Лицей “Вторая школа” имени В. Ф. Овчинникова

10 класс, 2023–2024 учебный год
Материалы занятий по спецматематике
Математический профиль

Бибиков Павел Витальевич

Оглавление

МАТЕРИАЛЫ МАТЕМАТИЧЕСКОГО ПРОФИЛЯ

Декомпозиция и линейность

Во многих задачах полезно использовать соображения *декомпозиции и линейности*. Иначе говоря, решить задачу для достаточно простых стартовых данных, а затем собрать из них решение в общем случае.

Пример: КТО. *Для любых попарно взаимно простых натуральных чисел m_1, ..., m_n и любых целых чисел r_1, ..., r_n существует такое целое число x, что $x \equiv_{m_i} r_i$ для любого $i = 1, ..., n$.*

Доказательство. Докажем, что для каждого $i = 1, ..., n$ существует такое целое число x_i, что $x_i \equiv_{m_j} \delta_{ij}$ (здесь $\delta_{ij} = 1$, если $i = j$ и 0, если $i \neq j$). Возьмем для удобства $i = 1$ и рассмотрим числа $m_2 ... m_n$, $2m_2 ... m_n$, ..., $(m_1 - 1)m_2 ... m_n$. Все эти числа дают попарно различные остатки при делении на m_1, поэтому среди них есть число x_1, которое дает остаток 1. Очевидно, что оно делится на m_2, ..., m_n.

Теперь возьмем число $x = r_1x_1 + r_2x_2 + ... + r_nx_n$. Оно будет искомым.

Хороший пример идей декомпозиции и линейности — *задачи интерполяции*. Пусть даны два набора чисел: x_0, x_1,..., x_n и y_0, y_1, ..., y_n, причём в первом наборе все числа различны. Требуется найти многочлен F степени не выше n такой, что $F(x_i) = y_i$ при $i = 0$, 1, ..., n.

1. **Интерполяционный многочлен Лагранжа.** Реализуйте идею декомпозиции и линейности, построив многочлены F_i, такие, что $F_i(x_j) = \delta_{ij}$, и затем многочлен F.

2. **Интерполяционный многочлен Ньютона.** Реализуйте идею декомпозиции, построив последовательность многочленов $\{f_i\}$, где $i = 0, 1, ..., n$, таких, что $f_i(x_j) = y_j$ для всех $j \leqslant i$.

3. **Целозначные многочлены.** Многочлен $p(x)$ (с действительными коэффициентами) называется *целозначным*, если он принимает целые значения при всех целых x. Докажите, что многочлен является целозначным тогда и только тогда, когда он представим в виде $a_0 + a_1C_x^1 + a_2C_x^2 + ... + a_nC_x^n$, где числа a_0, a_1, ..., a_n — целые и $C_x^k = \dfrac{x(x-1)...(x-k+1)}{k!}$.

4. Какую наименьшую степень может иметь приведенный многочлен $f(x)$, такой что $f(a)$ делится на 100 при любом целом a?

5. Многочлен степени n таков, что для любого $i = 0, 1, ..., n$ выполнено равенство $f(i) = 2^i$. Чему равно $f(n + 1)$? (Ответ нужно дать в законченном виде, без знака «...».)

Задачи для самостоятельного решения

1. **(a)** Для любых различных a, b, c, d, e докажите, что

$$\frac{(a-b)(a-c)(a-d)}{(e-b)(e-c)(e-d)} + \frac{(a-b)(a-c)(a-e)}{(d-b)(d-c)(d-e)} + \\ + \frac{(a-b)(a-d)(a-e)}{(c-b)(c-d)(c-e)} + \frac{(a-c)(a-d)(a-e)}{(b-c)(b-d)(b-e)} = 1.$$

(b) Для любых различных a, b, c, d докажите, что

$$\frac{a(b+c+d)}{(a-b)(a-c)(a-d)} + \frac{b(c+d+a)}{(b-c)(b-d)(b-a)} + \\ + \frac{c(d+a+b)}{(c-d)(c-a)(c-b)} + \frac{d(a+b+c)}{(d-a)(d-b)(d-c)} = 0.$$

2. **(a)** Дан приведенный многочлен $P(x)$ степени $n-1$. Для различных x_1, x_2, $\ldots x_n$ докажите, что

$$\sum_{i=1}^{n} \frac{P(x_i)}{(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)} = 1.$$

(b) Дан многочлен $P(x)$ степени не более $n-2$. Для различных $x_1, x_2, \ldots x_n$ докажите, что

$$\sum_{i=1}^{n} \frac{P(x_i)}{(x_i-x_1)(x_i-x_2)\ldots(x_i-x_{i-1})(x_i-x_{i+1})\ldots(x_i-x_n)} = 0.$$

3. Дана последовательность Фибоначчи $F_0 = 0, F_1 = 1, F_{n+2} = F_{n+1} + F_n$. Многочлен $P(x)$ степени 1011 таков, что $P(k) = F_k$ при $k \in \{1011, \ldots, 2022\}$. Докажите, что $P(2023) = F_{2023} - 1$.

4. Петя и Вася придумали десять многочленов пятой степени. Затем Вася по очереди называл последовательные натуральные числа (начиная с некоторого), а Петя каждое названное число подставлял в один из многочленов по своему выбору и записывал полученные значения на доску слева направо. Оказалось, что числа, записанные на доске, образуют арифметическую прогрессию (именно в этом порядке). Какое максимальное количество чисел Вася мог назвать?

5. Функция $f(x)$ при целых x принимает целые значения. Оказлось, что для любого простого p существует такой многочлен $Q_p(x)$ с целыми коэффицентами степени не выше 2022, что $f(n) - Q_p(n)$ делится на p при любом целом n. Докажите, что существует такой многочлен $g(x)$ с рациональными коэффициентами, что $f(n) = g(n)$ при любом натуральном n.

6. Имеется таблица 4×4, в каждой клетке которой стоит 0 или 1. Каждую минуту с ней проделывается следующая операция: для каждой клетки считается сумма чисел в соседних с ней по сторонам клетках, и одновременно в каждой клетке число заменяется на 0, если соответствующая сумма четна, и на 1 — если нет. Докажите, что в течение 6 минут какая-нибудь расстановка повторится дважды.

7. Многочлен $P(x)$ имеет степень не большую $2n$. Известно, что для каждого целого $k \in [-n, n]$ выполнено неравенство $|P(k)| \leqslant 1$. Докажите, что для любого $x \in [-n, n]$ выполняется неравенство $|P(x)| \leqslant 2^{2n}$.

8. Пусть $x_1, \ldots, x_n$ — различные вещественные числа. Докажите, что выражение $\sum_i \prod_{j \neq i} \frac{1 - x_i x_j}{x_i - x_j}$ равно 0 при четном n и 1 — при нечетном n.

Векторные пространства

Идеи декомпозиции и линейности могут быть обобщены для самых разных объектов с помощью общих понятий *векторного пространства*, *линейных комбинаций*, *базиса* и т.д. Первичными операциями, которые мы хотим уметь совершать, являются операция сложения объектов и операция умножения этих объектов на числа. Чтобы зафиксировать первичность этих операций, мы фиксируем их свойства в общем определении, частными случаями которого являются рассмотренные нами ранее примеры.

Определение. *Векторным пространством над полем* $\mathbb{R}$ называется множество V, в котором есть две операции: операция сложения «+» и операция умножения на вещественное число, причем эти операции удовлетворяют всем привычным нам свойствам ассоциативности, коммутативности и дистрибутивности.

Аналогично можно определять векторное пространство над произвольным полем. Наиболее часто в качестве полей используются поля $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_p$.

Важные примеры векторных пространств.

- $\mathbb{E}^2$ — евклидова плоскость;
- $\mathbb{R}^n$ — последовательности вещественных чисел длины n («n-мерное пространство»);
- $\mathbb{C}$ — множество комплексных чисел;
- $\mathbb{Q}[x]$, $\mathbb{R}[x]$, $\mathbb{C}[x]$, $\mathbb{Z}_p[x]$ — пространства многочленов с коэффициентами из соответствующих полей;
- множество решений однородной системы линейных уравнений (СЛУ);
- $\{a_n\}$ — множество последовательностей, элементы которых удовлетворяют соотношению $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_k a_{n-k}$ для всех $n \geqslant k$ (линейные рекурренты);
- $\mathcal{F} = \{F(x, y) : F(A_1) = \ldots = F(A_n) = 0\}$ — множество многочленов от двух переменных, обращающихся в нуль в заданных точках.

Реализация идеи декомпозиции заключается в выборе конкретного набора векторов, через которые с помощью операций сложения и умножения на числа можно выразить все другие векторы.

Определение. Пусть $v_1, \ldots, v_n$ — векторы из векторного пространства V. Выражение вида $\alpha_1 v_1 + \ldots + \alpha_n v_n$ называется *линейной комбинацией векторов* $v_1, \ldots, v_n$. Если существуют такие числа $\alpha_1, \ldots, \alpha_n$, не все равные 0, для которых линейная комбинация равна 0, то говорят, что векторы $v_1, \ldots, v_n$ *линейно зависимы*. В противном случае говорят, что векторы $v_1, \ldots, v_n$ *линейно независимы*.

Если векторы $e_1, \ldots, e_n$ линейно независимы, и каждый вектор v является их линейной комбинацией $v = x_1 e_1 + \ldots + x_n e_n$, то набор $\{e_1, \ldots, e_n\}$ называется *базисом векторного*

пространства V, а числа x_1, ..., x_n — *координатами вектора v в этом базисе.*

Лемма о линейной зависимости. Даны натуральные числа $m > n$. Известно, что векторы f_1, ..., f_m являются линейными комбинациями векторов e_1, ..., e_n. Тогда векторы f_1, ..., f_m линейно зависимы.

Следствие. Если у векторного пространства V есть базис, содержащий n векторов, то любой базис этого пространства содержит ровно n векторов. Число n называется *размерностью* векторного пространства V и обозначается через $\dim V$.

1. Докажите, что наборы векторов **(a)** $\{\sqrt{2}, \sqrt{3}, \sqrt{5}\}$; **(b)** $\{\sin x, \sin 2x, \sin 3x, \dots, \sin nx\}$ линейно независимы над полями $\mathbb{Q}$ и $\mathbb{R}$ соответственно.

2. Пусть x_0, x_1, ..., x_n — попарно различные вещественные числа. Определим многочлены F_0, F_1, ..., F_n соотношениями $F_i(x_j) = \delta_{ij}$. Докажите, что набор многочленов $\{F_0, F_1, \dots, F_n\}$ образует базис в пространстве многочленов степени не выше n.

3. Разложите многочлен $P(x)$ степени n по базису $\left\{1, \frac{x}{1!}, \frac{x^2}{2!}, \dots, \frac{x^n}{n!}\right\}$ (т.е. выразите его координаты в этом базисе через сам многочлен P).

4. Найдите базис пространства последовательностей Фибоначчи (т.е. последовательностей $\{F_n\}$ вида $F_n = F_{n-1} + F_{n-2}$), состоящий из геометрических прогрессий.

5. На плоскости даны четыре точки A, B, C, D общего положения. Докажите, что пространство $\mathcal{F}$ многочленов степени не выше 2 от двух переменных, обращающихся в нуль в этих точках, двумерно, и найдите какой-нибудь базис этого пространства.

Задачи для самостоятельного решения

1. Изначально все клетки доски 8×8 чёрные. Сколько различных раскрасок можно получить, перекрашивая столбцы и строки?

2. Есть n негорящих лампочек и k выключателей. Каждый выключатель соединён с некоторыми лампочками. При нажатии выключателя все соединённые с ним лампочки меняют своё состояние.
   (a) Докажите, что если $k < n$, то для любого соединения лампочек с выключателями найдётся комбинация горящих лампочек, которую невозможно получить.
   (b) Докажите, что если $k > n$, то для любого соединения можно нажать на некоторые выключатели так, чтобы ни одна лампочка в итоге не загорелась.

