородные полиномы степени d от двух переменных.

70. Пусть ABC треугольник с описанной окружностью ω и вневписанной окружностью Ω_A, касающейся отрезка BC. Обозначим пересечения этих окружностей за X и Y соответственно. Точки P и Q — проекции точки A на касательные в точках X и Y к Ω_A. Точка R — пересечение касательной к окружности (APX) в точке P с касательной к окружности (AQY) в точке Q. Докажите, что $AR \perp BC$.

Решения некотрых задач

6. Дан ромб $ABCD$ с острым углом B. Точка O — центр описанной окружности треугольника ABC. На продолжении луча OC за точку C выбрана точка P. Прямая PD пересекается с прямой, проходящей через точку O параллельно стороне AB, в точке Q. Докажите, что $\angle AQO = \angle PBC$.

Доказательство. Зафиксируем ромб и будем двигать точку P по прямой OC проективно.

$$\begin{array}{ccccccccccc} \mathcal{L}_A & \overset{A}{\to} & OC & \overset{D}{\to} & \mathcal{L}_D & \overset{D}{\to} & \ell & \overset{A}{\to} & \mathcal{L}_A & \overset{f}{\to} & \mathcal{L}_B \\ AP & & P & & DP & & Q & & AQ & & AP' \end{array}$$

Мы хотим проверить, что $AP = AP'$, где f сдвиг на вектор $\overrightarrow{AB}$ и поворот на угол $B2$ против чс. Положения $P = O, P = B, P = \inf$ очевидны. □

11. Отображение f из комплексной прямой $\mathbb{C}$ в себя задается в декартовых координатах как $f(z) = \dfrac{P(z)}{Q(z)}$, где P и Q — многочлены. Пусть дополнительно известно, что f биективно. Докажите, что f сохраняет двойные отношения любой четверки комплексных чисел.

Доказательство. НУО многочены взаимно просты. Известно, что для любого $c \in \mathbb{C}$ уравнение $P(z) - cQ(z) = 0$ имеет ровно один корень. Выберем c так, чтобы член при старшей чтепени не сокращался. Предположим, что P или Q степени хотя бы 2, тогда многочлен $P(z) - cQ(z)$ должен иметь кратные корни, то есть для единственного его корня z_0 выполненно $P(z_0) - cQ(z_0) = 0$ и $P'(z_0) - cQ'(z_0) = 0$. Домножим первое равенство на $Q'(z_0)$, второе на $Q(z_0)$ и вычтем. Получим $P(z_0)Q'(z_0) - P'(z_0)Q(z_0) = 0$, то есть, при $Q(z_0) \neq= 0$ (а это верно почти при всех c) $\left(\dfrac{P}{Q}\right)'(z_0) = 0$. Таким образом, для всех z кроме, быть может, конечного числа верно $\left(\dfrac{P}{Q}\right)'(z_0) = 0$, откуда $\dfrac{P(z)}{Q(z)} = const$, что противоречит взаимной простоте многочленов. □

14. Проекция окружности на себя. a) Пусть Ω — окружность, S — произвольная точка плоскости, не лежащая на окружности. Каждой точке $X \in \Omega$ сопоставим вторую точку $\mathcal{F}(X)$ пересечения прямой SX с Ω. Тогда отображение $\mathcal{F}\colon \Omega \to \Omega$ проективно. **b)** Докажите, что отображение, сопоставляющие точке X прямую $SX \in \mathcal{L}$ НЕ проективно.

Доказательство.

Точка S вне Ω:

Заметим, что $SX \cdot SY = const$. Тогда проекцию окружности на себя можно представить как $Y = \mathcal{I}_S^{\sqrt{SX \cdot SY}}$

Точка S внутри Ω: Заметим, что $Y = \mathcal{S}_S \circ \mathcal{I}_S^{\sqrt{SX \cdot SY}}$

Пункт b) следует из того, что люое проективное отображение должно быть проективно.

□

13. Перебрасывание окружности на касательную. Пусть точка X движется по прямой ℓ, которая касается окружности Ω. Обозначим основание второй касательной из X к Ω за $Y = \mathcal{F}(X)$. Тогда отображение $\mathcal{F}\colon \ell \to \Omega$ проективно.

Доказательство. $Y = \mathcal{H}_S^2 \circ \mathcal{I}_\Omega$, где S точка касания прямой ℓ с окружностью. □

14. Перебрасывание окружности на себя через прямую. a) Точка X лежит на окружности Ω, ℓ — фиксированная прямая, не касающаяся Ω. Пусть касательная к Ω, восстановленная в X, пересекает ℓ в точке Z, $Y = \mathcal{F}(X)$ — основание второй касательной из Z к Ω. Тогда отображение $\mathcal{F}\colon \Omega \to \Omega$ проективно. **b)** Докажите, что отображение, сопоставляющие точке X точку $Z \in \ell$ НЕ проективно.

Доказательство. Пусть L полюс прямой ℓ относительно Ω. Заметим, что XZ поляра точки $Y \in \ell$, значит, $L \in XZ$, тогда $\mathcal{F}$ просто проекция окружности на себя с центром в фиксированной точке L.

Пункт b) следует из того, что люое проективное отображение должно быть проективно. □

22. Выпуклый шестиугольник $AQCPBR$ вписан в окружность Ω, и при этом треугольники ABC и PQR описаны около одной и той же окружности γ. Прямая ℓ, параллельная прямой BC и не совпадающая с ней, касается γ. Пусть P_1 — точка пересечения прямой ℓ и отрезка QR. Докажите, что $\angle PAB = \angle P_1AC$.

Доказательство.

1. Будем двигать P по Ω проективно, зафиксировав треугольник ABC, тогда треугольник PQR будет вращаться по Понселе. По доказанной лемме точка P_2 касания γ с отрезком QR это образ точки P при гомографии Понселе. Согласно лемме о перебрасывании на касательную, примененной к окружности γ и касательной ℓ получаем, что точка P_1 проективно зависит от точки P_2, обозначим соответствующую гомографию за $\mathcal{F}$, за g — внутреннюю биссектрису $\angle BAC$.

2. $$\begin{array}{ccccccccccc} \Omega & \overset{\mathcal{P}}{\to} & \gamma & \overset{\mathcal{F}}{\to} & \ell & \overset{A}{\to} & \mathcal{L}_A & \overset{\mathcal{S}_g}{\to} & \mathcal{L}_A & \overset{A}{\to} & \Omega \\ P & & P_2 & & P_1 & & AP_1 & & AP' & & P' \end{array}$$

3. Утверждение задачи равносильно совпадению точек P и P', поэтому достаточно доказать его для каких-нибудь трех положений точки P. Положения $P = A, B, C$ очевидны.

□

28. a) Прямые a_t и b_t проективно вращаются вокруг точек A и B соответственно. Докажите, что точка пересечения прямых a_t и b_t проективно движется по некоторой конике (возможно, вырожденной) b) Точки A_t и B_t проективно движутся по прямым a и b соответственно. Докажите, что прямая A_tB_t огибает некоторую конику (или все время проходит через фиксированную точку).

Доказательство. Рассмотрим три точки X, Y, Z, принадлежащие ГМТ. Проведем конику Ω через точки A, B, X, Y, Z. Пусть прямая l_T, проходящая через A пересекает конику в точке T, а соответствующая ей прямая, проходящая через B пересекает Ω в точке T'. Обозначим за l_i прямые, проходящие через A, k_i — через B. Тогда:$(X, Y; Z, T) = (\ell_X, \ell_Y; \ell_Z; \ell_T) = (k_X, k_Y; k_Z; k_{T'}) = (X, Y; Z, T')$

Откуда следует, что $T = T'$. Более того видно, что точка T движется по конике проективно.

Двойственное утверждение получектся полярным преобразованием.

□

32. В остроугольном неравнобедренном треугольнике ABC отмечены изогонально сопряжённые точки P и Q. Точка W — середина дуги BAC окружности (ABC). Прямые WP и WQ второй раз пересекают окружность (ABC) в точках X и Y соответственно. Через точки P и Q проведены прямые, параллельные прямой AW; эти прямые пересекают стороны AB, AC в точках P_B, P_C, Q_B, Q_C. Докажите, что точки X, Y, P_B, P_C, Q_B, Q_C лежат на одной окружности.

Доказательство. Точки P_B, P_C, Q_B, Q_C образуют равнобедренную трапецию, поэтому лежат на одной окружности. Мы докажем, что точки P_B, P_C, X, Y лежат на одной окружности; аналогично доказывается про точки Q_B, Q_C, X, Y. Если эти три окружности не совпадают, то их радикальные оси P_BP_C, Q_BQ_C и XY пересекаются в одной точке. Из соображений непрерывности можно понять, что окружности совпадают.

Фиксируем треугольник ABC и точки P_B, P_C и двигаем точку P по прямой P_BP_C. Тогда точка Q движется по конике, проходящей через вершины треугольника ABC, а также точку W, изогонально сопряженную бесконечно удаленной точке прямой P_BP_C. Поэтому прямые WP, WQ, а значит, и точки X, Y двигаются проективно. Пусть XP_B и YP_C вторично пересекают окружность (ABC) в точках S и T. Достаточно доказать, что $ST \parallel P_BP_C$. Поскольку точки S и T движутся проективно, то достаточно проверить 3 положения. Положения, когда $P = P_B$, $P = P_C$, и когда P на окружности (ABC), очевидны. □

36. Точки A и B движутся с постоянными скоростями по двум прямым. Докажите, что направление прямой AB проективно.

Доказательство. Напомним, что направление прямой AB — бесконечно удаленная точка прямой AB. Выберем неподвижную точку O и отложим от нее вектор $\overrightarrow{OC} = \overrightarrow{AB}$. Поскольку точка C движется линейно, то направление прямой OC зависит от времени проективно, что и требовалось. □

37. Три точки движутся проективно. Сколько положений достаточно проверить, чтобы убедиться, что они всегда лежат на одной прямой? Тот же вопрос для трех проективно вращающихся прямых.