3. Есть доска 100×100 с изначально выключенными лампочками в клетках. За одну операцию разрешается поменять состояния всех лампочек в любом кресте (объединение строки и столбца). За какое минимальное число операций всю доску можно включить?

4. Имеется $n+1$ непустых подмножеств n-элементного множества. Докажите, что ненулевую часть из них можно покрасить в красный или синий цвет так, чтобы объединение красных подмножеств совпадало с объединением синих.

Пространства решений СЛУ

Определение. Пусть $\{a_{ij}\}, \{b_i\}$ — наборы вещественных чисел, где $i = 1, ..., n$ и $j = 1, ..., m$. Множество уравнений $\sum\limits_{j=1}^{m} a_{ij}x_j = b_i$ называется *системой линейных уравнений* (СЛУ). Множество ее решений обозначим через $V(S)$. Множество $V(S)$ является подмножеством в пространстве $\mathbb{R}^m = \{(x_1, ..., x_m) : x_i \in \mathbb{R}\}$ строк вещественных чисел длины m. В случае, когда $b_j = 0$ для всех j, система называется *однородной*. В случае, когда $m = n$, система называется *квадратной*. Заметим, что если S — однородная СЛУ, то множество ее решений $V(S)$ является векторным пространством.

Как описать пространство $V(S)$? Для этого используется *метод Гаусса* преобразования СЛУ S. А именно, с системой S можно совершать следующие операции, не изменяя пространства решений $V(S)$:

- прибавить к одной строке другую;
- умножить любую строку на ненулевое число;
- поменять местами любые две строки.

С помощью таких операций любую СЛУ можно привести к *ступенчатому виду*:

$$\begin{cases} a_{1p}x_p + ... + a_{1m}x_m = b_1 \\ a_{2q}x_q + ... + a_{2m}x_m = b_2 \\ ... \\ a_{kt}x_t + ... + a_{km}x_m = b_k \\ 0 = b_{k+1} \\ ... \\ 0 = b_n, \end{cases}$$

где $p < q < ... < t$ и $a_{1p}, ..., a_{kt} \neq 0$.

Отсюда следует, что любая СЛУ имеет или 0, или 1, или бесконечно много решений: переменные x_p, x_q, ..., x_t выражаются через остальные переменные, которые в свою очередь принимают произвольные значения. Переменные x_p, x_q, ..., x_t называются *зависимыми*, а все остальные переменные — *свободными*. Для однородной системы S размерность $\dim V(S)$ равна количеству свободных переменных.

1. **(a)** Приведите к ступенчатому виду СЛУ $\begin{cases} x + 5y + 4z + 3t = 1 \\ 2x - y + 2z - t = 0 \\ 5x + 3y + 8z + t = 1. \end{cases}$. **(b)** Запишите общее решение этой системы, выразив зависимые переменные через свободные. **(c)** Укажите базис соответствующей однородной СЛУ в пространстве $\mathbb{R}^4$.

2. **(a)** Докажите, что если для однородной системы S имеет место неравенство $m > n$, то пространство решений $V(S)$ содержит ненулевой вектор (и, как следствие, прямую, натянутую на этот вектор).
(b) Докажите, что если некоторая СЛУ с рациональными коэффициентами имеет вещественное решение, то она имеет и рациональное решение.

3. **(a)** Докажите, что если S — однородная СЛУ с пространством решений $V(S)$, а S' — неоднородная СЛУ с такой же как у S левой частью и решением $\mathbf{x}^0 = (x_1^0, \dots, x_m^0)$, то любое решение системы S' получается из $\mathbf{x}^0$ прибавлением некоторого вектора из пространства $V(S)$.
(b) Пусть S — квадратная однородная СЛУ, а S' — неоднородная СЛУ с такой же как у S левой частью. Известно, что система S имеет единственное решение. Докажите, что система S' также имеет единственное решение.

4. Петя вписал числа в клетки квадрата 3×3 так, что получился магический квадрат. Числа в каком наименьшем количестве клеток должен узнать Вася, чтобы восстановить весь квадрат?

5. Имеется клетчатая таблица $(k + 2) \times (\ell + 2)$, в её граничных клетках расставлены какие-то действительные числа. Докажите, что в клетках центрального прямоугольника $k \times \ell$ можно единственным образом расставить числа так, чтобы каждое из этих $k\ell$ чисел равнялось среднему арифметическому своих четырёх соседей по стороне.

6. Есть n монет неизвестной массы и весы. Разрешается положить несколько монет на одну чашу весов и такое же количество монет на другую чашу весов. Весы либо указывают, что массы на двух чашах равны, либо указывают, какая чаша тяжелее. Докажите, что потребуется по крайней мере $n - 1$ взвешиваний, чтобы определить, все ли монеты имеют одинаковую массу.

Задачи для самостоятельного решения

1. Внутри отрезка $[0, 1]$ выбрали n различных точек. *Отмеченной точкой* назовём одну из выбранных или конец отрезка. Оказалось, что любая из внутренних n точек является серединой какого-то отрезка с концами в отмеченных точках. Докажите, что все выбранные точки рациональны.

2. Дана таблица $m \times n$, заполненная вещественными числами. Известно, что сумма чисел в любой строке и в любом столбце целая. Докажите, что можно округлить каждое нецелое число в таблице вверх или вниз так, чтобы суммы новых чисел в каждой строке и столбце совпали бы с исходными суммами.

3. На математической конференции каждые два математика либо знакомы, либо незнакомы. Математики собрались на банкет, который проходит в двух больших столовых. Каждый математик хочет находиться в том помещении, в котором находится четное число его знакомых. Известно, что существует способ рассадить математиков по столовым так, чтобы удовлетворить пожелания каждого из них. Докажите, что тогда количество таких рассадок равно степени двойки.

Векторные пространства квадрик и кубик

Теорема Паскаля. Рассмотрим произвольную непустую кривую $\mathcal{K}$, заданную квадратичным многочленом, и отметим на ней шесть точек A_1, ..., A_6. Обозначим через ℓ_i прямые A_iA_{i+1} (здесь $i = 1, ..., 6$). Положим также $P_i = \ell_i \cap \ell_{i+3}$ (здесь $i = 1, 2, 3$ и сложение индексов осуществляется по модулю 6). Тогда точки P_1, P_2, P_3 лежат на одной прямой.

Доказательство. Рассмотрим кубику $\mathcal{Q} = \mathcal{K} \cdot p$, где $p = P_1P_2$. Кроме того, рассмотрим две кубики $q_1 = \ell_1\ell_3\ell_5$ и $q_2 = \ell_2\ell_4\ell_6$. Заметим, что все три кубики $\mathcal{Q}$, q_1, q_2 проходят через точки A_i, P_1 и P_2. Множество кубик, проходящих через эти точки, является векторным пространством размерности 2, и $\{q_1, q_2\}$ — его базис. Поэтому существуют такие числа λ_1 и λ_2, что $\mathcal{Q} = \lambda_1 q_1 + \lambda_2 q_2$. На q_1, q_2 лежит точка P_3, поэтому $P_3 \in \mathcal{K} \cdot p$. Но $P_3 \notin \mathcal{K}$, поэтому $P_3 \in p$, что и требовалось.

Замечание. Во многих (но не во всех!) задачах далее можно считать квадрику окружностью.

1. Пусть квадрика $\mathcal{K}$ проходит через точки A, B, C, D. Обозначим через ℓ_{AB} уравнение прямой AB, и т.д. Докажите, что найдутся такие числа λ и μ, для которых верно равенство
$$\mathcal{K} = \lambda\ell_{AB} \cdot \ell_{CD} + \mu\ell_{BC} \cdot \ell_{AD}.$$

2. **Теорема Паппа.** Даны две прямые ℓ и m. На прямой ℓ отмечены точки L_i, а на прямой m — точки M_j, где $i, j = 1, 2, 3$. Пусть $P_i = L_iM_{i+1} \cap L_{i+1}M_i$, где $i = 1, 2, 3$. Докажите, что точки P_1, P_2, P_3 лежат на одной прямой.

3. **Теорема о девяти точках на кубике.** Даны шесть прямых ℓ_i, m_j, где $i, j = 1, 2, 3$ общего положения. Пусть $A_{ij} := \ell_i \cap m_j$. Кубика $\mathcal{C}$ проходит через точки A_{ij} для всех i, j, за исключением, быть может, точки A_{33}. Докажите, что тем не менее точка A_{33} лежит на $\mathcal{C}$.

4. С помощью пучков прямых и разложений по базису докажите *теорему Дезарга*: если три прямые принадлежат одному пучку, и на каждой из прямых выбраны соответственно точки A_1, A_2, B_1, B_2 и C_1, C_2, то точки пересечения соответствующих сторон треугольников $A_1B_1C_1$ и $A_2B_2C_2$ лежат на одной прямой.

(a) Задачи для самостоятельного решения

1. Восьмиугольник вписан в квадрику. Обозначим через ℓ_i, $i = 1, \ldots, 8$ прямые, последовательно содержащие его стороны. Докажите, что точки пересечения прямых ℓ_i и ℓ_{i+3} лежат на одной квадрике.

2. **(a)** В квадрику $\mathcal{K}$ вписаны два четырехугольника $ABCD$ и $A_1B_1C_1D_1$. Обозначим через $XYZT$ четырехвершинник, образованный прямыми AA_1, BB_1, CC_1 и DD_1 (т.е. его стороны последовательно лежат на указанных прямых). Также отметим точки U и V пересечения прямых AC и BD, A_1C_1 и B_1D_1 соответственно. Докажите, что точки X, Y, Z, T, U и V лежат на одной квадрике.
(b) Дан вписанный четырехугольник $ABCD$. Проведем биссектрисы его углов и обозначим через X, Y, Z и T точки пересечения двух соседних биссектрис. Обозначим также через O центр окружности $(ABCD)$ и через P точку пересечения его диагоналей. Докажите, что точки X, Y, Z, T, O и P лежат на одной квадрике.

3. **Теорема Штейнера.** На квадрике $\mathcal{K}$ выбраны точки A_1, ..., A_6. Докажите, что прямые Паскаля шестивершинников

$$A_1A_2A_3A_4A_5A_6, \quad A_1A_4A_5A_2A_3A_6, \quad A_1A_4A_3A_6A_5A_2$$

пересекаются в одной точке.

4. **(a)** Прямые AB и CD пересекаются в точке P, прямые BC и AD — в точке Q. Кубика $\mathcal{C}$ проходит через точки A, B, C, D, P и Q. Докажите, что касательные к кубике $\mathcal{C}$, проведенные в точках P и Q, пересекаются на $\mathcal{C}$.
(b) Прямая пересекает кубику в точках A, B и C. Касательные к кубике, проведнные в этих точках, повторно пересекают ее в точках A_1, B_1 и C_1. Докажите, что точки A_1, B_1 и C_1 лежат на одной прямой. (*Указание.* Наличие касательных указывает на то, что какие-то точки или прямые склеиваются...)

Матрицы и определители

При изучении систем линейных уравнений удобно использовать язык матриц. Матрица — это прямоугольная таблица из чисел. Сами числа (элементы матрицы) индексируются двумя индексами, первый из которых обозначает номер строки, а второй — номер столбца. Т.е. пишут $A = (a_{ij})$, имея в виду запись $A = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & \dots & a_{mn} \end{pmatrix}$. Также говорят, что матрица A имеет размер $m \times n$. Матрица $A^T = (a_{ji})$ называется *транспонированной к* A и имеет размер $n \times m$.

Если $\mathbf{v} = (v_1, \dots, v_n)$ — вектор, то произведением $A\mathbf{v}$ является вектор, чьи компоненты получаются скалярным перемножением строк матрицы A на вектор $\mathbf{v}$ (например, $a_{11}v_1 + \dots + a_{1n}v_n$). Таким образом, пространство решений системы линейных уравнений — это в точности множество векторов $\mathbf{v}$, таких, что $A\mathbf{v} = 0$.