Доказательство. Проективно движущиеся по прямым точки имеют степень зависимости 1. Проведем прямую через две из данных точек, она имеет степень зависимости не выше 2. Чтобы проверить, что на ней лежит оставшаяся точка степени 1, нужно проверить 4 положения. Рассуждение для проективно вращающихся прямых двойственно рассуждению для точек. □

38. Точки X и Y движутся со степенями a и b. Докажите, что середина отрезка, их соединяющего, движется со степенью не выше, чем $a + b$.

Доказательство. Пусть точки имеют однородные координаты $[x_1 : y_1 : z_1]$ и $[x_2 : y_2 : z_2]$. Тогда их декартовы координаты $(\frac{x_1}{z_1}, \frac{y_1}{z_1})$ и $(\frac{x_2}{z_2}, \frac{y_2}{z_2})$, а декартовы координаты середины имеют вид $(\frac{x_1z_2+x_2z_1}{2z_1z_2}, \frac{y_1z_2+y_2z_1}{2z_1z_2})$. Тогда однородные координаты середины $[x_1z_2 + x_2z_1 : y_1z_2 + y_2z_1 : 2z_1z_2]$ — многочлены степени $a + b$ от времени. □

40. Полярное преобразование не меняет степень зависимости.

Доказательство. Проективные преобразования плоскости линейны в однородных координатах, поэтому не меняют степень зависимости. Сделаем проективное преобразование, переводящее конику в единичную окружность $x^2 + y^2 = z^2$. Несложно видеть, что поляра точки $[x : y : z]$ относительно этой окружности — прямая с координатами $[x : y : -z]$, откуда следует, что степень зависимости сохраняется. □

47. На прямой Эйлера неравнобедренного треугольника ABC отмечена точка X, лежащая внутри треугольника; точка O — центр окружности (ABC). Прямые AX, BX, CX пересекают соответственные стороны треугольника ABC, в точках A_1, B_1, C_1. Докажите, что окружности (AOA_1), (BOB_1), (COC_1) имеют две общие точки.

Доказательство. Считаем, что треугольник неравнобедренный. Пусть A_2, B_2, C_2 — образы A_1, B_1, C_1 при инверсии относительно описанной окружности. Будем доказывать, что прямые AA_2, BB_2, CC_2 пересекаются в одной точке. Фиксируем треугольник ABC и двигаем X по прямой Эйлера. Заметим, что A_2, B_2, C_2 двигаются проективно по окружностям, поэтому их степени зависимости равны 2. Нужно проверить 7 положений. Если X лежит на одной из сторон треугольника, утверждение очевидно. Положения, когда X — ортоцентр, точка пересечения медиан и центр описанной окружности, легко проверяются. Найдем 7-ое положение: пусть окружность (BOC) пересекает AB и AC в точках X и Y; и пусть M и N — середины AB и AC. Тогда XN и YM пересекаются в точке O, и по теореме Паппа точка X пересечения CX и BY лежит на прямой Эйлера. Она и будет седьмым положением. □

Point moving

David Brodsky

Presented by: David Brodsky, Alexey Zaslavskiy, Oleg Zaslavskiy, Ivan Frolov and Fedor Nilov

Life requires movement

Aristotle

1 Projective movement

Lemmas and theorems formulated in this section may be used without proof. As usually they are standard assertions of projective geometry — if you want it is not hard to verify their correctness.

Definition 1.1 Projective plane. *The projective plane* $\mathbb{RP}^2$ *is the Euclidean plane completed by infinite points, each such point is the common point of some class of parallel lines. So each line is completed by one infinite point, and this point is the same for all parallel lines. All infinite points form the infinite line. A line completed by an infinite point is called a projective line.*

Definition 1.2 Cross-ratio of four points on a projective line *Let points* A, B, C, D *lie on a projective line* ℓ*. The cross-ratio* $(A, B; C, D)$ *of these points on* ℓ *is the value*

$$\frac{\overrightarrow{CA}}{\overrightarrow{CB}} : \frac{\overrightarrow{DA}}{\overrightarrow{DB}}$$

We suppose that an infinite point divide any segment in ratio $1 : 1$*.*

Definition 1.3 Pencil of lines. *The pencil of lines* $\mathcal{L}_A$ *of point* A *is the set of all lines passing through* A*.*

Not that the set of all parallel lines is the pencil of the corresponding infinite point.

Definition 1.4 Cross-ratio of four lines on a pencil. *Let lines* a, b, c, d *pass through a point* O *(the set of lines passing through* O *is a pencil). Choose arbitrary directing vectors* $\overrightarrow{v}_a, \overrightarrow{v}_b, \overrightarrow{v}_c, \overrightarrow{v}_d$ *on these lines. The cross-ratio* $(a, b; c, d)$ *of the given lines is the value*

$$\frac{\sin\angle(\overrightarrow{v}_c, \overrightarrow{v}_a)}{\sin\angle(\overrightarrow{v}_c, \overrightarrow{v}_b)} : \frac{\sin\angle(\overrightarrow{v}_d, \overrightarrow{v}_a)}{\sin\angle(\overrightarrow{v}_d, \overrightarrow{v}_b)}$$

Remark: *Generally the sign of* $\sin\angle(\overrightarrow{v}_x, \overrightarrow{v}_y)$ *is not defined by the lines* x *and* y*, because we may choose the directing vector by two ways. But if we change the direction of one vector, the signs of two sines invert, and the value of the cross-ratio does not change.*

Definition 1.5 Cross-ratio of points on a circle *Let points A, B, C, D lie on a circle Ω. Mark an arbitrary point O* **on this circle**. *The cross-ratio $(A, B; C, D)$ of points on Ω is he cross-ratio of lines $(OA, OB; OC, OD)$. This definition is correct because the value of an inscribed angle is constant.*

Lemma 1.1 *Let points A, B, C, D lie on a line ℓ, and a point O lie not on this line. Then*

$$(A, B; C, D) = (OA, OB; OC, OD)$$

1. Let we consider points of the plane as complex numbers. Make sure that the cross-ratio of four points of a line or a circle corresponding to a, b, c, d equals $\frac{c-a}{c-b} : \frac{d-a}{d-b}$.

Later we will define the cross-ratio for four points of an arbitrary conic. In this case the result of the last problem **IS NOT CORRECT**.

Definition 1.6 Homography. *A map $\mathcal{F}$ is called projective, or homography if*

$$(\mathcal{F}(A), \mathcal{F}(B); \mathcal{F}(C), \mathcal{F}(D)) = (A, B; C, D)$$

. The map may transform a line, a pencil or a circle (a conic) to a line, a pencil or a circle (a conic).

Lemma 1.2 *Let $A, B, C \in \ell, k \in \mathbb{R}$, then there exists a unique point $D \in \ell$ such that $(A, B, C, D) = k$.*

Theorem 1.1 *Each homography of lines may be presented as a composition of several central projections and parallel translations.*

Definition 1.7 Projective movement. *Fixe some projective line $\mathcal{T}$. Say that a point X moves on a projective line or a circle ℓ projectively, if there exists a projective map $\mathcal{F}\colon \mathcal{T} \to \ell$ such that $X = \mathcal{F}(t \in \mathcal{T})$. The line $\mathcal{T}$ may be considered as the axis of time.*

A projective rotation of a line on a pencil is defined similarly.

Definition 1.8 The line rotating projectively *The line ℓ rotates projectively in the pencil $\mathcal{L}$ if there exists a projective map $\mathcal{F}\colon \mathcal{T} \to \mathcal{L}$*

such that $\ell = \mathcal{F}(t \in \mathcal{T})$.

Later we will use the following notations for several special homographies.

- $\ell \overset{S}{\to} \mathcal{L}_S$ — projection centered at point S, mapping a line ℓ to a pencil $\mathcal{L}_S$.
- $\mathcal{R}_S^{\psi}$ — rotation centered at S to angle ψ counterclockwise.

- $\mathcal{H}_S^k$ — homothety centered at S with coefficient k

Demonstrate, how the projective movement helps to solve problems.

Example 1.1 *Let A_1 be the touching point of the incircle of triangle ABC with the side BC, and D be an arbitrary point on BC. Denote as I_B and I_C the incenters of triangles $\Delta ABD, \Delta ACD$ respectively. Prove that $\angle I_B A_1 I_C = 90^\circ$*

Divide the solution into several typical steps.

1. Fix ΔABC and move projectively I_B on the bisector of $\angle ABC$.
2. Construct a homography $\mathcal{F}\colon BI \to BI$, the identity of this homography is equivalent to the required assumption.

   Present «a chain» of homographies as a table, denote as ℓ_b, ℓ_c the bisectors of $\angle B$ and $\angle C$ perspectively:

   $$\begin{array}{ccccccccccc} \ell_b & \overset{A}{\to} & \mathcal{L}_A & \overset{\mathcal{R}_A^{\frac{\alpha}{2}}}{\longrightarrow} & \mathcal{L}_A & \overset{A}{\to} & \ell_b & \overset{A_1}{\to} & \mathcal{L}_{A_1} & \overset{\mathcal{R}_{A_1}^{\frac{\pi}{2}}}{\longrightarrow} & \mathcal{L}_{A_1} & \overset{A_1}{\to} & \ell_b \\ I_B & & AI_B & & AI_C & & I_C & & A_1 I_C & & A_1 I'_B & & I'_B \end{array}$$

   We indicate the lines and the pencils transformed by the homographies in the top row, and the corresponding moving objects in the bottom one. The assumption of the problem is equivalent to the identity $I = I'$
3. Verify that the assumption is correct for some three positions of I_B. As usually it is useful to choose degenerated positions. For the given problem consider $I_B = B, I_B = I, I_B = P$, where P is the incenter of triangle ABA_1. For each of these cases the problem is clear. Since a homography is uniquely defined by the images of three points, the constructed homography of ℓ_1 is the identity, hence the assumption is correct for any position of I_B.

   Now train to solve problems using the projective movement. In several problems it is useful to remember that directions are points of the infinite line.