1. **(a)** Решите систему уравнений $\begin{cases} ax + by = e, \\ cx + dy = f \end{cases}$.

(b) Пусть $\overline{v}_1 = (x_1, y_1)$ и $\overline{v}_2 = (x_2, y_2)$ — два вектора на плоскости $\mathbb{E}^2$. Вычислите площадь параллелограмма, натянутого на векторы $\overline{v}_1$ и $\overline{v}_2$.

Определение. Пусть $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ — матрица 2×2. Тогда величина $\det A := ad - bc$ называется *определителем* матрицы A.

Геометрически определитель матрицы — это ориентированная площадь параллелограмма, натянутого на векторы–столбцы матрицы A: если $\overline{v}_1 = \binom{a}{c}$ и $\overline{v}_2 = \binom{b}{d}$, то $\det(A) = \det(\overline{v}_1, \overline{v}_2)$.

2. Докажите следующие свойства определителя:
(a) $\det(\overline{v}_1, \overline{v}_2) = -\det(\overline{v}_2, \overline{v}_1)$,
(b) $\det(\lambda\overline{v}_1, \overline{v}_2) = \lambda \cdot \det(\overline{v}_1, \overline{v}_2)$,
(c) $\det(\overline{v}_1, \overline{v}_2 + \overline{v}_3) = \det(\overline{v}_1, \overline{v}_2) + \det(\overline{v}_1, \overline{v}_3)$,
(d) $\det A = \det A^T$.

3. Определитель матрицы 3×3 — это ориентированный объем параллелепипеда, натянутого на три вектора $(\overline{v}_1, \overline{v}_2, \overline{v}_3)$.
(a) Докажите свойства **(a) – (c)** определителя матрицы 3×3 из предыдущей задачи.

(b) Выведите явную формулу для определителя матрицы $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$.

(c) Задачи для самостоятельного решения

Определение. Пусть x_1, x_2, ..., x_n — перестановка чисел 1, 2, ..., n в каком-то порядке. *Инверсией* называется пара чисел (x_i, x_j) такая, что $i < j$, но $x_i > x_j$. Перестановка x_1, x_2, ..., x_n называется *чётной*, если в ней чётное число инверсий, и *нечётной* в противном случае. *Знак* перестановки σ — это величина $\operatorname{sgn}(\sigma)$, равная $+1$, если перестановка σ четна, и -1, если нечетна.

Любую перестановку можно изобразить в виде ориентированного графа: вершины графа — числа 1, 2, ..., n; ребро $i \to j$ означает, что $\sigma(i) = j$. *Циклом перестановки* называется цикл соответствующего графа.

1. **(a)** Чему равен знак перестановки $(n, n-1, n-2, \dots, 2, 1)$?
   (b) Докажите, что транспозиция двух элементов перестановки меняет ее четность.
   (c) Докажите, что четных и нечетных перестановок поровну.

2. Докажите, что следующие свойства эквивалентны:

   - перестановка содержит чётное количество инверсий;
   - перестановку можно получить из тождественной, используя чётное количество транспозиций;
   - перестановку нельзя получить из тождественной, используя нечётное количество транспозиций;
   - перестановка содержит чётное количество циклов чётной длины.

3. В некотором городе разрешаются только парные обмены квартир (если две семьи обмениваются квартирами, то в тот же день они не имеют права участвовать в другом обмене). Докажите, что любой обмен квартирами можно осуществить за два дня.

4. Пусть $A = (\overline{v}_1, \dots, \overline{v}_n)$ — матрица размера $n \times n$. *Определитель* матрицы A — это функций от координат векторов $\overline{v}_i$, которая линейна по каждому аргументу и кососимметрична по каждой паре аргументов (т.е. при транспозации любых двух аргументов функция меняет знак). Докажите, что если $\overline{v}_i = (a_{1i}, a_{2i}, \dots, a_{ni})^T$, то

$$\det A = \sum_{\sigma} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)},$$

   где $\operatorname{sgn}(\sigma)$ — знак перестановки σ.

Ранги матриц

Ранее мы связали с каждой квадратной матрицей A размера $n \times n$ некоторое число $\det A$, которое называлось определителем матрицы A, и доказали, что однородная система линейных уравнений, заданная матрицей A, имеет единственное решение, если и только если $\det A \neq 0$ (такие матрицы называются *невырожденными*). Сейчас мы рассмотрим вопрос о том, что происходит в случае $\det A = 0$. Как мы помним, в этом случае множество решений соответствующей СЛУ является векторным пространством. Оказывается, размерность этого векторного пространства является важной характеристикой матрицы A. Рассмотрим ее подробнее.

Напомним, что матрицу $n \times n$ можно рассматривать как набор из n векторов векторного пространства $\mathbb{R}^n$, координаты которых записаны по столбцам, и в таком случае $\det A$ — это ориентированный объем параллелепипеда, натянутого на эти векторы. Также ранее мы доказали, что $\det A = \det A^T$, т.е. можно рассматривать координаты векторов, записанных в строку. Именно так мы и будем делать: сейчас для нас будет удобна именно такая нотация.

Итак, рассмотрим матрицу A размера $n \times m$, состоящую из n строк и m столбцов, причем строки матрицы A будем считать векторами $\overline{v}_1, \ldots, \overline{v}_n$: $A = (\overline{v}_1, \ldots, \overline{v}_n)$.

Определение. *Рангом* матрицы $A = (\overline{v}_1, \ldots, \overline{v}_n)$ называется максимальное количество линейно независимых векторов из набора $\{\overline{v}_1, \ldots, \overline{v}_n\}$. Иначе говоря ранг $\operatorname{rk} A$ матрицы A — это размерность векторного пространства, порожденного векторами $\overline{v}_1, \ldots, \overline{v}_n$.

Теорема. Пусть $A = (\overline{v}_1, \ldots, \overline{v}_n)$ — матрица размера $n \times m$ однородной СЛУ S, и $V(S)$ — векторное пространство решений этой СЛУ. Тогда $\dim V(S) = m - \operatorname{rk} A$.

Доказательство. Приведем матрицу A к ступенчатому виду. С точки зрения векторов это означает, что на каждом шаге мы заменяем вектор-строку на линейную комбинацию этого вектора и какого-то другого вектора из нашей матрицы. Поскольку наличие или отсутствие линейной зависимости векторов не меняется при замене этих векторов на их линейные комбинации, ранг матрицы не меняется в результате приведения ее к ступенчатому виду. Поэтому можно считать, что матрица A имеет ступенчатый вид.

Заметим, что в таком случае все ненулевые строки матрицы A — это в точности максимальная система линейно независимых векторов в ней (остальные векторы равны $\overline{0}$, а оставшиеся содержат зависимые переменные, поэтому между ними нет зависимостей). Значит, $\operatorname{rk} A$ — это количество ненулевых строк в ее ступенчатом виде. С другой стороны, каждая ненулевая строка содержит ровно одну зависимую переменную, поэтому количество независимых переменных равно $m - \operatorname{rk} A$. Но это и есть размерность векторного пространства решений СЛУ, что и требовалось доказать.

1. Вычислить ранги следующих матриц: **(a)** $\begin{pmatrix} 1 & 1 & 1 \\ 2 & 2 & 2 \\ 3 & 3 & 3 \end{pmatrix}$, **(b)** $\begin{pmatrix} 0 & 4 & 10 & 1 \\ 4 & 8 & 18 & 7 \\ 10 & 18 & 40 & 17 \\ 1 & 7 & 17 & 3 \end{pmatrix}$,

(c) $\begin{pmatrix} 2 & -1 & 3 & -2 & 4 \\ 4 & -2 & 5 & 1 & 7 \\ 2 & -1 & 1 & 8 & 2 \end{pmatrix}$, **(d)** $\begin{pmatrix} 4 & -7 & -2 & 1 \\ -1 & 3 & 3 & -4 \\ -3 & 5 & 1 & 0 \\ -2 & 3 & 0 & 1 \\ 1 & -2 & -1 & 1 \end{pmatrix}$.

2. Докажите, что для квадратной матрицы A размера $n \times n$ условие $\det A \neq 0$ равносильно условию $\operatorname{rk} A = n$.

3. **(a)** Докажите, что если в матрице A можно выбрать r строк и r столбцов, таких, что матрица B, образованная элементами, стоящими на их пересечении, невырождена (т.е. $\operatorname{rk} B = r$), то $\operatorname{rk} A \geqslant r$.
(b) Докажите, что если $\operatorname{rk} A \geqslant r$, то в матрице A можно выбрать r строк и r столбцов, таких, что матрица B, образованная элементами, стоящими на их пересечении, невырождена.

Следствие. Ранг матрицы — это размер максимальной невырожденной ее подматрицы.

4. Докажите, что $\operatorname{rk} A = \operatorname{rk} A^T$. В частности, отсюда следует, что ранг матрицы равен максимальному количеству линейно независимых векторов-столбцов.

Операции над матрицами

В прошлых листках мы связали с каждой матрицей A ее ранг $\operatorname{rk} A$ — максимальное количество ее линейно независимых векторов-строк или векторов-столбцов. Кроме того, с каждой квадратной матрицей мы связали ее определитель $\det A$, причем $\det A \neq 0$ тогда и только тогда, когда $\operatorname{rk} A$ равен размеру матрицы A. Теперь наша цель — изучить операции над матрицами и понять, как определитель и ранг матрицы меняются при этих операциях.

Одна такая операция нам уже известна — это транспонирование матрицы, т.е. замена ее строк на столбцы, и наоборот. Как мы помним, $\det A^T = \det A$ и $\operatorname{rk} A^T = \operatorname{rk} A$. Теперь изучим операции между несколькими матрицами.

Определение. *Суммой матриц $A = (a_{ij})$ и $B = (b_{ij})$* одинакового размера называется матрица $C = A + B = (a_{ij} + b_{ij})$. Т.е. сложение матриц происходит покомпонентно.
Произведением матриц $A = (\overline{v}_1, \dots \overline{v}_n)^T$ размера $n \times k$ и $B = (\overline{w}_1, \dots, \overline{w}_m)$ размера $k \times m$ называется матрица $C = AB = (\overline{v_i} \cdot \overline{w}_j)$ размера $n \times m$. Иначе говоря, чтобы найти элемент, находящийся в матрице AB в i-й строке и j-м столбце, нужно скалярно перемножить вектор-строку $\overline{v}_i$ матрицы A и вектор-столбец $\overline{w}_j$ матрицы B.
Единичной матрицей E называется матрица (δ_{ij}) размера $n \times n$ (т.е. ее диагональные элементы равны 1, а все остальные элементы равны 0).
Обратной матрицей к квадратной матрице A размера $n \times n$ называется матрица A^{-1}, такая, что $AA^{-1} = E$.

1. Вычислите произведения AB и BA следующих матриц: **(a)** $A = \begin{pmatrix} 4 & 2 \\ 9 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 3 & 1 \\ -3 & 4 \end{pmatrix}$; **(b)** $A = \begin{pmatrix} 2 & 1 \\ -3 & 0 \\ 4 & -1 \end{pmatrix}$ и $B = \begin{pmatrix} 5 & -1 & 6 \\ -3 & 0 & 7 \end{pmatrix}$; **(c)** $A = \begin{pmatrix} 1 & 0 & -2 \\ 2 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 2 & -1 & 1 \\ 0 & -3 & 1 \\ 1 & 2 & 1 \end{pmatrix}$.

2. Дана матрица $A = (a_{ij})$ размера $n \times m$ и вектор-столбец $\overline{v} = (x_1, \dots, x_m)^T$. Вычислите произведение $A\overline{v}$.

3. Вычислите A^{-1} и B^{-1} для следующих матриц: **(a)** $A = \begin{pmatrix} 4 & 2 \\ 9 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 3 & 1 \\ -3 & 4 \end{pmatrix}$; **(b)** $A = \begin{pmatrix} 1 & 0 & -2 \\ 2 & 1 & -1 \\ 0 & 1 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 2 & -1 & 1 \\ 0 & -3 & 1 \\ 1 & 2 & 1 \end{pmatrix}$.

4.* Докажите следующие свойства: **(a)** $\det(AB) = \det A \cdot \det B$; **(b)** $\operatorname{rk}(AB) \leqslant \min(\operatorname{rk} A, \operatorname{rk} B)$; $\operatorname{rk}(A + B) \leqslant \operatorname{rk} A + \operatorname{rk} B$.

Связь ранга и операций над матрицами

Напоминание. *Ранг матрицы A размера $n \times k$*, состоящей из вектор-столбцов $\overline{a}_1, \ldots, \overline{a}_k$, равен максимальному количеству линейно независимых векторов этого набора.
Ранг матрицы B размера $k \times m$, состоящей из вектор-строк $\overline{b_1}, \ldots, \overline{b}_k$, равен максимальному количеству линейно независимых векторов этого набора.
Ранг матрицы равен размерности векторного пространства, порожденного ее вектор-столбцами. Иначе говоря, с каждой матрицей $A = (\overline{a}_1, \ldots, \overline{a}_k)$ можно связать векторное пространство V_A, чьи элементы — это всевозможные линейные комбинации векторов $\overline{a}_1, \ldots, \overline{a}_k$, и тогда $\operatorname{rk} A = \dim V_A$.
Аналогично, с каждой матрицей B, образованной вектор-строками $B = (\overline{b}_1, \ldots, \overline{b}_k)^T$, можно связать векторное пространство V_B, чьи элементы — это всевозможные линейные комбинации векторов $\overline{b}_1, \ldots, \overline{b}_k$, и тогда $\operatorname{rk} B = \dim V_B$.
Наконец, ранг матрицы равен максимальному размеру ее невырожденной подматрицы.

1. Пусть $A = (a_{ij})$ — матрица размера $n \times k$ и $B = (b_{ij})$ — матрица размера $k \times m$. Определим матрицу $C = AB = (c_{ij})$ размера $n \times m$ как произведение матриц A и B.
(a) Запишите элементы $c_{11}, c_{12}, \ldots, c_{1m}$ через a_{ij} и b_{ij}.
(b) Запишите вектор-строку $\overline{c}_1 = (c_{11}, c_{12}, \ldots, c_{1m})$ как линейную комбинацию вектор-строк $\overline{b}_1, \ldots, \overline{c}_k$.
(c) Докажите, что $\operatorname{rk}(AB) \leqslant \operatorname{rk} B$.
(d) Докажите, что $\operatorname{rk}(AB) \leqslant \operatorname{rk} A$.
(e) Докажите, что если матрицы A и B квадратные, причем матрица B невырождена, то $\operatorname{rk}(AB) = \operatorname{rk} A$.

2. **(a)** Пусть $V, W \subseteq U$ — векторные подпространства в векторном пространстве U. Определим сумму $V + W$ векторных пространств V и W как всевозможные суммы векторов из V и W: $V + W = \{v + w : v \in V, w \in W\}$. Докажите, что $\dim(V + W) = \dim V + \dim W - \dim(V \cap W)$.
(b) Пусть $A = (\overline{a}_1, \ldots, \overline{a}_m)$ и $B = (\overline{b}_1, \ldots, \overline{b}_m)$ — матрицы одинакового размера, образованные вектор-столбцами. Определим векторные пространства V_A, V_B и V_{A+B} как пространства, образованные всевозможными линейными комбинациями вектор-столбцов соответствующих матриц. Докажите, что $V_{A+B} \subseteq V_A + V_B$.
(c) Докажите, что $\operatorname{rk}(A + B) \leqslant \operatorname{rk} A + \operatorname{rk} B$.

3.* Пусть A — квадратная матрица над полем $\mathbb{R}$, все недиагональные элементы которой одинаковы и равны $t \geqslant 0$, а все диагональные элементы строго больше t. Докажите, что матрица A невырождена. (*Указание*: рассмотрите матрицу $D = A - tJ$, где $J = (1)$ — матрица из единиц, и докажите, что однородная СЛУ $D\overline{v} = -tJ\overline{v}$ имеет лишь нулевое решение.)

Ранги и комбинаторика

Напоминания. *Ранг матрицы A размера $n \times k$*, состоящей из вектор-столбцов $\overline{a}_1$, ..., $\overline{a}_k$, равен максимальному количеству линейно независимых векторов этого набора.
Ранг матрицы B размера $k \times m$, состоящей из вектор-строк $\overline{b_1}$, ..., $\overline{b}_k$, равен максимальному количеству линейно независимых векторов этого набора.
Ранг матрицы равен размерности векторного пространства, порожденного ее вектор-столбцами. Иначе говоря, с каждой матрицей $A = (\overline{a}_1, \dots, \overline{a}_k)$ можно связать векторное пространство V_A, чьи элементы — это всевозможные линейные комбинации векторов $\overline{a}_1$, ..., $\overline{a}_k$, и тогда $\operatorname{rk} A = \dim V_A$.
Аналогично, с каждой матрицей B, образованной вектор-строками $B = (\overline{b}_1, \dots, \overline{b}_k)^T$, можно связать векторное пространство V_B, чьи элементы — это всевозможные линейные комбинации векторов $\overline{b}_1$, ..., $\overline{b}_k$, и тогда $\operatorname{rk} B = \dim V_B$.
Наконец, ранг матрицы равен максимальному размеру ее невырожденной подматрицы.

Суммой матриц $A = (a_{ij})$ и $B = (b_{ij})$ одинакового размера называется матрица $C = A + B = (a_{ij} + b_{ij})$. Т.е. сложение матриц происходит покомпонентно.
Произведением матриц $A = (\overline{v}_1, \dots \overline{v}_n)^T$ размера $n \times k$ и $B = (\overline{w}_1, \dots, \overline{w}_m)$ размера $k \times m$ называется матрица $C = AB = (\overline{v_i} \cdot \overline{w}_j)$ размера $n \times m$. Иначе говоря, чтобы найти элемент, находящийся в матрице AB в i-й строке и j-м столбце, нужно скалярно перемножить вектор-строку $\overline{v}_i$ матрицы A и вектор-столбец $\overline{w}_j$ матрицы B.
Единичной матрицей E называется матрица (δ_{ij}) размера $n \times n$ (т.е. ее диагональные элементы равны 1, а все остальные элементы равны 0).
Обратной матрицей к квадратной матрице A размера $n \times n$ называется матрица A^{-1}, такая, что $AA^{-1} = E$.

Имеют место следующие неравенства: $\operatorname{rk}(AB) \leqslant \min(\operatorname{rk} A, \operatorname{rk} B)$, $\operatorname{rk}(A + B) \leqslant \operatorname{rk} A + \operatorname{rk} B$. Также если матрица B квадратная и невырожденная, то $\operatorname{rk}(AB) = \operatorname{rk} A$.

Важный факт. Пусть A — квадратная матрица над полем $\mathbb{R}$, все недиагональные элементы которой одинаковы и равны $t \geqslant 0$, а все диагональные элементы строго больше t. Тогда матрица A невырождена.

1. Пусть X — конечное множество из n элементов, а $\mathcal{F}$ — семейство его собственных подмножеств, такое, что для каждой пары различных элементов из X есть единственное подмножество из $\mathcal{F}$, которое их содержит. Докажите, что $|\mathcal{F}| \geqslant n$.

2. Пусть $\mathcal{F} - \{A_1, \dots, A_k\}$ — набор различных подмножеств множества из n элементов, такой, что все пересечения $A_i \cap A_j$ для $i \neq j$ имеют фиксированный размер $t \in [1; n]$. Докажите, что $k \leqslant n$.

3. Назовем *костепенью* пары вершин графа количество вершин графа, смежных с ними обеими. Докажите, что если все костепени графа на n вершинах нечетны, то и n нечетно.

4. На встречу пришли $2n$ людей. Каждый человек знаком с четным количеством других людей (знакомство взаимно). Докажите, что есть пара человек, имеющая четное число общих знакомых.

Комбинаторная теорема о нулях

В этом листке мы познакомимся с важной модификацией известной теоремы Гильберта о нулях, которая часто бывает полезна в различных комбинаторных задачах. Грубо говоря, утверждается, что многочлен от многих переменных на достаточно большом конечном множестве принимает ненулевое значение. Размеры этого множества могут быть описаны в терминах степеней переменных, входящих в старший член этого многочлена. Более того, можно даже явно выписать формулу, позволяющую находить коэффициент при старшем члене. С этой точки зрения комбинаторная теорема о нулях является обобщением интерполяционного многочлена Лагранжа.

Необходимые сведения

Пусть K — произвольное поле, т.е. множество, в котором определены все четыре арифметические операции: сложения, вычитания, умножения и деления, причем эти операции удовлетворяют привычным нам свойствам коммутативности, ассоциативности и дистрибутивности. В качестве основных примеров можно рассматривать поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и $\mathbb{Z}_p$.

Следующая теорема известна под названием теоремы Гильберта о нулях и является одной из фундаментальных теорем в алгебраической геометрии.

Теорема Гильберта о нулях. Пусть g_1, ..., $g_m \in \mathbb{C}[x_1, \dots, x_n]$ — произвольные многочлены с комплексными коэффициентами, и X — множество нулей системы уравнений $g_1 \dots = g_m = 0$. Пусть также $f \in \mathbb{C}[x_1, \dots, x_n]$ — такой многочлен, который зануляется на X, т.е. $f(x) = 0$ для всех $x \in X$. Тогда существуют такое натуральное k и многочлены h_1, ..., $h_m \in \mathbb{C}[x_1, \dots, x_n]$, что

$$f^k = \sum_{i=1}^{m} h_i g_i.$$

Замечание. Вообще говоря, теорема Гильберта о нулях справедлива над любым алгебраически замкнутым полем. Поле называется *алгебраически замкнутым*, если любой многочлен с коэффициентами из этого поля имеет корень, принадлежащий этому полю (отсюда следует, что все его корни принадлежат данному полю). Поле комплексных чисел $\mathbb{C}$ — единственный известный нам пример алгебраически замкнутого поля (это по сути и есть основная теорема алгебры). Тем не менее, доказательство теоремы Гильберта о нулях для поля $\mathbb{C}$ гораздо проще, нежели для общего случая (хотя и оно далеко не просто).

Эта теорема доказывается с помощью методов, выходящих за рамки школьной программы. Однако в таком виде теорема нам и не понадобится. Нас будет интересовать частный случай этой теоремы. Удивительно, что этот частный случай, хоть и доказывается довольно легко, но при этом, во-первых, крайне полезен в самых разных ситуациях, а во-вторых,

содержит более сильное по сравнению с классической теоремой Гильберта о нулях утверждение. Оно и называется *комбинаторной теоремой о нулях*.

Комбинаторная теорема о нулях. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле, $S_1, \ldots, S_n \subset K$ — его непустые конечные подмножества (возможно, пересекающиеся) и

$$g_i(x_1, \ldots, x_n) = \prod_{s \in S_i} (x_i - s), \qquad \text{где } i = 1, \ldots, n.$$

Предположим, что многочлен $f \in K[x_1, \ldots, x_n]$ зануляется на решетке $S_1 \times \ldots \times S_n$, т.е.

$$f(s_1, \ldots, s_n) = 0 \qquad \text{для всех наборов } (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n.$$

Тогда существуют такие многочлены $h_1, \ldots, h_n \in K[x_1, \ldots, x_n]$, что $\deg h_i \leqslant \deg f - \deg g_i$ и

$$f = \sum_{i=1}^{n} h_i g_i.$$

Доказательство. Положим $t_i = |S_i| - 1$ (причина необходимости вычесть единицу станет ясна из дальнейшего). Рассмотрим редукцию многочлена f по модулям $g_1, \ldots, g_n$. А именно, представим сначала f как многочлен от x_1 со старшим коэффициентом $f_1(x_2, \ldots, x_n)$. Тогда разность $f - f_1 g_1$ имеет по переменной x_1 степень не выше t_1. Применяя последовательно аналогичные действия для оставшихся переменных, мы получим конце концов новый многочлен $\overline{f} = f - h_i g_1 - \ldots - h_n g_n$, степень которого по переменной x_i не превосходит t_i, причем $\deg h_i \leqslant \deg f - \deg g_i$ (поскольку в ходе нашего процесса мы на каждом шаге не увеличивали степень многочлена). Наша цель — доказать, что $\overline{f} \equiv 0$.