2. A line ℓ rotates projectively around a fixed point P. A point $S \neq P$ is fixed. Prove that the projection of S to ℓ moves projectively. Find the trajectory of this point

3. The external bisectors BB_1 and CC_1 of triangle ABC meet at point I_A. A line ℓ passing through I_A meets AB and AC at points X and Y respectively. Prove that the reflections of BY and CX about BB_1 and CC_1 respectively meet on B_1C_1.

4. Let points B_1, C_1 lie on the sides AC, AB of triangle ABC in such a way that lines BB_1, CC_1 meet on the altitude AA_1. Prove that the lines A_1B_1 and A_1C_1 are symmetric with respect to AA_1.

5. Points A_2, B_2 and C_2 lie on cevians AA_1, BB_1, CC_1 (i.e. concurrent lines) respectively of triangle ABC. Let $A_3 = BC_2 \cap B_2C$. points B_3 and C_3 are defined similarly. Prove that AA_3, BB_3 and CC_3 concur.

6. Let $ABCD$ be a rhombus with acute angle B. Let O the circumcenter of triangle ABC. A point P lie on the extension of OC beyond C. The line PD meets the line passing through O and parallel to AB at point Q. prove that $\angle AQO = \angle PBC$.

7. Let ABC be an acute-angled triangle with circumcircle Ω and incircle ω. A point P lies on a segment joining the centers of Ω and ω. Denote as A', B' and C' the second common points of AP, BP and CP with Ω. Prove that the internal bisectors of $\angle BA'C, \angle CB'A$ and $\angle AC'B$ concur at a point lying on the center line of Ω and ω.

8. Let $ABCD$ be a circumscribed quadrilateral with incenter I. Points P and Q lie on AI and CI respectively in such a way that $\angle PBQ = \frac{1}{2}\angle ABC$. Prove that $\angle PCQ = \frac{1}{2}\angle ADC$

9. Let S be the projection of the orthocenter of triangle ABC to the median AM. A circle ω passes through A and S, and meets AB and AC at Q and P respectively. Prove that BP and CQ meet on ω.

10. a) Let f be a homography of a projective line ℓ to itself. Parametrize the finite points of the line by x. Prove that f is fractionally linear, i.e. $f(x) = \dfrac{ax+b}{cx+d}$, where a, b, c and d are fixed numbers. b) Let f be a homography from ℓ_1 to ℓ_2. Set Cartesian coordinates on a plane. Prove that $f(x,y) = (\dfrac{a_1x+b_1y+c_1}{dx+ey+f}, \dfrac{a_2x+b_2y+c_2}{dx+ey+f})$, where $a_1, a_2, b_1, b_2, c_1, c_2, d, e$ are fixed numbers. c) Prove that any map of $\mathbb{R}^{\not\in}$ defined by the formulas of p. b) may be uniquely extended to a projective map of the projective plane.

11. A map f from a complex line ℓ_1 to itself is defined as $f(z) = \dfrac{P(z)}{Q(z)}$, where P, Q are polynomials. Let f be a bijection. Prove that f conserve the cross-ratio of any four points.

2 Projective movement +

It is a wonder that an inversion limited to a line or a circle also conserve cross-ratios!

Theorem 2.1 *Let an inversion $\mathcal{I}$ maps a circle or a line Ω to a circle or a line $\widetilde{\Omega}$. Then for any four points $A, B, C, D \in \Omega$ we have $(A, B; C, D) = (\mathcal{I}(A), \mathcal{I}(B); \mathcal{I}(C), \mathcal{I}(D))$*

The simplest proof of this theorem use the following properties of complex numbers: a number equals to its conjugated if and only if it is real; the cross-ratio of four complex numbers is real if and only if the corresponding points are collinear or concyclic; the inversion centered at the origin with radius 1 maps z to $\dfrac{1}{\overline{z}}$.

Denoting the complex coordinates of points as a, b, c and d we obtain:

$$(a^*, b^*; c^*, d^*) = \left(\frac{1}{\overline{a}}, \frac{1}{\overline{b}}; \frac{1}{\overline{c}}, \frac{1}{\overline{d}}\right) = \frac{\dfrac{1}{\overline{c}} - \dfrac{1}{\overline{a}}}{\dfrac{1}{\overline{c}} - \dfrac{1}{\overline{b}}} : \frac{\dfrac{1}{\overline{d}} - \dfrac{1}{\overline{a}}}{\dfrac{1}{\overline{d}} - \dfrac{1}{\overline{b}}} =$$

$$= \frac{\overline{c} - \overline{a}}{\overline{c} - \overline{b}} : \frac{\overline{d} - \overline{a}}{\overline{d} - \overline{b}} = \overline{\frac{c - a}{c - b} : \frac{d - a}{d - b}} = \frac{c - a}{c - b} : \frac{d - a}{d - b} = (a, b; c, d).$$

This allows to do the following useful remark:

12. Projection of a circle to itself. a) Let Ω be a circle, and S be an arbitrary point not lying on it. Map each point $X \in \Omega$ to the second common point $\mathcal{F}(X)$ of SX with Ω. Then the map $\mathcal{F}\colon \Omega \to \Omega$ is projective. **b)** Prove that the map transforming a point X to the line SX is NOT projective

13. Transfering of a circle to a tangent Let X move along a line ℓ touching a circle Ω. Let the second tangent from X to Ω touche it at $Y = \mathcal{F}(X)$. Then $\mathcal{F}\colon \ell \to \Omega$ is projective.

14. Transfering of a circle to itself via a line. Let X lie on a circle Ω, and ℓ be a fixed line. Let the tangent to Ω at X meet ℓ at point Z, and $Y = \mathcal{F}(X)$ be the base of the second tangent from Z toΩ. Then $\mathcal{F}\colon \Omega \to \Omega$ is projective.

The lemmas proved above help to solve problems using the projective movement.

15. Let γ_A, γ_B, γ_C — be the excircles of triangle ABC touching the sides BC, CA, AB respectively. Denote as ℓ_A the common external tangent of γ_B and γ_C distinct from BC. Define ℓ_B, ℓ_C similarly. Draw from a point lying on ℓ_A the tangent to γ_B distinct from ℓ_A and find its common point X with ℓ_C. Similarly find the common point Y of the tangent from P to γ_C and ℓ_B. Prove that the line XY touches γ_A.

16. An acute-angled triangle ABC with orthocenter H is inscribed into a circle ω centerd at O. A line l passes through H and meets the minor arcs AB and AC at points P and Q respectively. Let AA' be the diameter of ω. The lines $A'P$ and $A'Q$ meet BC at points K and L respectively. Prove that O, K, L and A' are concyclic.

17. Let S be the projection of the incenter I of an circumscribed quadrilateral $ABCD$ to the diagonal AC. Prove that $\angle BSA = \angle DSA$

18. A pentagon $ABCDE$ is circumscribed around a circle ω. The pairs of rays EA and CB, AE and CD, AB and DC, BC and ED meet at points P, Q, X, Y respectively. The circle ω touches AE at point R. It is known that $XY \parallel AE$. Let the circles $(AXQ), (PYE)$ meet at points S, T. Prove that S, T, R are collinear.

19. A line ℓ passes through the circumcenter O of triangle ABC and meets the sides AB, AC at points P, Q respectively. Prove that one common point of the circles with diameters BQ, CP lies on the nine-points-circle of triangle ABC, and the second one lies on its circumcircle.

20. 2023 lines concur. A circle is inscribed into each of 4046 formed angles in such a way that the circle inscribed into adjacent angles are tangent. A point is marked on each side of the angles. For each angle except one the segment joining the points marked on the sides of this angle touches the inscribed circle. Prove that this is correct for the remaining angle.

21. F ix the sidelines AB, AC and the incircle ω of triangle ABC. Prove that the touching point of ω with the side BC projectively depends on the Feuerbach point of this triangle

Theorem 2.2 *(May be used without proof) Let ABC be a triangle with circumcircle Ω and incircle (or excircle) ω. Let A' lie on Ω, and the tangents from it to ω meet Ω for the second time at B' and C'. Then the line $B'C'$ touches ω.*

Note that we have in this configuration a bijection: each point A of the circumcircle corresponds to the touching point of BC with the incircle. A hypothesis emerges that the corresponding map between to circles is projective.

Lemma 2.1 Homographies of Poncelet configuration. *Consider a Poncelet rotation of triangle ABC conserving the circumcircle and the incircle. Let A_1 be the touching point of side BC with the incircle, S_A and T_A be the midpoints of two arcs BC, and I_A be the center of the excircle touching the side BC, then all these points projectively depend on A.*

Call the map transforming A to A_1 as Poncelet homography and denote it as $\mathcal{P}$.

Mark the incenter I and the circumcenter O of triangle ABC. Note that

- The midpoint S_A of arc BC not containing A is the image of A in the projection of the circumcirle to itself centered at I.
- The point T_A is the image of S_A in the projection centered at O.
- Point A_1 is obtained from S_A by the homothety mapping the circumcircle to the incircle.
- By the trident theorem I_A is the image of the midpoint S_A of arc BC in the homothety centered at I with coefficient 2.

The homographies mapping A to S_A, T_A, A_1, I_A are presented, thus these points projectively depend on A

Usually the Poncelet homographies work effectively with the method of polynomial movement generalizing the projective movement. But it is possible to solve several difficult problems using the methods described above.

22. A convex hexagon $AQCPBR$ is inscribed into a circle Ω in such a way that the triangles ABC and PQR have a common incircle γ. A line ℓ parallel to BC and distinct from it touches γ. Let P_1 be the common point of ℓ and QR. Prove $\angle PAB = \angle P_1AC$.

23. Triangles ABC and DEF have a common incircle ω and circumcircle γ. Let L and K be the touching points of BC and EF respectively with ω, and M, N be the second common points of AL and DK respectively with γ, Prove that AM, EF, BC, ND concur.

24. Let the vertices A and B of a triangle projevtively move in the Poncelet rotation. Prove that this triangle is regular.