Заметим, что многочлен $\overline{f}$ равен 0 на множестве $S_1 \times \ldots \times S_n$. Докажем, что отсюда следует искомое тождество $\overline{f} = 0$.

Будем вести доказательство индукцией по количеству переменных n. Для $n = 1$ это следует из теоремы Безу: многочлен от одной переменной степени не выше t_1, обращающийся в 0 в $t_1 + 1$ точке, тождественно равен 0 (вот для чего нужна единица в определении t_i). Для совершения шага индукции рассмотрим $\overline{f}$ как многочлен от x_n:

$$\overline{f}(x_1, \ldots, x_n) = \sum_{i=0}^{t_n} \overline{f}_i(x_1, \ldots, x_{n-1}) x_n^i.$$

Зафиксируем произвольный набор $(s_1, \ldots, s_{n-1}) \in S_1 \times \ldots \times S_{n-1}$. Тогда многочлен $\overline{f}(s_1, \ldots, s_{n-1}, x_n)$ является многочленом от одной переменной x_n степени не выше t_n и принимает в $t_n + 1$ точке значение 0. Значит, он тождественно равен 0, откуда следует, что $\overline{f}_i(s_1, \ldots, s_{n-1}) = 0$, т.е. многочлены $\overline{f}_i$ от $(n-1)$ переменной зануляются на всей решетке $S_1 \times \ldots \times S_{n-1}$. Применяя предположение индукции, получаем, что $\overline{f}_i \equiv 0$, откуда и $\overline{f} \equiv 0$, что и требовалось доказать.

В процессе доказательства КТН мы использовали теорему Безу: коэффициенты многочлена от одной переменной однозначно задаются его значениями в подходящем количестве точек. Оказывается, что аналогичный факт справедлив и для многочленов большей степени, и такой факт также носит название комбинаторной теоремы о нулях.

Комбинаторная теорема о нулях, версия 2. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле, $S_1, \dots, S_n \subset K$ — его непустые конечные подмножества (возможно, пересекающиеся), такие, что $|S_i| = d_i + 1$ для всех $i = 1, \dots, n$. Пусть также $f \in K[x_1, \dots, x_n]$ — многочлен с коэффициентами из поля K, а $x_1^{d_1} \dots x_n^{d_n}$ — его моном. Тогда если этот моном является старшим относительно какого-то лексикографического порядка, то коэффициент $[f]_{x_1^{d_1} \dots x_n^{d_n}}$ при этом мономе однозначно задается значениями многочлена f на решетке $S_1 \times \dots \times S_n$. А именно, справедлива следующая формула:

$$[f]_{x_1^{d_1} \dots x_n^{d_n}} = \sum_{(s_1,\dots,s_n) \in S_1 \times \dots \times S_n} \frac{f(s_1, \dots, s_n)}{\varphi_{s_1,S_1} \cdot \dots \cdot \varphi_{s_n,S_n}}, \tag{1}$$

где $\varphi_{s,S} := \prod\limits_{t \in S, t \neq s} (s - t)$.

Замечания. 1. Условие «моном $x_1^{d_1} \dots x_n^{d_n}$ является старшим относительно какого-то лексикографического порядка» означает, что у любого монома $x_1^{e_1} \dots x_n^{e_n}$ с ненулевым коэффициентом хотя бы одна степень e_i строго меньше соответствующей степени d_i.
2. Можно пробовать восстановить коэффициенты при мономах многочлена f, решая соответствующую систему линенйных уравнений, которые получаются при подстановке в многочлен f элементов решетки $S_1 \times \dots \times S_n$. Однако данная система может иметь бесконечное количество неизвестных, т.к. всегда можно добавить к многочлену f мономы, удовлетворяющие условию п.1 и зануляющиеся на решетке $S_1 \times S_n$. Смысл данной формулировки КТН заключается в том, что тем не менее можно явно найти часть решений такой бесконечной системы.

Доказательство. Заметим, что обе части формулы (1) линейны по f, поэтому достаточно доказать эту формулу в случае, когда f — это моном, т.е. без ограничения общности можно считать, что $f(x_1, \dots, x_n) = x_1^{e_1} \dots x_n^{e_n}$, причем либо $(e_1, \dots, e_n) = (d_1, \dots, d_n)$, либо существует такой индекс i, что $e_i < d_i$. Заметим, что в случае, когда f — это моном, правая часть формулы (1) раскладывается на множители:

$$\sum_{(s_1,\dots,s_n) \in S_1 \times \dots \times S_n} \frac{s_1^{c_1} \dots s_n^{c^n}}{\varphi_{s_1,S_1} \cdot \dots \cdot \varphi_{s_n,S_n}} = \prod_{i=1}^{n} \frac{s_i^{c_i}}{\varphi_{s_i,S_i}}.$$

Заметим, что при $n = 1$ формула (1) верна: это следует из интерполяционного многочлена Лагранжа. Осталось заметить, что в случае $(e_1, \dots, e_n) = (d_1, \dots, d_n)$ каждая дробь $\dfrac{s_i^{e_i}}{\varphi_{s_i,S_i}}$ равна 1 (мы применяем формулу интерполяционного многочлена Лагранжа к многочлену $x_i^{d_i}$), а в случае, когда $e_i < d_i$ дробь $\dfrac{s_i^{e_i}}{\varphi_{s_i,S_i}}$ (а вместе с ней и вся правая часть формулы (1)) равна 0. В обоих случаях правая часть оказывается равной коэффициенту при мономе $x_1^{e_1} \dots x_n^{e_n}$. Таким образом, формула (1) доказана.

Перед тем как применять комбинаторную теорему о нулях, посмотрим, как можно вычислять коэффициенты при мономах различных многочленов. Для этого используется один трюк, который мы обсудим на следующем известном примере.

Пример. Пусть $f(x_1, \dots, x_n) = (x_1+\dots+x_n)^{d_1+\dots+d_n}$. Докажите, что $[f]_{x_1^{d_1}\dots x_n^{d_n}} = \dfrac{(d_1+\dots+d_n)!}{d_1!\dots d_n!}$.

Решение. Конечно, эту задачу несложно решить комбинаторно: у нас есть $d_1+\dots+d_n$ скобок $(x_1+\dots+x_n)$, и мы хотим выбрать из них d_i штук, откуда возьмем слагаемое x_i. Сделать это можно

$$C_{d_1+\dots+d_n}^{d_1} \cdot C_{d_2+\dots+d_n}^{d_2} \cdot \dots \cdot C_{d_{n-1}+d_n}^{d_{n-1}} \cdot C_{d_n}^{d_n} = \frac{(d_1+\dots+d_n)!}{d_1!\dots d_n!}$$

способами. Но наша цель — научиться применять формулу (1), поэтому мы рассмотрим другое решение.

Чтобы применить формулу (1), нам нужно вычислить значения многочлена f на некоторой решетке $S_1 \times \dots \times S_n$, где $|S_i| = d_i + 1$. Попробуем в качестве множеств S_i взять такие: $S_i = \{0, 1, 2, \dots, d_i\}$. К сожалению, значение многочлена f в произвольной точки так определенной решетки устроено трудно — это какая-то большая степень. Идея заключается в том, чтобы изменить многочлен f, не изменяя при этой коэффициента $[f]_{x_1^{d_1}\dots x_n^{d_n}}$, и изменит ь его таким образом, чтобы почти во всех точках нашей решетки значения измененного многочлена g были бы равны 0.

Рассмотрим в качестве многочлена g следующий:

$$g(x_1, \dots, x_n) = \prod_{s=0}^{d_1+\dots+d_n-1} (x_1 + \dots + x_n - s).$$

Ясно, что изменив каждую скобку на константу s, мы не изменим старших членов, в частности, $[f]_{x_1^{d_1}\dots x_n^{d_n}} = [g]_{x_1^{d_1}\dots x_n^{d_n}}$. С другой стороны, для любого набора $(x_1, \dots, x_n)$, отличного от $(d_1, \dots, d_n)$, найдется такое s из отрезка $[0; d_1+\dots+d_n-1]$, что $x_1+\dots+x_n = s$, так что для всех точек решетки $S_1 \times \dots \times S_n$, кроме точки $(d_1, \dots, d_n)$, значение многочлена g равно 0. Кроме того, $g(d_1, \dots, d_n) = (d_1+\dots+d_n)!$, а $\phi_{d_i,S_i} = d_i!$. Таким образом,

$$[f]_{x_1^{d_1}\dots x_n^{d_n}} = [g]_{x_1^{d_1}\dots x_n^{d_n}} = \sum_{(x_1,\dots,x_n)\in S_1\times\dots\times S_n} \frac{g(x_1, \dots, x_n)}{\phi_{x_1,S_1} \cdot \dots \cdot \phi_{x_n,S_n}} = \frac{(d_1+\dots+d_n)!}{d_1!\dots d_n!},$$

что и требовалось.

Этот пример может показаться искусственным, однако в следующей задаче элементарного комбинаторного решения неизвестно, а сама задача называется *гипотезой Дайсона*, и возникла она в теории случайных матриц в 1962 г.

Гипотеза Дайсона. Пусть $f(x_1, \dots, x_n) = \prod_{1\leqslant i\neq j\leqslant n}(x_i - x_j)^{d_i}$, где d_1, ..., d_n — произвольные неотрицательные целые числа. Докажите, что

$$[f]_{(x_1^{d_2+\dots+d_n}\dots x_n^{d_1+\dots+d_{n-1}})} = \frac{(d_1+\dots+d_n)!}{d_1!\dots d_n!}.$$

Следствие. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле и $f \in K[x_1, \dots, x_n]$ — произвольный многочлен, старший член которого имеет вид $Cx_1^{d_1} \dots x_n^{d_n}$,

где $C \neq 0$ (т.е. степень $\sum d_i$ является максимальной среди всевозможных степеней мономов, входящих в f; если существует несколько мономов максимальной степени, можно взять любой из них). Обозначим через $S_1, \ldots, S_n \subset K$ произвольные непустые конечные подмножества поля K (возможно, пресекающиеся), такие, что $|S_i| \geqslant d_i + 1$. Тогда существует такой набор $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$, что $f(s_1, \ldots, s_n) \neq 0$.

Мы приведем два доказательства этого следствия: с помощью первой версии КТН и второй версии.

Первое доказательство. Предположим противное, рассмотрим многочлены g_i, указанные в первой версии комбинаторной теоремы о нулях, и представим f в виде $\sum\limits_i h_i g_i$. Старший член $x_1^{d_1} \ldots x_n^{d_n}$ многочлена f должен также быть старшим членом в представлении $\sum\limits_i h_i g_i$. Но $\deg h_i g_i = \deg g_i + \deg h_i \leqslant \deg f$, причем в случае равенства старший коэффициент многочлена $h_i g_i$ содержит множитель $x_i^{|S_i|}$, который получается при раскрытии скобок в произведении $\prod\limits_{s \in S_i} (x_i - s) = g_i$. Таким образом, моном $x_1^{d_1} \ldots x_n^{d_n}$ в выражении $\sum\limits_i h_i g_i$ отстствует, что невозможно. Мы получили противоречие.

Второе доказательство. Вновь предположим противное: пусть $f(s_1, \ldots, s_n) = 0$ для всех наборов $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$. Тогда, применяя формулу для коэффициента при старшем мономе из второй версии КТН, получаем, что $[f]_{x_1^{d_1} \ldots x_n^{d_n}} = 0$ — противоречие.

Аддитивная комбинаторика

В чем смысл комбинаторной теоремы о нулях? В том, что она позволяет переводить на алгебраический язык комбинаторные утверждения. Обычно это происходит примерно по такой схеме. Неравенства, связанные с каким-то переменными в задаче, позволяют найти старший член многочлена f, который строится по данным условия. А вот построение самого многочлена f может представлять определенные сложности. Наша цель — рассуждая от противного, построить такой многочлен, который занулялся бы в слишком большом числе точек и при этом был бы ненулевым. Обычно построение такого многочлена состоит из двух этапов.

Первый этап (более простой, так сказать, *регулярный*) заключается в переформулировке условия задачи в терминах зануления каких-то многочленов (обычно линейных) и затем перемножении полученных многочленов. Это обычно обеспечивает наличие довольно большого числа нулей у многочлена.

Второй этап (более хитрый, *нерегулярный*), заключается в модификации многочлена, полученного на первом этапе, таким образом, чтобы он, во-первых, занулялся именно во всех точках, а во-вторых, имел бы ненулевой старший член (напомним, что старшинство обеспечивается ограничениями из условий задачи).

В простых ситуациях бывает достаточно и первого этапа, но обычно без второго этапа не обойтись. При этом способы подправить многочлен на первый взгляд кажутся довольно

изощренными. Поэтому мы покажем три разных способа, как можно реализовать такую поправку; другие задачи обычно требуют только небольшой модификации этих приемов.

Пример. В трехмерном пространстве рассматриваются отличные от начала координат точки с целыми неотрицательными координатами, не превосходящими n. Каким наименьшим числом плоскостей, не проходящих через начало координат, можно покрыть эти точки?

Решение. Пример $\{x = i\}, \{y = j\}, \{z = k\}$, где $i, j, k = 1, \ldots, n$, показывает, что $3n$ плоскостей достаточно. Докажем, что меньшим числом плоскостей обойтись не удается.

Предположим противное: пусть нам удалось покрыть нужные нам точки $3n - 1$ плоскостью. Пусть $\{a_l x + b_l y + c_l z + d_l = 0\}$ — уравнения этих плоскостей. Мы хотим построить многочлен, зависящий от трех переменных x, y, z, который бы принимал нулевое значение во всех наших точках, а также в начале координат. Его построение мы осуществим в два этапа.

На первом этапе ясно, что нужно рассмотреть произведение

$$f_1(x, y, z) = \prod_{l=1}^{3n-1} (a_l x + b_l y + c_l z + d_l).$$

Этот многочлен зануляется во всех нужных нам точках, отличных от начала координат.

На втором этапе нам нужно добиться зануления и в начале координат. Для этого полезно сделать такой трюк. Давайте возьмем многочлены из нашего примера и перемножим их, т.е. рассмотрим многочлен

$$f_2(x, y, z) = \prod_{i,j,k=1}^{n} (x - i)(y - j)(z - k).$$

Он также зануляется во всех наших точках, кроме начала координат. Но тогда положим $\delta = f_1(0, 0, 0)/f_2(0, 0, 0)$ и рассмотрим многочлен $f = f_1 - \delta f_2$. Он и будет искомым.

Заметим, что $\deg f = 3n$. Очевидно, что коэффициент при мономе $x^n y^n z^n$ равен $-\delta$ и отличен от 0. Рассмотрим множества $S_1 = S_2 = S_3 = \{0, 1, \ldots, n\}$, мощность каждого из которых равна $n + 1$. Тогда многочлен f зануляется на решетке $S_1 \times S_2 \times S_3$, а значит, он тождественно равен нулю, что невозможно. Полученное противоречие доказывает наше утверждение.

1. **Теорема Коши–Дэвенпорта.** Пусть p — простое число и $A, B \subset \mathbb{Z}_p$ — два непустых подмножества в $\mathbb{Z}_p$, состоящие из a и b элементов соответственно. Тогда

$$|A+B| \geqslant \min(p, a+b-1).$$

2. Пусть p — простое и $A \subset \mathbb{Z}_p$ — произвольное непустое подмножество. Положим $A \oplus A = \{a+a' : a, a' \in A, a \neq a'\}$. Докажите, что тогда $|A \oplus A| \geqslant \min(p, 2|A|-3)$.

3. Пусть p — простое число, $A_0, \ldots, A_k \subset \mathbb{Z}_p$ — некоторые непустые подмножества и $h \in \mathbb{Z}_p[x_0, \ldots, x_k]$ — произвольный многочлен. Положим

$$\oplus_h \sum_i A_i := \{a_0 + \ldots + a_k : a_i \in A_i, h(a_0, \ldots, a_k) \neq 0\}.$$

Положим $|A_i| = t_i + 1$ и $m = \sum_i t_i - \deg h$. Тогда если коэффициент при мономе $\prod_i x_i^{t_i}$ в многочлене $(x_0 + \ldots + x_k)^m h(x_0, \ldots, x_k)$ не равен 0 в $\mathbb{Z}_p$, то $\left| \oplus_h \sum_i A_i \right| \geqslant m+1$.

4. Пусть p — простое число и $A_0, \ldots, A_k \subset \mathbb{Z}_p$ — некоторые непустые подмножества. Предположим, что $|A_i| \neq |A_j|$ для всех $i \neq j$, и $\sum_i |A_i| \leqslant p + C_{k+2}^2 - 1$. Тогда

$$\left|\{a_0 + \ldots + a_k : a_i \in A_i, a_i \neq a_j\}\right| \geqslant \sum_i |A_i| - C_{k+2}^2 + 1.$$

5. Пусть p — простое число, $S_1, \ldots, S_k \subset \mathbb{Z}_{\geqslant 0}$ — произвольные подмножества, содержащие 0 и не содержащие двух сравнимых по модулю p чисел. Предположим, что $\sum_i (|S_i|-1) \geqslant p$. Тогда для любых $a_1, \ldots, a_k \in \mathbb{Z}_p$ уравнение $\sum_i a_i x_i = 0$ имеет отличное от нулевого решение $(x_1, \ldots, x_k) \in S_1 \times \ldots \times S_k$.

6. В вершинах правильного 100-угольника написаны по два различных числа a и b. Докажите, что можно стереть по одному числу из каждой вершины так, чтобы никакие две соседние вершины не содержали бы одинаковых чисел.

Комбинаторная теорема о нулях – 2

Комбинаторная теорема о нулях. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле, $S_1, \ldots, S_n \subset K$ — его непустые конечные подмножества (возможно, пересекающиеся) и

$$g_i(x_1, \ldots, x_n) = \prod_{s \in S_i} (x_i - s), \qquad \text{где } i = 1, \ldots, n.$$

Предположим, что многочлен $f \in K[x_1, \ldots, x_n]$ зануляется на решетке $S_1 \times \ldots \times S_n$, т.е.

$$f(s_1, \ldots, s_n) = 0 \qquad \text{для всех наборов } (s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n.$$

Тогда существуют такие многочлены $h_1, \ldots, h_n \in K[x_1, \ldots, x_n]$, что $\deg h_i \leqslant \deg f - \deg g_i$ и

$$f = \sum_{i=1}^{n} h_i g_i.$$

Комбинаторная теорема о нулях, версия 2. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле, $S_1, \ldots, S_n \subset K$ — его непустые конечные подмножества (возможно, пересекающиеся), такие, что $|S_i| = d_i + 1$ для всех $i = 1, \ldots, n$. Пусть также $f \in K[x_1, \ldots, x_n]$ — многочлен с коэффициентами из поля K, а $x_1^{d_1} \ldots x_n^{d_n}$ — его моном. Тогда если этот моном является старшим относительно какого-то лексикографического порядка, то коэффициент $[f]_{x_1^{d_1} \ldots x_n^{d_n}}$ при этом мономе однозначно задается значениями многочлена f на решетке $S_1 \times \ldots \times S_n$. А именно, справедлива следующая формула:

$$[f]_{x_1^{d_1} \ldots x_n^{d_n}} = \sum_{(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n} \frac{f(s_1, \ldots, s_n)}{\varphi_{s_1, S_1} \cdot \ldots \cdot \varphi_{s_n, S_n}}, \tag{2}$$

где $\varphi_{s,S} := \prod\limits_{t \in S, t \neq s} (s - t)$.

Следствие. Пусть K — произвольное (не обязательно алгебраически замкнутое) поле и $f \in K[x_1, \ldots, x_n]$ — произвольный многочлен, старший член которого имеет вид $C x_1^{d_1} \ldots x_n^{d_n}$, где $C \neq 0$ (т.е. степень $\sum d_i$ является максимальной среди всевозможных степеней мономов, входящих в f; если существует несколько мономов максимальной степени, можно взять любой из них). Обозначим через $S_1, \ldots, S_n \subset K$ произвольные непустые конечные подмножества поля K (воможно, пресекающиеся), такие, что $|S_i| \geqslant d_i + 1$. Тогда существует такой набор $(s_1, \ldots, s_n) \in S_1 \times \ldots \times S_n$, что $f(s_1, \ldots, s_n) \neq 0$.

Пример (теорема Алона-Фридланда-Калаи). Пусть p — простое число и $G = (V, E)$ — мультиграф без петель, удовлетворяющий следующим условиям:

- $\Delta(G) \leqslant 2p - 1$ (максимальная степень вершины не больше $2p - 1$);
- $\frac{2|E|}{|V|} > 2p - 2$ (средняя степень вершин больше $2p - 2$).

Тогда в G есть p-регулярный подграф (т.е. подграф, степень каждой вершины которого равна p).

Решение. В задачах, связанных с графами, многочлены обычно строятся по таком принципу. Давайте занумеруем все ребра нашего графа и сопоставим каждому ребру e переменную x_e. (В некоторых ситуациях нужно нумеровать вершины, это часто бывает полезно при раскрашивании вершин графа.) Переменные нашего многочлена f будут принимать либо значение 0, либо значение 1, т.е. множества $S_e = \{0, 1\}$. Смысл этого ограничения в том, что если нам нужно найти подграф с требуемыми свойствами, то достаточно указать набор его ребер. Мы сформулируем эти свойства в терминах нашего многочлена, а затем возьмем те ребра e, для которых $x_e = 1$. Для того, чтобы найти вершины, из которых выходят нужные нам ребра, полезно рассмотреть числа $a_{v,e}$, которые индексируются двумя числами: первое — это номер вершины v, второе — номер ребра e. Тогда $a_{v,e} = 1$, если ребро e выходит из вершины v, и $a_{v,e} = 0$ в противном случае. Поэтому оставить вершину v и некоторые выходящие из нее ребра — это все равно что рассмотреть линейную комбинацию $\sum\limits_{e \in E} a_{v,e} x_e$, где переменные x_e принимают значения 0 или 1. Мы хотим оставить такие ребра, чтобы степени всех вершин были бы равны p.

Приступим к реализации нашего плана. Наличие простого числа p указывает на необходимость работы над полем $\mathbb{Z}_p$ и использовании малой теоремы Ферма для зануления каких-то выражений. Если нас интересуют вершины v, чья степень равна p, то это все равно что обращение в нуль суммы $\sum\limits_{e \in E} a_{v,e} x_e$ при различных значениях x_e. Поэтому сначала занулим практически все такие суммы, рассмотрев многочлен

$$f_1(x_e) = \prod_{v \in V} \Big(1 - \big(\sum_{e \in E} a_{v,e} x_e\big)^{p-1}\Big).$$

Этот многочлен зануляется при всех значениях переменных $\{x_e\}$, для которых $\sum\limits_{e \in E} a_{v,e} x_e \not\equiv_p 0$.