The last problem may seem too hard. We propose to return to it after the learning of *the relativity principle*.

It is known that the Poncelet theorem is correct not only for a triangle but for ane n-gon. So the following question is natural:

25. Consider a Poncelet rotation of polygon $A_1A_2...A_{2k+1}$. Does A_{k+1} projectively depend on the touching point of side A_1A_{2k+1} with the incircle?

Now we do not know an elementary proof of this assertion.

3 Conics

Definition 3.1 Conic. *An image of a circle in a projective map of the plane is called a non-degenerated conic. A degenerated conic is a pair of lines (possibly coinciding).*

You may use without proof that any non-degenerated conic is a circle, an ellipse, a parabola, or a hyperbola; and that any conic is the set of points (x, y) satisfying to an equation $ax^2 + by^2 + cxy + dx + ey + f = 0$, where a, b, c, d, e, f are real constants.

The following assertion may be used without proof:

Theorem 3.1 *There exists a unique conic passing through five point such that any three of them are not collinear.*

Definition 3.2 Cross-ratio of four points on the conic *Let A, B, C, D lie on a conic Ω, and S be an arbitrary point of this conic. The cross-ratio $(A, B; , C, D)$ on the conic equals to the cross-ratio $(SA, SB; SC, SD$.*

26. Prove that this definition is correct.

27. Three points A, B and C of a conic $\mathcal{C}$ are collinear. Prove that $\mathcal{C}$ is degenerated.

28. a) Lines a_t and b_t rotate projectively around points A and B respectively. Prove that the common point of a_t and b_t move projectively along some conic (probably degenerated) b) Points A_t and B_t move projectively along lines a and b respectively. Prove that the line A_tB_t envelops some conic (or passes through a fixed point).

When the conic in the previous problem is degenerated?

29. Points A_t and B_t move along two lines with fixed velocities. Which is the conic envelopped by the line joining these points?

Conics often appear as locus of points.

30. A circle and a line meeting at points A and B are give. Find the locus of points such that the tangent to the circle equals the distant to the line.

31. Similar isosceles triangles BA_1C, CB_1A, AC_1B have the sides of triangle ABC as the bases (All triangles are constructed inside ABC, or all triangles are constructed outside it). Prove that the lines AA_1, BB_1, CC_1 concur and find the locus of their common points.

The using of conics may be useful in problems not coherent directly wit them.

32. Let points P и Q be isogonally conjugated with respect to an acute-angled scalene triangle ABC. A point W is the midpoint of arc BAC of the circumcircle of ABC. The lines WP and WQ meet the

circumcircle of ABC for the second time at points X and Y respectively. The lines passing through P and Q and parallel to AW meet AB, AC at points P_B, P_C, Q_B, Q_C. Prove that X, Y, P_B, P_C, Q_B, Q_C are concyclic.

33. The incircle of scalene triangle ABC touches BC, CA, and AB at points A_1, B_1, and C_1 respectively. Three flies creep along the lines AA_1, BB_1, and CC_1 with fixed velocities in such a way that in some moment they were at points A, B, and C, and in some other time they were at A_1, B_1, and C_1 respectively. In some time all three flies were collinear on a line p_1, and in some other time they were collinear on a line p_2. Prove that $p_1 \perp p_2$.

34. Points P, Q lie on the sides AD, CD of quadrilateral $ABCD$ in such a way that $\angle ABP = \angle CBQ$. Denote as S the common point of CP and AQ. Prove that $\angle PBS = \angle QBD$.

35. Let ABC be a triangle with incenter I. A line ℓ meets AI, BI, and CI respectively at points D, E, F distinct from A, B, C, and I. The perpendicular bisectors to segments AD, BE, and CF form a triangle Δ with incircle ω. Prove that ω and the circumcircle of ABC are tangent.

4 Polynomial dependences

Definition 4.1 Projective plane. *Projective plane is the set of all lines passing through a fixed point O of the space, these lines are called points of the projective plane.*

We can choose on any line in $\mathbb{R}^3$ passing through the origin an arbitrary point (x, y, z) distinct from the origin. So all non-zero triplets $[x : y : z]$ code points of the projective plane and are called homogenious coordinates. This definition naturally corresponds to the previous one: if a plane $\alpha|z = 1$ not containing O is fixed in the space, then each point A of this plane corresponds to the line OA, and each infinite point corresponds to the line passing through O, parallel to α, and having the same direction. The triple $[0 : 0 : 0]$ does not define any point of the projectibe plane.

Note that the axes OX and OY in the space are parallel to α, and the axis OZ is perpendicular this plane. Projecting OX and OY to α we obtain the standart coordinates in this plane. The point (x, y) of α has homogenious coordinates $[x : y : 1]$. The infinite points of the projective plane have homogenious coordinates $[x : y : 0]$.

Let p, q be two different points of the projective plane. Consider the plane passing through p, q, and O — it is defined by an equation $ax + by + cz = 0$, where a triple $[a : b : c]$ is defined up to a factor. We call $[a : b : c]$ the homogenious coordinates of a line. The triple $[0 : 0 : 0$ does not define any line.

It is clear that the point $[x_0 : y_0 : z_0$ lies on the line $[a : b : c$ if and only if $ax_0 + by_0 + cz_0 = 0$. From this we obtain by substitution the following

Lemma 4.1 *The coordinates of the line passing through the points $[x_1 : y_1 : z_1]$ and $[x_2 : y_2 : z_2]$ may be defined as*

$$[y_1z_2 - z_1y_2 : z_1x_2 - x_1z_2 : x_1y_2 - y_1x_2]$$

and the common point of the lines $[a_1 : b_1 : c_1]$ and $[a_2 : b_2 : c_2]$ has the coordinates

$$[b_1c_2 - c_1b_2 : c_1a_2 - a_1c_2 : a_1b_2 - b_1a_2]$$

Similarly we may define the homogenious coordinates on the projective line coding its points by the pairs $[x : y]$ defined up to factor. Since the time is a point of the projective line we can consider it as a pair $[t_1 : t_2]$.

Earlier we considered the maps from the projective line to the projective plane (and concretely to lines or conics on it) conserving the cross-ratios. Now we add the *polynomial maps* i.e. the functions $\mathcal{F}\colon \mathcal{RP}^1 \to \mathcal{RP}^2$ mapping a pair $[t_1 : t_2]$ to a triple of polynomials $P(t_1, t_2)$, $Q(t_1, t_2)$, $R(t_1, t_2)$ corresponding to he homogenious coordinates of a point of the projective plane.

Clearly the polynomials P, Q, R have to satisfy to several conditions. If this map cotrrectly transforms the points of projective line to the points of the projective plane the polynomials have to be homogenious ($t_1^2 + 2t_1t_2$ satisfies and $t_1^3 + 2t_1t_2$ does not satisfy) and they degrees have to be equal. Also all three polynomials may not equal zero, thus we suppose that they are relatively prime.

Definition 4.2 Power law *Say that the degree of dependence of point X on the time equals k, if the homogenious coordinates of X may be defined as $[P_1(t_1, t_2) : P_2(t_1, t_2) : P_3(t_1, t_2)]$, where P_i are relatively prime polynomials of degree k. The degrees of dependence of lines are defined similarly.*

It is easy to see that this definition is correct.

Lemma 4.2 Addition of degrees. *Let points X and Y move with degrees a and b respectively. Then the degree of the line XY is not greater than $a + b$.*

Denote the coordinates of X and Y as $[x_1 : x_2 : x_3]$ and $[y_1 : y_2 : y_3]$ respectively. Then the coordinates of XY are $y_1z_2 - y_2z_1 : z_1x_2 - z_2x_1 : x_1y_2 - x_2y_1$. If the degrees of polynomials x_i are not greater than a, and the degrees of y_i are not greater than b, then the degrees of these polynomials are not greater than $a + b$. This estimation is not precise only if the obtained polynomials are not relatively prime.

Lemma 4.3 *Let a point X of degree 1 move one the line not passing trough a point S. Then the degree of line SX also equals 1.*

By the addition degree lemma the degree of SX is not greater than $0 + 1 = 1$. Since the line is not constant this estimation is precise.

In the following chapter we prove the general theorem: if the point X moves on an arbitrary trajectory, then the degree of SX equals to the degree of X.

Theorem 4.1 *The degree of point X projectively moving on a line equals 1. The degree of the line rotating projectively is also 1.*

Firstly demonstrate that any projective map between two lines may be presented as a composition of central projections and translations.

Let the map transform the points A_1, B_1, C_1 of line ℓ_1 to the points A_2, B_2, C_2 of ℓ_2. If $\ell_1 \parallel \ell_2$ project ℓ_1 to any line not parallel to it. Let a translation of ℓ_1 mapping A_1 to A_2 map B_1 and C_1 to B' and C' respectively. Denote as S the common point of $B'B_2$ and $C'C_2$ (may be infinite). The projection centered at S realize the required homography.

Clearly the translation does not change the degree of dependence. Hence we have to prove that that the projection does not change the degree. his follows from the previous lemma.

This theorem yields that if Y projectively depend on X and both points move on the lines then their degrees are equal. This is also correct for two rotating lines. Even more is true.

Theorem 4.2 *A homography of lines transforms the homogenious coordinates of their points linearly.*

This theorem may be used without proof.

Lemma 4.4 Redoubling of degree on a conic. *A point X moving projectively along a circle (a conic) has degree 2.*

Fix two points A, B on a circle, then the lines $a = AX$ and $b = BX$ rotate projectively, therefore X is the common point of two lines with degrees 1, and my the addition of degrees lemma we obtain the required assertion.

Similarly the homography of a line (a pencil) to a circle may at most redouble the degree of any point.