Теперь нам нужно как-то подправить этот многочлен, чтобы включить во множество ее нулей случай $\{x_e\} = \{0\}$. Простейший многочлен от переменных $\{x_e\}$, также зануляющийся практически всюду, – это многочлен

$$f_2(x_e) = \prod_{e \in E} (1 - x_e).$$

Осталось скомбинировать многочлены f_1 и f_2 в многочлен $f = f_1 - f_2$.

Итак, рассмотрим многочлен f. Заметим, что

$$\deg f = \max\big((p-1)|V|, |E|\big) = |E|$$

в силу ограничения на среднюю степень вершин. Рассмотрим моном $\prod_{e \in E} x_e$, коэффициент при котором очевидно, не равен 0. Тогда найдется такой набор $\{x_e\} = \{\alpha_e\}$, для которого $f(\alpha_e) \neq 0$. Заметим, что, во-первых, этот набор отличен от нулевого, а во-вторых, тогда $\sum_{e \in E} a_{v,e}\alpha_e \equiv 0 \pmod{p}$ для всех вершин v, т.е. степень каждой вершины кратна p. Выберем теперь подграф в G, состоящий из всех вершин и тех ребер e, для которых $\alpha_e = 1$. Вспоминая, что максимальная степень вершин меньше $2p$, заключаем, что каждая вершина в нашем подграфе имеет степень 0 или p. Поскольку набор $\{\alpha_e\}$ отличен от нулевого, то все вершины не могут иметь степень 0. Оставим те вершины, которые имеют ненулевую степень. Вместе с выбранными ребрами они образуют искомый p-регулярный граф.

1. В вершинах правильного 100-угольника написаны по два различных числа a и b. Докажите, что можно стереть по одному числу из каждой вершины так, чтобы никакие две соседние вершины не содержали бы одинаковых чисел.

2. Пусть p — простое число и $G = (V, E)$ — граф на $|V| > d(p-1)$ вершинах. Тогда существует такое непустое подмножество $U \subset V$, что количество d-клик в графе G, имеющих общие вершины с U, кратно p.

Конечные проективные плоскости

Ранее мы обсуждали комбинаторные задачи, которые можно решить с помощью векторных пространств и систем линейных уравнений. Обычно для этого необходимо параметризовать объекты в задаче набором переменных (векторами в многомерном пространстве), и тогда условия, накладываемые на эти переменные, определяют некоторое векторное подпространство или матрицу, характеристики которых позволяют дать ответ на поставленный вопрос.

Сейчас мы рассмотрим несколько иную, в каком-то смысле более геометрическую конструкцию, связанную с параметризацией данных задачи и поиском соотношений между этими данными. А именно, нам будет полезно трактовать объекты задачи как точки, а наборы из этих объектов — как прямые. Оказывается, что если так введенные наборы точек и прямых удовлетворяют некоторым естественным аксиомам, то можно очень многое сказать о количестве точек и прямых, а также использовать классическую геометрическую интуицию для толкования комбинаторных условий задач.

1. Даны 1985 множеств, каждое из которых состоит из 45 элементов, причём объединение любых двух множеств содержит ровно 89 элементов. Сколько элементов содержит объединение всех этих 1985 множеств?

2. **Определение.** *Конечной проективной плоскостью* называется конечное множество объектов («*точки*»), среди которых выбраны некоторые подмножества («*прямые*»), удовлетворяющее следующие условиям:

1. Через любые две точки проходит ровно одна прямая.
2. Любые две прямые пересекаются ровно в одной точке.
3. Существуют четыре точки, никакие три из которых не лежат на одной прямой.

(a) Докажите, что на любой прямой лежит одинаковое количество точек. Будем в дальнейшем обозначать это количество через $n + 1$.
(b) Докажите, что через любую точку проходит $n + 1$ прямых.
(c) Докажите, что на конечной проективной плоскости ровно $n^2 + n + 1$ точек и ровно $n^2 + n + 1$ прямых. В таком случае говорят, что конечная проективная плоскость *имеет порядок n*.
(d) Нарисуйте конечную проективную плоскость порядка 2 (она называется *плоскостью Фано*).

Факт. Для любого простого числа $p > 2$ существует конечная проективная плоскость порядка p (и даже порядка p^k, где k — произвольное натуральное число).

3. В классе ученики ходят на 10 кружков, каждый кружок посещают четверо, и для любых двух кружков есть только один ученик, который ходит на оба кружка. Сколько может быть учеников в классе?

4. Фокусник с помощником показывают фокус. В ряд стоят 13 закрытых пустых шкатулок. Фокусник уходит, а зритель на виду у помощника прячет по монетке в любые две шкатулки по своему выбору. Затем возвращается фокусник. Помощник открывает одну шкатулку, в которой нет монетки. Далее фокусник указывает на 4 шкатулки, и их одновременно открывают. Цель фокусника — открыть обе шкатулки с монетками. Предложите способ, как договориться фокуснику с помощником, чтобы этот фокус всегда удавался.

5. **(a)** У правильного 1981-угольника отмечены 64 вершины. Доказать, что существует трапеция с вершинами в отмеченных точках.

(b) Какое максимальное число вершин можно отметить в правильном 31-угольнике таким образом, что никакие 4 из них не образовывали трапецию, и никакие 3 не образовывали равнобедренный треугольник?

Проективные пространства и многочлены в кольцах $\mathbb{Z}_{p^m}[x]$

Сейчас мы свяжем теоретические факты, которые мы осваивали, работая с векторными пространствами (базис, размерность, координаты, СЛУ…), геометрические основы проективной геометрии и комбинаторику конечных проективных плоскостей. Оказывается, что все три этих сюжета тесно связаны друг с другом, и сегодня мы поговорим об этих взаимосвязях.

Начнем с уже знакомой нам проективной геометрии. Напомним, что суть проективной геометрии заключается в отказе от параллельности: в ней любые две прямые пересекаются. Классики проективной геометрии для достижения этой цели говорили не очень понятное логически, но вполне приемлемое с точки зрения наглядности утверждение: *параллельные прямые пересекаются в бесконечно удаленной точке*. Однако этим словам можно придать формальный смысл. Делается это с помощью так называемой *модели связки проективной плоскости*. Напомним ее.

Рассмотрим евклидову плоскость $\mathbb{E}^2 := \alpha$ и трехмерное пространство $\mathbb{E}^3$, содержащее эту плоскость. Выберем в этом пространстве произвольную точку O, не лежащую в плоскости α, и рассмотрим множество всевозможных прямых, проходящих через эту точку. Это множество называется *проективной плоскостью* и обозначается через $\mathbb{R}P^2$, а каждая прямая, проходящая через точку O, называется *проективной точкой*. Если пересечь проведенные нами через O прямые плоскостью α, то почти все прямые пересекут ее в каких-то точках. Т.е. каждая проективная точка высечет на евклидовой плоскости точку обычную. Однако есть и такие проективные точки, которые не видны на плоскости α. Это в точности те проективные точки, которые соответствуют прямым, параллельным плоскости α. Все такие точки лежат в евклидовой плоскости α_∞, параллельной плоскости α и проходящей через O. Именно эти проективные точки и называются *бесконечно удаленными* с точки зрения плоскости α — ведь на ней они просто не видны!

Если вместо прямых мы будем проводить через точку O в трехмерном пространстве $\mathbb{E}^3$ плоскости, то на евклидовой плоскости α они высекут прямые. Поэтому логично назвать такие плоскости *проективными прямыми* а проективную прямую α_∞ — *бесконечно удаленной* прямой для евклидовой плоскости α.

Остановимся пока на этом геометрическом введении и попробуем обобщить наши конструкции, заменив в них евклидово пространство $\mathbb{E}^3$ на *векторное пространство* V. Именно подобная общность конструкции поможет нам в дальнейшем единообразно определить и классическую проективную геометрию, и конечные проективные плоскости из комбинаторики.

Итак, рассмотрим векторное пространство V размерности $n+1$ (единицу мы плюсуем, потому что изначально мы стартовали с евклидовой плоскости, а затем поднялись в трехмерное евклидово пространство. Сейчас мы сразу берем пространство на единицу большей размерности). Для каждого ненулевого вектора $v \in V$ определим *прямую* $\hat{v}$, натяну-

тую на вектор v, как множество векторов, пропорциональных v: $\hat{v} = \{\lambda v : \lambda \in \mathbb{R}^*\}$. Множество всех таких векторов назовем *проективным пространством* и обозначим через PV (иногда оно также называется *проективизацией пространства* V). Элементы этого пространства, т.е. прямые $\hat{v}$, назовем *проективными точками*. Размерность этого пространства по определению полагается равной n (обратите внимание, что проективное пространство PV не является векторным: в нем невозможно корректно определить операцию сложения проективных точек!).

Если мы хотим определить *проективные прямые*, то вместо прямых λv нужно проводить двумерные подпространства $U \subset V$. Такие подпространства размерности 2 мы будем называть *проективными прямыми*. Проводя подпространства размерности 3, 4 и т.д., мы получаем возможность говорить о проективных подпространствах размерностей 2, 3 и т.д.

Таким образом, мы получили общую конструкцию проективного пространства размерности n. Как это часто бывает в математике, за общность мы платим наглядностью: текущая конструкция очень абстрактна и малопонятна. Давайте попробуем как-то ее увидеть.

В математике часто работает следующий принцип: *чтобы увидеть какой-то объект, необходимо задать его в координатах.* Иначе говоря, координаты — это некоторый паспорт объекта: мы можем посмотреть его и распознать, что это за объект. К сожалению, типичная проблема заключается в том, что координаты (как и паспорта) могут меняться (например, при смене системы координат), поэтому стоит помнить, что координаты не могут полностью заменить собой сам определяемый объект: они существуют лишь потому, что существует объект.

Тем не менее, вспомним, что когда мы работали с векторными пространствами, мы также вводили координаты для распознавания векторов. Для этого мы сначала выбирали некоторый базис, т.е. максимальный набор линейно независимых векторов, а затем выражали произвольный вектор через вектора базиса с помощью их линейных комбинаций. Поступим так и сейчас: зафиксируем базис $\{e_0, e_1, \dots, e_n\}$ в пространстве V (напомним, что векторов базиса должно быть $n+1$, поскольку количество векторов базиса совпадает с размерностью пространства) и рассмотрим произвольный ненулевой вектор v. Тогда существует единственный набор вещественных чисел $(x_0, x_1, \dots, x_n)$, такой, что $v = x_0 e_0 + x_1 e_1 + \dots + x_n e_n$. Числа $(x_0, x_1, \dots, x_n)$ называются *координатами вектора v в базисе* $\{e_0, e_1, \dots, e_n\}$. Таким образом, если мы зафиксировали базис $\{e_0, e_1, \dots, e_n\}$, то вместо вектора v, увидеть который невозможно, мы можем работать со строкой вещественных чисел $(x_0, x_1, \dots, x_n)$, являющихся его координатами, и это представление уже вполне конкретно.

Давайте попробуем перенести понятие координат вектора на проективные точки. Напомним, что проективная точка $\hat{v}$ представляет собой набор векторов λv, чьи координаты, как легко видеть, равны $(\lambda x_0, \lambda x_1, \dots, \lambda x_n)$. Иначе говоря, координаты любого вектора, лежащего на прямой $\hat{v}$, отличаются от координат вектора v умножением на ненулевую константу. Этот факт обозачают следующим образом: вместо набора чисел $(x_0, x_1, \dots, x_n)$ пишут набор $(x_0 : x_1 : \dots : x_n)$. Двоеточие подчеркивает, что координаты определены с точностью до умножения на ненулевую константу. Так определенные наборы чисел

будем называть *однородными координатами* проективной точки $\hat{v}$. Таким образом, проективные точки в n-перном проективном пространстве можно мыслить как наборы из $n+1$ вещественных чисел, определенные с точностью до пропорциональности.