Remark: Clearly the dual lemma is also correct: let a line ℓ rotates around a circle (a conic) in such a way that the degree of touching point equals k. Then the degree of ℓ is not grater than $2k$

Theorem 4.3 *To prove the coincidence of two points with degrees k and l it is sufficient to verify $k+l+1$ dispositions.*

Not that the coincidence of points at time $[t_1 : t_2]$ is equivalent to the equality of the ratios of polynomials on t_1, t_2 defining the coordinates of points:

$$\begin{cases} \dfrac{P_x(t_1,t_2)}{P_y(t_1,t_2)} = \dfrac{Q_x(t_1,t_2)}{Q_y(t_1,t_2)} \\ \dfrac{P_x(t_1,t_2)}{P_z(t_1,t_2)} = \dfrac{Q_x(t_1,t_2)}{Q_z(t_1,t_2)} \end{cases}$$

This is equivalent to:

$$\begin{cases} P_x(t_1,t_2)Q_y(t_1,t_2) = P_y(t_1,t_2)Q_x(t_1,t_2) \\ P_x(t_1,t_2)Q_z(t_1,t_2) = P_z(t_1,t_2)Q_x(t_1,t_2) \end{cases}$$

And to prove the identity of two homogemious polynomials with degrees not grater than $k + l$ it is sufficient to verify $k + l + 1$ Not proportional dispositions. In fact if the polynomial equals zero at points (x_i, y_i) where $y_i \neq 0$, then dividing $P(t_1, t_2)$ onto t_2^d where d is the degree of polynomial, we obtain a polynomial on $\dfrac{t_1}{t_2}$ with the number of roots greater than its degree, hence it is equal to zero. If several y_i equal to zero, consider another time parameter $[\tau_1 : \tau_2]$ such that the infinite time τ does not correspond to any (x_i, y_i).

Similarly to prove that a line with degree k passes through a point with degree l it is sufficient to verify $k + l + 1$ dispositions.

The lemmas formulated above are «basic» and allow to solve many hard problems. Consider an example:

Example 4.1 *Points P and Q lie on the sideline BC of scalene triangle ABC in such a way that $BP = CQ$. Let ω be the incircle of the triangle, and ω_A be the excircle touching the side BC. Points S and T lie on ω and ω_A respectively in such a way that PS touches ω, and QT touches ω_A. Let AS and AT meet BC at points X and Y respectively. Probe that $BX = CY$.*

1. Choose a time and homogenious coordinates on the plane. Move P projectively along BC. Denote the degree of a point as d.
2. Point S projectively depend on P and moves along the circle, hence ny the redoubling of degree lemma $d(S) \leq 2$.
3. By the addition of degrees lemma $d(AS) \leq d(S) + d(A) \leq 2 + 0 = 2$
4. By the same lemma $d(X) \leq d(BC) + d(AS) \leq 0 + 2 = 2$. Similarly $d(Y) \leq 2$, because P and Q are symmetric with respect to the midpoint M of BC, i.e Q projectively depend on P.
5. Let $Y' = \mathcal{S}_M(X)$. Clearly $d(Y') = d(X) \leq 2$, thus we have to prove two points with degrees 2 coincide, for this it is sufficient to verify $2 + 2 + 1 = 5$ dispositions.
6. The dispositions $P = C, P = B, P = A_1$ — the touching point of the incircle, $P = M$, $P = \infty$ are clear.

Solving problems it is useful to understand how degenerated cases habe to be considered. Let in some moment we have to draw the line through two coinciding points: By the formula the coordinates of this line are $[0 : 0 : 0]$, which yields that all following polynomials equal zero. Hence the required assertion is always correct in degenereted dispositions. But we have to be accurate, consider the following example: a point X moves projectively on a conic, and S is a fixed point of this conic. Let we want to prove that several point Y of degree 1 lies always on SX. We have to interpretate correctly the line SX, when $S = X$. If we estimate the degree of SX by the degrees addition lemma its degree do not exceed 2, and if $X = S$ SX is the «zero line», this give us one disposition (because we did not estimate the degree precisely) and we have to find three other disposition. But if we consider SX as a line rotating projectively in the pencil of S, then we initially have to verify three dispositions but when $X = S$ the line has to be considered as the tangent and not the «zero line».

Now try to solve several exercises.

36. Points A and B move along two lines with constant velocities. Prove that the direction of line AB is projective.

37. Three points move projectively. How many positions have to be verified for prove that they are always collinear? The same question for three lines rotating projectively.

38. P oints X and Y move with degrees a and b respectively. Prove that the degree of the midpoint of segment is not greater than $a + b$.

39. Let P be a fixed point of a circle ω, and A move with degree a. Let B be such point that the arc PB is twice greater than the arc PA (we count the length of an arc counterclockwise). Prove that the degree of B is at most $2b$.

40. P olar transformations do not change the degree of dependence.

Now solve several problems.

41. Let $ABCDEF$ be a convex cyclic hexagon. The intersection of triangles ACE and BDF is a hexagon. Prove that its main diagonals concur.

42. Two perpendicular lines meet at the orthocenter of an acute-angled triangle. Prove that the midpoints of segments carving by these lines on the sidelines are collinear.

43. A triangle ABC and three collinear points P, Q, R are given. The lines AP, BP, and CP meet the circumcircle of ABC at points A', B', and C' respectively. The lines $A'Q, B'Q, C'Q$ meet the circumcircle at points A'', B'', and C''. The lines $A''R$, $B''R$, $C''R$ meet this circle at points A''', B''', and C'''. Prove that the lines AA''', BB''', CC''' concur at a point lying on the line passing through P, Q, and R.

44. A point X is marked on the circumcircle of triangle ABC. The lines BX and CX meet the altitudes CC_1 and BB_1 at points P and Q respectively. Prove that the midpoint of segment PQ lies on B_1C_1.

45. Let AH_A be the altitude of an acute-angled triangle ABC, and O be the center of its circumcircle Ω. The lines ℓ_A, ℓ_B, ℓ_C touch Ω at A, B, C respectively. Let S be the orthocenter of triangle formed by ℓ_A, ℓ_B, ℓ_C. Prove that the lines OH_A and SH_A are symmetric with respect to BC.

46. The excircle of triangle ABC centered at I_A touches the side BC at A_1 and touches the sidelines AB, AC at C_1, B_1 respectively. A point P of the line I_AC_1 is such that $AP \perp BI_A$. A point Q of the line I_AB_1 is such that $AQ \perp CI_A$. Prove that P, Q, A_1 are collinear.

47. Let X lie inside a scalene triangle ABC on its Euler line; and O be the circumcenter of ABC. The lines AX, BX, CX meet the opposite sides of ABC at A_1, B_1, C_1 respectively. Prove that the circle (AOA_1), (BOB_1), (COC_1) are coaxial.

48. A triangle ABC with orthocenter H is given. Points A_1, B_1, and C_1 kie on the circumcircle of the triangle in such a way that the lines AA_1, BB_1, and CC_1 concur. Denote as A_2, B_2, and C_2 the reflections of A_1, B_1, and C_1 about the midpoints of the corresponding sidelines. Prove that A_2, B_2, C_2, and H are concyclic.

49. A triangle ABC with orthocenter H is given. Points A_1, B_1, and C_1 kie on the circumcircle of the triangle in such a way that the lines AA_1, BB_1, and CC_1 concur. Denote as A_2, B_2, and C_2 the reflections of A_1, B_1, and C_1 about the corresponding sidelines. Prove that A_2, B_2, C_2, and H are concyclic.

50. The Turner theorem. Let points P, Q be inverse with respect to the circumcircle of triangle ABC, P_C be the reflection of P about AB, and P_CQ meet AB at point C'. Points A', B' are defined similarly. Prove that A', B', C' are collinear.

51. Let $ABCD$ be a convex quadrilateral with $\angle B = \angle D$. Prove that the midpoint of BD lies on a common internal tangent to the incircles of triangles ABC and ACD.

52. A triangle ABC is given. Denote as A_1 the common point of the medial line parallel to BC and the line joining the feet of altitudes to AB, AC. Points B_1, C_1 are defined similarly. Prove that the orthocenter of triangle $A_1B_1C_1$ lies on the Euler line of triangle ABC.

53. Let $ABCD$ be a cyclic quadrilateral, ω be its circumcircle, and P be the common point of its diagonals. Denote as I_A, I_B, I_C, and I_D the incenters of triangles APB, BPC, CPD, and DPA respectively. Let S_A, S_B, S_C, and S_D be the midpoints of «minor» arcs AB, BC, CA, and DA of ω. Prove that the lines I_AS_A, I_BS_B, I_CS_C, and I_DS_D concur.

5 Polynomial movement +

This chapter contains three subjects which be learned independently: generalizations of the theorems proved above, the relativity principle, and the combination of the movement with the Poncelet theorem.

To prove the advanced theorems concerning the polynomial movement we need to use the instruments most powerful than the real numbers. All definitions and theorems of the previous chapter are working for the complex numbers. Instead the real projective line $\mathbb{RP}^1$ we will consider $\mathbb{CP}^1$ — the set of lines in $\mathbb{C}^2$ passing through $(0,0)$. Homogenious coordinates on the complex projective line are pairs $[z_1 : z_2]$ defined up to factor. The complex projective plane $\mathbb{CP}^2$, the homogenius coordinates on it, the pencils, etc. are defined similarly. Not that many results of previous chapters are correct for the complex numbers too. The unit comples circle is the set of solutions in $\mathbb{C}^2$ of the equation $x^2 + y^2 = 1$, or the set of points $[x : y : z]$ in $\mathbb{CP}^2$ such that $x^2 + y^2 = z^2$. Any non-degenerated conic may be obtained from a circle by a projective map (transforming the lines to the lines) and may be defined as the set of roots of an irreducible homogenious polynomial $P(x, y, z) = 0$.

54. Prove that a complex line and a non-degenerated complex conic have at most two common points. Do they intersect obviously?

The complex numbers are better than the real ones because any polynomial $f(x)$ distinct from a constant has a root (this may be used without proof). Furthermore any line of degree n on $\mathbb{CP}^2$ (i.e the set of roots of a homogenious polynomial of degree n) meets a line of degree m at mn points counting their multiplicity. This assertion is the general Bezou theorem. In this chapter we will use only the following patial case of the Besou theorem:

55. a) Prove that a homogenious non-constant polynomial $f(t_1, t_2)$ may be divided to some linear polynomial $at_1 + bt_2$ **b)**. Prove that any homogenious polynomial $f(t_1, t_2)$ may be uniquely (up to permutations and common factors) presented as a product $p_1^{\alpha_1} p_2^{\alpha_2} ... p_n^{\alpha_n}$, where p_i are homogenious linear polynomials.

Clearly the last problem is similar to the main theorem of the arithmetic.

Lemma 5.1 ***(The complex degrees addition lemma).*** *Let points X and Y move with degrees a and b respectively. Then the degree of the line XY is at most $a + b$, and if X and Y are distinct at any time, this estimation is precise.*

Denote the homogenious coordinates of points as $[x_1 : x_2 : x_3]$ and $[y_1 : y_2 : y_3]$ respectively, Then the line XY is defined by th coordinates $[y_1z_2 - z_1y_2 : z_1x_2 - x_1z_2 : x_1y_2 - y_1x_2]$. If the degree of x_i is at most a, and the degree of y_i is at most b the degrees of these polynomials do not exceed $a + b$. If this estimation is not precise then three obtained polynomials have a common divisor $d(t_1, t_2)$. Choose any linear divisor$p = at_1 + bt_2$ of d. Then at time $[b : -a]$ XY is «zero line»m i.e X and Y coinside, contradiction.

Lemma 5.2 *Let a point X of degree a move on a line not passing through a point S. Then the degree of line SX also equals a.*

Follows from the previous assertion.

Summing we obtain:

Theorem 5.1 *Let f be a homography of lines or pencils. Then f does not change the degree of dependence.*

Now we have to learn homographies using conics. We proved that the transfering of a point to a conic redoubles its degree. The inverse assertion is also true.

Theorem 5.2 ***(Throwing off conic).*** *Let a point X of degree k move on a conic, and S be fixed on it. Then the degree of line SX equals $\frac{k}{2}$, in partial k is even.*

You will prove this theorem solving the problems (we suppose that all object are complex).

56. A conic ω is given. Choose an arbitrary point S NOT on this conic and a line ℓ not passing through S. Let f be the projection of the conic from S to ℓ. Prove that any point of the line has two prototypes (excepting may be a finite set of points).

57. A point X moves polynomially on a conic ω. Choose an arbitrary point T ON ω and consider the projection of ω from S to the line $z = 0$. Let this projection map X to X'. So we defined the map g from the line of tome to the line $z = 0$. **a)** Prove that there exists a number k such that each point of line $z = 0$ (excepting may be a finite set) has exactly k prototypes in the map g. **b)** Prove that X coincide with almost any point of ω exactly k times.

58. Denote as X'' the image of X in the map f from the problem preceding the previous one. Count by two methods how many times X'' coincides with a general point of ℓ and obtain from this the theorem.

To start the next subject consider an example. Suppose that the vertices of any triangle move with degrees a, b, and c respectively. How can we estimate the degree of its circumcenter? It is not hard to see that the degree of the mid point of the segment joining two points with degrees a and b is at most $a + b$. The direction of the line passing through the points with degrees $aandbalsohasthedegreenotexceedinga$ + b, $hencethedegreeoftheperpendicularbisectorisnotgreaterthan(a + b) + (a + b) = 2(a + b)(bytheadditiondegre$ + c).$Meetingthesebisectorsandusingtheadditionprincipleweobtainthatthedegreeofthecircumcenterisnotgreat$ + 2b + 2c.

This result sets thinking: the obtained estimation is not symmetric. Probably this means that the estimation is not precise. Furthemore we can suppose that the real estimation equals $2(a + b + c)$. The following instrument allows to prove this hypothesis.

Definition 5.1 Polynomial substitution *Suppose that subsets $P_1, P_2, ...P_n$ of projective plane are fixed, and for any points $p_1 \in P_1, p_2 \in P_2..., p_n \in P_n$ a point $[p_{0_x} : p_{0_y} : p_{0_z}] = \mathcal{R}(p_1, p_2, ..., p_n)$ is defined such that there exist homogenious polynomials R_x, R_y, R_z on $3n$ variables, $p_{0_x} = R_x(p_{1_x}, p_{1_y}...p_{n_z})$, and p_{0_y}, p_{0_z} are defined similarly. Call such $\mathcal{R}$ a polynomial substitution on n points.*

Definition 5.2 Relative degree of dependence. *Let $\mathcal{R}$ be some polynomial substitution on two points, points q_1, q_2 move with several degrees, and $q = \mathcal{R}(q_1, q_2)$. Let r_1 be the minimal natural number such that for any time $[\tau_1 : \tau_2]$ the degree of $\mathcal{R}(q_1, q_2(\tau_1, \tau_2))$ is not greater than r_1 (the degree may be different for different $[\tau_1 : \tau_2]$). Call such r_1 the relative degree of dependence of q on q_1.*

The relative degrees of point depending on more than two points are defined similarly. Fix all q_i except one and see the degree of dependence of q on the remaining point.

59. Relativity principle. Let points $q_1, q_2..., q_n$ move polynomially, and the relative degrees of $q = \mathcal{R}(q_{1_t}, q_{2_t}, ...q_{n_t})$ equal $r_1, r_2, ...r_n$ for some polynomial substitution $\mathcal{R}$. Then the degree of q is not grater than $r_1 + r_2 + ... + r_n$.

60. Let the verices of a triangle move with degrees a, b, and c respectively. Then the degrees of the circumcenter and the orthocenter of this triangle are njt greater than $2(a + b + c)$.

61. Let points A and B projectively move along a conic ω. a) Prove that the line AB envelops some conic γ (or passes through a fixed point). b) Prove that ω and γ touch at two points of $\mathbb{CP}^{\not\in}$ (i.e. the coordinates of touching points may be complex).

62. Let points A and B projectively move along a conic ω. Prove that the common point of tangents to the conic at A and B moves projectively along some conic or a line.

63. Let A move along a conic with degree $2a$, and B move along an arbitrary trajectory with degree b. Denote as C the second common point of line AB with the conic. Then the degree of C is not greater than $2a + 2b$.

64. Four points move with degrees a, b, c, and d. Then to prove that they are concyclic $2(a+b+c+d)+1$ disposition are sufficient.

It may be useful to apply the Poncelet theorem not only to the circumcircle and the incircle of a triangle, but also to its circumcircle and excircle. There are six degenerated disposition in this configuration: parametrizing a tangent ℓ to the excircle we can consider two dispositions when ℓ touches the circumcircle and the excircle, two disposition when it passes through the common points of these circles, and two disposition when the triangle is isosceles.

65. Denote the circumcircle and the excircle of triangle ABC as Ω and ω respectively. Let they meet at points X and Y. The common external tangents to Ω and ω touch Ω at points U and V. Prove that the tangents to ω at X and Y pass through U and V.

66. Let ω de the excircle of triangle ABC touching the side BC. The common external tangents to ω and (ABC) touch (ABC) at point X and Y. Prove that the line XY passes through the feet of bisectors from B and C.

67. The excircle ω of triangle ABC touches the side BC at point A_1 and meets the circumcircle of ABC at points X and Y. The tangents to ω at X and Y meet at point Z. Denote as S the midpoint of arc BAC. Prove that the lines SA_1 and AZ meet on the circumcircle of ABC.

68. The excircle ω of triangle ABC touches the side BC at point A_1 and meets the circumcircle of ABC at points X and Y. The lines A_1X and A_1Y meet the perpendicular bisector to the altitude from A at points U, V. Prove that AUA_1V is a parallelogram.

69. Let a line ℓ of degree d rotate around a point O. Fix two different vectors $\overrightarrow{OA}$ and $\overrightarrow{OB}$ with origin O. Prove that $\dfrac{\sin\angle(\ell, \overrightarrow{OA})}{\sin\angle(\ell, \overrightarrow{OB})} = P(t_1, t_2)$, where $P(t_1, t_2)$ is a homogenious polynomials with degree

d.

70. Let ω be the circumcircle of triangle, and Ω_A be the excircle touching the side BC. Denote the common points of these circles as X and Y. Let P and Q be the projections of A to the tangents at X and Y to Ω_A. The tangent to the circle (APX) at P meets the tangent to the circle (AQY) at Q at point R. Prove that $AR \perp BC$.

Дискретная задача Дидоны и проблема Бобылева

Ивлев Ф.А., Исмаилов А., Канель-Белов А.Я., Иванов-Погодаев И.А., Golafshan M.

A Предварительные задачи

Вводная серия относится к классическим фактам о *задаче Дидоны* о минимальной поверхности. Пусть Ф — фигура минимального периметра с заданной площадью S.

A1 Докажите, что любая хорда фигуры Ф, делящая пополам ее периметр, делит пополам ее площадь и наоборот.

A2 Докажите, что хорда из предыдущей задач перпендикулярна границе фигуры Ф.

A3 (Задача Дидоны) Докажите, что фигура Ф максимальной площади заданного периметра есть круг.

A4 Укажите кривую минимальной длины, которая делит равносторонний треугольник на две равные по площади части.

A5 Докажите, что среди всех n-угольников заданного периметра максимальную площадь имеет правильный.

A6 Докажите, что среди всех n-угольников с заданными длинами сторон максимальную площадь имеет описаный.

A7 Докажите, что площадь n-угольника из предыдущей задачи не зависит от порядка его сторон.

A8 (Многомерная задача Дидоны) Докажите, что тело заданной площади поверхности с максимальным объемом есть шар.

A9 Докажите, что тетраэдр заданной площади поверхности с максимальным объемом — правильный.

A10 Докажите что параллелепипед заданной площади поверхности с максимальным объемом есть куб.

A11 (Задача для исследования) Что можно сказать про многомерные обобщения?

B Дискретная задача Дидоны

B1 Клеточный многоугольник с клетками двух цветов назовем *хорошим*, если в нем ровно четверть клеток — черная. Верно ли, что любой хороший квадрат 12×12 можно разрезать на 9 хороших многоугольников?

Рассмотрим бесконечную клетчатую плоскость (квадратную, треугольную, шестиугольную). Пусть отмечено несколько клеток. Отмеченная клетка называется *граничной*, если она граничит хотя бы с одной неотмеченной клеткой. Пусть имеется n отмеченных граничных клеток. *Дискретной задачей Дидоны* будем называть вопрос максимизации числа отмеченных клеток.

B2 Решите дискретную задачу Дидоны для квадратной решетки (*граничные* — это по стороне).

B3 Решите дискретную задачу Дидоны для квадратной решетки (*граничные* — это по стороне или углу).

B4 Решите дискретную задачу Дидоны для правильной шестиугольной решетки (*граничные* — это по стороне).

B5 Решите дискретную задачу Дидоны для правильной треугольной решетки (*граничные* — это по стороне).

B6 Решите дискретную задачу Дидоны для кубической решетки (*граничные* — это по грани).

B7 * Придумайте многомерное обобщение для кубической решетки.

Задачу также можно поставить немного по-другому: например, если множество граничных клеток расположено внутри некоторого квадрата, и мы не учитываем клетки на границе этого квадрата. Множество граничных клеток, не попадающих на границу квадрата (или, аналогично, куба) будем называть *свободной поверхностью*.

B8 Решите дискретную задачу Дидоны для свободной поверхности участка квадратной решетки в квадрате $k \times k$ (то есть, в свободной поверхности n клеток, *граничные* клетки — по стороне, мы минимизируем число отмеченных клеток в квадрате $k \times k$).

B9 * Решите дискретную задачу Дидоны для свободной поверхности участка кубической решетки в кубе $k \times k \times k$ (*граничные* – это по грани).

B10 * Решите дискретную задачу Дидоны для свободной поверхности участка многомерной кубической решетки в кубе $k \times k \times \cdots \times k$ (*граничные* – это по грани).

B11 (Открытый вопрос) Выведите из предыдущего пункта проблему куба (см. цикл C).

C Свойства многомерья

Начнем с известной задачи В.И.Арнольда

C1 Какой процент объёма занимает мякоть в стомерном арбузе диаметра 1 метр, если толщина корки — 1 см?

Продолжим тему.

C2 К чему стремится объем n-мерного шара радиуса 2022 при $n \to \infty$?

C3 Докажите, что в n-мерный куб при $n \gg 1$ можно поместить главное здание МГУ.

Расстоянием между множествами A и B будем называть такое максимальное число d, что любое расстояние между точками x и y, где $x \in A$, $y \in B$, будет не меньше d.

C4 Докажите, что сечением многомерного куба плоскостью может быть многоугольник, сколь угодно близкий к окружности (то есть, расстояние между многоугольником и окружностью может быть сделано меньше любого заранее заданного числа $\delta > 0$).

C5 В многомерном единичном кубе дано множество M объема $0,99$ и точка A. Докажите, что расстояние от M до A может быть сколь угодно большим.

Тем не менее, есть убежденность в положительном решении следующей проблемы.

Проблема многомерного куба. В n-мерном кубе единичного объема расположены два множества M_1 и M_2 объема ε каждое. Тогда расстояние между ними не превосходит некоторой константы $F(\varepsilon)$.

Замечание. Константа F зависит только от ε, но не от размерности.

Решение проблемы многомерного куба нам не известно, атака на нее есть одна из целей этого проекта.

C6 **. Проблема многомерного шара. В n-мерном шаре единичного объема расположено два множества M_1 и M_2 объема ε каждое. Тогда расстояние между ними не превосходит некоторой константы $G(\varepsilon)$.

C7 Решите проблему многомерного шара для выпуклых тел.

C8 * (Проблема Бобылева.) Решите проблему многомерного куба для выпуклых тел.

Замечание. Можно поставить аналогичные вопросы для симплексов (многомерных тетраэдров) и многомерных октаэдров. Однако такие вопросы в данный момент представляются нам преждевременными, по крайней мере до решения проблемы куба.

Функциональный анализ изучает многомерные и бесконечномерные пространства. Проблемы куба и шара несомненно прольют дополнительный свет на соответствующую проблематику, в особенности относящуюся к теории меры и к пониманию устройства бесконечномерных пространств.

При чем тут **задача Дидоны?**

Открытый вопрос. Проблема минимальной свободной поверхности в кубе. Опишем следующий класс подмножеств точек единичного k-мерного куба. Выбираем любое натуральное число $n \leqslant k$, выбираем n координат и включаем в подмножество все точки, у которых выбранные координаты неотрицательны, причём сумма их квадратов не превосходит некоторого C, а остальные координаты — числа от 0 до 1. Включаем в класс все множества, получающиеся всевозможными такими выборами. Тогда подмножество куба, имеющее фиксированный объём и минимальную свободную поверхность (то есть, площадь той части поверхности, которая не выходит на границу куба, минимальна), достигается на одном из множеств этого класса.

C9 Проблема минимальной свободной поверхности в шаре. Множество объема V в шаре единичного объема B с минимальной площадью той части поверхности, которая не выходит на границу шара, устроено как $B \cap B'$, где B' – шар, чья поверхность перпендикулярна поверхности B.

C10 Выведите проблему куба из проблемы минимальной свободной поверхности в кубе.

Указание. Если M – некоторое множество точек внутри куба, то при $\delta \to 0$ объем δ-окрестности M асимптотически равен $Vol(M) + \delta S(M)$.

Замечание. Асимптотика $Vol(M) + \delta S(M)$ лежит в основе определения *площади поверхности по Минковскому.*

C11 Выведите проблему шара из проблемы минимальной свободной поверхности в шаре.

О дискретной задаче Дидоны. Хотя проблема минимальной свободной поверхности в кубе представляется очень трудной, дискретный аналог этой задачи (достаточный для решения задачи куба), как нам кажется, поддается решению.

D Нумерация клеток куба

D1 В квадрате 8×8 расставлены числа от 1 до 64. Докажите, что найдутся две соседние по стороне клетки, числа в которых отличаются не менее чем на 5.

D2 Клетки доски $N \times N$ занумерованы числами от 1 до N^2. Докажите, что найдутся две соседние по стороне клетки, разность номеров которых не меньше N.

D3 Тот же вопрос для куба со стороной N.

D4 Тот же вопрос для многомерного куба.

E Кривая Пеано

E1 Докажите, что существует непрерывное отображение отрезка на квадрат.

E2 Докажите, что бесконечно много пар точек обязаны склеиться.

E3 Верно ли, что бесконечно много троек точек обязаны склеиться?

E4 Верно ли, что бесконечно много четверок точек обязаны склеиться?

E5 Исследуйте многомерные обобщения.

E6 Исследуйте системы склеенных точек и расстояния между их прообразами.

Свойства многомерья (ещё).

C12.

а) Найдите минимально возможное n такое, что равносторонний треугольник со стороной 100 содержится в n-мерном единичном кубе $[0,1]^n$. Каков максимальный периметр треугольника, лежащего в 11-мерном единичном кубе?

б) Тот же вопрос для квадрата со стороной 10.

в) (Задача на исследование) Аналогичный вопрос для вложения k-мерного куба в единичный n-мерный куб.

г) Каков максимальный радиус трехмерного шара, лежащего внутри четырехмерного единичного куба?

Дискретная изопериметрическая задача

Будем рассматривать решётку $\mathcal{L}$, заданную набором попарно не параллельных векторов $\vec{v}_1, \ldots, \vec{v}_n$:

$$\mathcal{L} = \left\{ \sum_{i=1}^{n} a_i \vec{v}_i \,\middle|\, a_i \in \mathbb{Z} \right\}.$$

Пусть $\mathcal{L}$ обладает таким свойством: в любом конечном куске плоскости (например, квадрате) содержится конечное количество точек $\mathcal{L}$.

Для фигуры F определим понятия: $S(F)$ – площадь F, $P(F)$ – периметр F, $c(F)$ – количество точек $\mathcal{L}$ в F.

F1. Докажите, что существуют такие константы $\alpha, \beta > 0$, что для любой фигуры F

$$c(F) \in [\alpha S(F) - \beta P(F); \alpha S(F) + \beta P(F)].$$

Графом нашей решётки назовём $G = (\mathcal{L}, E)$, где ребром соединена любая пара точек из $\mathcal{L}$, отличающихся на $\vec{v}_i$ для некоторого i. Для любого $S \subset \mathbb{R}^2$ (хотя можно считать $S \subset \mathcal{L}$) определим ∂S, как подмножество рёбер из E, один конец которых входит в S, а другой – нет. Нас будет интересовать минимизация

$$\frac{|\partial S|}{\sqrt{|S \cap \mathcal{L}|}}$$

при фиксированном $|S \cap \mathcal{L}|$.

Пусть нам дан простой многоугольник M. Для $t > 0$ за tM обозначим результат применения гомотетии с коэффициентом t к нашему многоугольнику, т. е. раздуваем его в t раз. Введём величину

$$\gamma(M) = \lim_{t \to \infty} \frac{|\partial(tM)|}{\sqrt{c(tM)}}.$$

F2. Находим $\gamma(M)$:

F2.1 Докажите, что $c(tM) \sim \alpha t^2 S(M)$ при $t \to \infty$.

F2.2 Для работы с $\partial(tM)$ рассмотрим одну из сторон M, заданную вектором $\vec{a}$. Докажите, что количество ребёр из $\partial(tM)$, проходящих через эту сторону, входит в $[\alpha f(\vec{a})t - C; \alpha f(\vec{a})t + C]$, где C – константа, не зависящая от t, и

$$f(\vec{a}) = \sum_{i=1}^{n} |[\vec{a}, \vec{v}_i]|.$$

F2.3 Совмещая предыдущие два пункта, выведите формулу для $\gamma(M)$.

В общем случае задача минимизации

$$\frac{|\partial S|}{\sqrt{|S \cap \mathcal{L}|}}$$

кажется трудной. В частности, неясно, как показать, что множеству S стоит иметь какой-то хороший вид, например быть выпуклым. Однако за счёт полученной нами формулы для $\gamma(M)$ мы можем что-то понять про «оптимальный» M.

F3. Докажите, что «оптимальный» M является выпуклым, иначе говоря, для минимизации $\gamma(M)$ будем лишь рассматривать выпуклые многоугольники.

Отметим, что здесь могут быть актуальны теорема Жордана, т. е. что понятие «внутренности» простого многоугольника вообще имеет смысл, и критерий выпуклости многоугольника: все внутренние углы не превосходят 180°.

F4. Докажите, что «оптимальный» M имеет стороны, параллельные векторам $\vec{v}_i$, задающим решётку, т. е. будем лишь рассматривать многоугольники такого типа.

F5. Докажите, что для простого многоугольника M, образованного последовательностью векторов $\vec{a}_i$ (его стороны)

$$S(M) = \left| \frac{1}{2} \sum_{i<j} [\vec{a}_i, \vec{a}_j] \right|.$$

Используя последний факт, мы получаем, что вопрос минимизации $\gamma(M)$, сводится к своего рода алгебраической задачи минимизации

$$\frac{\left(\sum_{i=1}^{m} f(\vec{a}_i) \right)^2}{\left| \sum_{i<j} [\vec{a}_i, \vec{a}_j] \right|},$$

причём мы можем считать, что $m \leqslant 2n$.

F6. Докажите, что «оптимальный» M существует. Как следствие

$$\gamma_p = \min_M \gamma(M),$$

определён.

Можно даже сказать, что γ_p является алгебраическим числом, если координаты v_i – алгебраические числа.

F7. Докажите, что оптимальный M является центрально-симметричным.

F8. Докажите, что в оптимальном M встречаются стороны, параллельные каждому из векторов v_i, задающих решётку.

F9. Оптимальное значение M достигается на центрально-симметричном выпуклом многоугольнике со сторонами, совпадающими с векторами задающими решётку (надо будет взять $\vec{v}_i$ и $-\vec{v}_i$). На основе этого выразите γ_p через константу α и вектора $\vec{v}_1, \ldots, \vec{v}_n$.

F10. Покажите, что при $n = 3$, т. е. три вектора задают решётку, все оптимальные многоугольники должны иметь вид, описанный в задаче 9, с точностью до гомотетии.

Dido's discrete problem and Bobylev's problem

Ivlev F.A., Ismailov A., Kanel-Belov A.Ya., Ivanov-Pogodaev I.A., Golafshan M.

August 2, 2022

Contents

A) Preliminary tasks

The introductory series refers to the classical facts about Dido's minimal surface problem. Let Φ be a figure of the minimum perimeter with a given area S.

A1 Prove that any chord of the figure Φ bisecting its perimeter bisects its area and vice versa.

A2 Prove that the chord from the previous problem is perpendicular to the boundary of the figure Φ.

A3 (Dido's task) Prove that the figure Φ of the maximum area of a given perimeter is a circle.

A4 Specify a curve of minimum length that divides an equilateral triangle into two equal parts in area.

A5 Prove that among all n-gons of a given perimeter, the regular one has the maximum area.

A6 Prove that among all n-gons with given side lengths, the described one has the maximum area.

A7 Prove that the area of the n-gon from the previous problem does not depend on the order of its sides.

A8 (Dido's multidimensional problem) Prove that a body of a given surface area with a maximum volume is a ball.

A9 Prove that the tetrahedron of a given surface area with the maximum volume is regular.

A10 Prove that a parallelepiped of a given surface area with a maximum volume is a cube.

A11 (Research task) What can we say about multidimensional generalizations?

B) The discrete Dido problemThe discrete Dido problem

B1 A cellular polygon with cells of two colors will be called good if exactly a quarter of the cells in it are black. Is it true that any good square 12×12 can be cut into 9 good polygons?

Consider an infinite checkered plane (square, triangular, hexagonal). Let several cells be marked. A marked cell is called a boundary cell if it borders at least one unmarked cell. Let there be n marked boundary cells. The discrete problem of Dido will be called the question of maximizing the number of marked cells.

B2 Solve the discrete Dido problem for a square lattice (the boundary ones are on the side).

B3 Solve the discrete Dido problem for a square lattice (the boundary ones are on the side or corner).

B4 Solve the discrete Dido problem for a regular hexagonal lattice (the boundary ones are on the side).

B5 Solve the discrete Dido problem for a regular triangular lattice (the boundary ones are on the side).

B7 ***Come up with a multidimensional generalization for a cubic lattice.

The problem can also be posed a little differently: for example, if the set of boundary cells is located inside a certain square, and we do not take into account the cells on the border of this square. The set of boundary cells that do not fall on the boundary of a square (or, similarly, a cube) will be called a free surface.The problem can also be posed a little differently: for example, if the set of boundary cells is located inside a certain square, and we do not take into account the cells on the border of this square. The set of boundary cells that do not fall on the boundary of a square (or, similarly, a cube) will be called a free surface.

B8 To solve the discrete Dido problem for the free surface of a square lattice section in the square $k \times k$ (that is, in the free surface of n cells, the boundary cells are on the side, we minimize the number of marked cells in the square kk).

B9 * Solve the discrete Dido problem for the free surface of a section of a cubic lattice in a $k \times k \times k$ cube (the boundary ones are along the face).

B10 * Solve the discrete Dido problem for the free surface of a section of a multidimensional cubic lattice in a cube $k \times k \times \cdots \times k$ (the boundary ones are along the face).

B11 (Open question) Derive the cube problem from the previous paragraph (see cycle C).

C) Properties of the multidimensionalProperties of the multidimensional

Let's start with the well-known problem of V.I. Arnold:

C1 What percentage of the volume is occupied by the pulp in a one-dimensional watermelon with a diameter of 1 meter, if the thickness of the crust is 1 cm?

Let's continue the topic.

C2 What does the volume of an n-dimensional ball of radius 2022 tend to at $n \to \infty$?

C3 Prove that the main building of the Moscow State University can be placed in an n-dimensional cube at $n \gg 1$. The distance between sets A and B will be called such a maximum number d that any distance between points x and y, where $x \in A$, $y \in B$, will be at least d.

C4 Prove that the section of a multidimensional cube plane can be a polygon arbitrarily close to the circle (that is, the distance between the polygon and the circle can be made less than any predetermined number $\delta > 0$).

C5 In a multidimensional unit cube, a set M of volume $0,99$ and a point A are given. Prove that the distance from M to A can be arbitrarily large.

Nevertheless, there is a conviction in a positive solution to the following problem.

The problem of a multidimensional cube. In the n-dimensional cube of a unit volume there are two sets M_1 and M_2 of volume ε each. Then the distance between them does not exceed some constant $F(\varepsilon)$.

Remark. The constant F depends only on ε, but not on the dimension.

We do not know the solution to the multidimensional cube problem, an attack on it is one of the goals of this project.

C6 **. The multidimensional ball problem. In an n-dimensional sphere of a unit volume there are two sets M_1 and M_2 of volume ε each. Then the distance between them does not exceed some constant $G(\varepsilon)$.

C7 Solve the multidimensional ball problem for convex bodies.

C8 * (Bobylev's problem.) Solve the multidimensional cube problem for convex bodies.

Remark. Similar questions can be posed for simplices (multidimensional tetrahedra) and multidimensional octahedra. However, such questions seem premature to us at the moment, at least until the cube problem is solved.

Functional analysis studies multidimensional and infinite-dimensional spaces. The problems of the cube and the sphere will undoubtedly shed additional

light on the relevant problems, especially those related to the theory of measure and to the understanding of the structure of infinite-dimensional spaces.

What does **Dido's task** have to do with it?

An open question. The problem of the minimum free surface in a cube.

We describe the following class of subsets of points of a unit k-dimensional cube. We choose any natural number $n \leqslant k$, choose n coordinates and include in the subset all points whose selected coordinates are non—negative, and the sum of their squares does not exceed some C, and the remaining coordinates are numbers from 0 to 1. We include in the class all the sets obtained by all possible such choices. Then a subset of the cube having a fixed volume and a minimal free surface (that is, the area of the part of the surface that does not extend to the boundary of the cube is minimal) is achieved on one of the sets of this class.

C9 **The problem of the minimum free surface in the ball.** The set of volume V in a ball of unit volume B with the minimum area of the part of the surface that does not extend to the boundary of the ball is arranged as $B \cap B'$, where B' is a ball whose surface is perpendicular to the surface of B.

C10 Derive the cube problem from the problem of the minimum free surface in the cube.

Hint. If M is some set of points inside the cube, then for $\delta \to 0$ the volume The δ-neighborhood of M is asymptotically equal to $Vol(M) + \delta S(M)$.

Remark. The asymptotics of $Vol(M) + \delta S(M)$ is the basis for determining the surface area by Minkowski.

C11 Derive the ball problem from the problem of the minimum free surface in the ball.

On the discrete Dido problem. Although the problem of the minimal free surface in a cube seems to be very difficult, a discrete analogue of this problem (sufficient to solve the cube problem), it seems to us, can be solved.

D) Numbering of cube cells

D1 The numbers from 1 to 64 are placed in an 8×8 square. Prove that there are two adjacent cells on the side, the numbers in which differ by at least 5.

D2 In the cell, the boards $N \times N$ are numbered with numbers from 1 to N^2. Prove that there are two adjacent cells on the side whose number difference is not less than N.

D3 The same question for a cube with side N.

D4 The same question for a multidimensional cube.

E) The Peano curve

E1 Prove that there is a continuous mapping of a segment to a square.

E2 Prove that infinitely many pairs of points are bound to stick together.

E3 Is it true that infinitely many triples of points are bound to stick together?

E4 Is it true that infinitely many fours of points are bound to stick together?

E5 Explore multidimensional generalizations.

E6 Explore the systems of glued points and the distances between their prototypes.