Именно этот факт будет для нас ключевым при построении связи между классической проективной геометрией и конечными проективными плоскостями. Используя определенные выше конструкции, построим обе эти геометрии с точки зрения однородных координат.

Вновь начнем с классической проективной геометрии. Возьмем трехмерное векторное пространство V (в качестве такого пространства можно мыслить как раз обычное евклидово пространство $\mathbb{E}^3$, элементами которого являются векторы с началом в точке O) и зафиксируем в нем базис $\{e_0, e_1, e_2\}$. Тогда произвольный ненулевой вектор v в нем можно представить в виде линейной комбинации $v = x_0e_0 + x_1e_1 + x_2e_2$, а соответствующую вектору v проективную точку $\hat{v}$ — в виде однородных координат $(x_0 : x_1 : x_2)$. Таким образом, зафиксировав базис пространства V, мы можем работать с проективными точками как с наборами вещественных чисел, определенных с точностью до умножения на константу.

Теперь поймем, как увидеть проективную прямую. Мы помним, что по определению это в точности двумерная плоскость, проходящая через O. Такую плоскость можно задать уравнением $a_0x_0+a_1x_1+a_2x_2 = 0$, а это уравнение в свою очередь определяется тройкой чисел (a_0, a_1, a_2). Интересно отметить, что и эти числа определены с точностью до умножения на ненулевую константу, поэтому соответствующую проективную прямую тоже можно задать набором $(a_0 : a_1 : a_2)$.

Такое координатное представление дает возможность работать с проективными точками и прямыми на аналитическом языке. Например, из него следует так называемый *принцип двойственности*: если взять утверждение проективной геометрии, в котором содержатся условия на точки и прямые, а затем поменять слова «точка» и «прямая» местами, то мы также получим верное утверждение. Действительно, если взять проективную точку $(x_0 : x_1 : x_2)$ и проективную прямую $(a_0 : a_1 : a_2)$, то тот факт, что прямая проходит через точку, можно записать в виде равенства $a_0x_0 + a_1x_2 + a_2x_2 = 0$. Но такое же равенство означает, что точка $(a_0 : a_1 : a_2)$ лежит на прямой $(x_0 : x_1 : x_2)$, что и доказывает прицип двойственности.

Давайте подумаем, что можно изменить в нашей конструкции проективной плоскости. Понятно, что можно менять размерность. Но этого мы не хотим: трехмерная и двумерная геометрии как-то привычнее. Вспомним, что при определении векторного пространства V (которое как раз и порождает нам проективную плоскость) мы расматривали операцию умножения на константы. По умолчанию мы привыкли брать эти константы из поля вещественных чисел $\mathbb{R}$ — это удобно и хорошо согласуется с нашим алгебраическим опытом, в котором декартову плоскость мы обозначале через $\mathbb{R}^2$, имея в виду возможность задать любую точку на плоскости парой вещественных чисел. Но ведь можно вместо вещественных чисел ввести и другие. Главное, чтобы эти числа допускали бы четыре арифметические операции — $+$, $-$, $\times$ и $/$. Таким множества называются *полями*, и помимо уже знакомого нам поля вещественных чисел $\mathbb{R}$ нам известны также поле рациональных

чисел $\mathbb{Q}$, поле комплексных чисел $\mathbb{C}$ и поле остатков по простому модулю $\mathbb{Z}_p$.

Переход к векторным пространствам над комплексными числами по сути представляет собой далекое обобщение счета в комплексных из обычной геометрии. Добавляя большее количество измерений, мы соответсвенно увеличиваем сложность рассматриваемых геометрических объектов. Сегодня комплексная геометрия является активно развивающейся областью математики, со своими открытыми проблемами и важными научными результатами.

Использование вместо вещественных чисел рациональных ($\mathbb{Q}$) на практике встречается редко, поскольку рациональные числа в каком-то смысле слишком «никакие»: их достаточно мало, чтобы работать с алгеброй (например, почти никогда не удается извлечь квадратные корни), и достаточно много, чтобы представлять что-то комбинаторное (рациональных чисел даже на отрезке $[0;1]$ бесконечно много).

А вот замена поля $\mathbb{R}$ на поле $\mathbb{Z}_p$ является очень важной. Поговорим о ней подробнее. Поле $\mathbb{Z}_p$ в отличие от полей $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ *конечно*: в нем в точности p элементов. Это означает, что трехмерное векторное пространство V, определенное над этим полем, также будет конечным (обратите внимание: не просто конечной размерности, а конечным — в нем конечное количество векторов!). Сколько же векторов будет содержать пространство V? Чтобы понять это, нам снова поможет координатная запись. Зафиксируем базис пространства V (мы даже не будем никак его обозначать — он нам не пондобтся для каких-либо записей) и будем мыслить векторы как наборы из координат (x_0, x_1, x_2). Поскольку элементы x_0, x_1, x_2 лежат в $\mathbb{Z}_p$, каждый из них принимает ровно p значений. Значит, всего таких различных троек ровно p^3, и потому в пространстве V будет в точности p^3 векторов.

А теперь возьмем это пространство и построим его проективизацию PV. С точки зрения геометрии представить себе это очень сложно: ведь пространство V конечно, это просто россыпь отдельно лежащих векторов с общим началом. Но с точки зрения однородных координат здесь все понятно: каждая проективная точка — это набор $(x_0 : x_1 : x_2)$ остатков из $\mathbb{Z}_p$, не все из которых равны 0 и которые определены с точностью до умножения на ненулевой остаток из $\mathbb{Z}_p$. Давайте поймем, сколько таких наборов существует. Ненулевых наборов ровно $p^3 - 1$, причем из одного набора мы можем получить сразу $p - 1$ наборов с помощью умножения на ненулевые остатки из $\mathbb{Z}_p$. Значит, всего однородных наборов в точности $\dfrac{p^3 - 1}{p - 1} = p^2 + p + 1$. В точности столько же, сколько точек было на конечной проективной плоскости!

Таким образом, возникает вполне правдоподобная гипотеза:

> *если V — трехмерное векторное пространство над полем $\mathbb{Z}_p$, то проективное пространство PV является конечной проективной плоскостью порядка $p + 1$.*

Для доказательства этой гипотезы нам необходимо проверить аксиомы конечной проективной геометрии. Проверку аксиом 1 и 2 проще всего осуществить так. Забудем на время, что мы работаем над полем $\mathbb{Z}_p$, и будем толковать координаты x_0, x_1 и x_2 как обычные числа, не придавая им конкретных значений. Тогда мы по сути попадем в обычный ев-

клидов мир классической проективной геометрии, где соответствующие аксиомам 1 и 2 утверждения выполняются. Их выполнение является некоторым полиномиальным соотношением на координаты объектов (точек и прямых). Осуществив редукцию по модулю p этих полиномиальных соотношений, мы получим соответствующее выполнение их уже над полем $\mathbb{Z}_p$. Ну а аксиома 3 проверяется руками: достаточно взять точки $(1:0:0)$, $(0:1:0)$, $(0:0:1)$ и $(1:1:1)$.

Таким образом, мы доказали существование конечной проективной плоскости порядка $p+1$ для любого простого числа p. Осталось сделать еще один шаг: доказать существование конечной проективной плоскости порядка p^m+1 для любого натурального m. Что нам для этого нужно? По факту нам нужно найти поле $\mathbb{F}_q$, которое содержало бы в точности $q = p^m$ элементов. Тогда, заменив поле $\mathbb{Z}_p$ на поле $\mathbb{F}_q$ и повторив все предыдущие рассуждения, мы немедленно получим конструкцию конечной проективной плоскости порядка $q+1$.

Итак, все упирается в вопрос о том, какими бывают конечные поля. Как ни странно, этот вопрос относится к алгебре многочленов, и он весьма непрост. Путь к ответу на него мы разобьем на несколько задач.

1. **(a)** Пусть $\mathbb{F}$ — конечное поле из q элементов. Докажите, что существует такое простое число p, что $\underbrace{1+\ldots+1}_{p} = 0$. Число p называется *характеристикой* поля $\mathbb{F}$ и обозначается через $\operatorname{char}\mathbb{F}$.
(b) Рассмотрим поле $\mathbb{F}$ характеристики p как векторное пространство над полем $\mathbb{Z}_p$. Выведите отсюда, что $q = p^m$ для некоторого натурального числа m.

Из этой задачи следует, что конечное поле может содержать только $q = p^m$ элементов для некоторого простого p и натурального m. В частности, не существует полей из 6, 10 или 12 элементов. Поэтому с помощью данных конструкций невозможно построить, например, конечную проективную плоскость из $6^2+6+1 = 43$ точек. На самом деле ее просто не существует. Однако данная задача не доказывает существования полей из p^m элементов для любых пар (p, m). Доказать это — отдельное дело, и очень непростое. Опишем план доказательства.

Зафиксируем простое число p и натуральное число m. Рассмотрим кольцо многочленов $\mathbb{Z}_p[x]$. Предположим, что в этом кольце существует неприводимый многочлен f степени m. Тогда можно построить поле $\mathbb{F}_q$ из $q = p^m$ элементов следующим образом. Рассмотрим *фактор* $\mathbb{Z}_p[x]/(f)$. На самом деле это в точности кольцо остатков многочленов из $\mathbb{Z}_p[x]$ при делении на многочлен f. Напомним, что поскольку кольцо многочленов $\mathbb{Z}_p[x]$ строится над полем $\mathbb{Z}_p$, к его элементам применимы привычные нам факты из алгебры многочленов: деление с остатком и теорема Безу. В частности, многочлены степени d над $\mathbb{Z}_p$ имеют не более d корней, и если a — корень многочлена $g \in \mathbb{Z}_p[x]$, то $g(x) = (x-a)h(x)$ для некоторого многочлена $h \in \mathbb{Z}_p[x]$. Таким образом, множество $\mathbb{Z}_p[x]/(f)$ представляет собой совокупность остатков многочленов при делении на f.

Заметим, что все такие многочлены имеют вид $a_0 + a_1x + \ldots + a_{m-1}x^{m-1}$, где a_0, a_1, ..., $a_{m-1} \in \mathbb{Z}_p$. Получается, что мощность фактора $\mathbb{Z}_p[x]/(f)$ равна p^m. На самом деле этот

фактор и есть наше искомое поле. Для этого нам достаточно проверить, что многочлены из него можно складывать, вычитать, умножать и делить. С первыми тремя операциями проблем не возникает, а вот проверить наличие операции деления несколько труднее. Сделать это можно так.

Пусть $g \in \mathbb{Z}_p[x]/(f)$ — ненулевой многочлен. Мы хотим найти такой многочлен $h \in \mathbb{Z}_p[x]/(f)$, что $gh = 1$. Для этого рассмотрим многочлен g как многочлен из кольца $\mathbb{Z}_p[x]$ и по алгоритму Евклида найдем многочлены h и u, такие, что $gh + fu = 1$. Здесь важно отметить, что существование таких многочленов для *любого ненулевого* многочлена g следует как раз из неприводимости многочлена f: если f приводим, то взяв в качесте g его сомножитель, мы очевидно не сможем найти многочлены h и u, т.к. $(g, f) \neq 1$.

Таким образом, из неприводимости многочлена f и алгоритма Евклида следует существование обратного многочлена для любого ненулевого многочлена $g \in \mathbb{Z}_p[x]/(f)$. Это и означает, что фактор $\mathbb{Z}_p[x]/(f)$ является полем.

Пример. Построим поле $\mathbb{F}_4$ из 4 элементов. Для этого нам нужно взять кольцо многочленов $\mathbb{Z}_2[x]$ и найти в нем неприводимый многочлен f второй степени. Несложно проверить, что можно взять $f(x) = x^2 + x + 1$. Таким образом, поле $\mathbb{F}_4 = \mathbb{Z}_p[x]/(x^2 + x + 1)$ состоит из четырех элементов $\{0, 1, x, x + 1\}$ и имеет следующую таблицу умножения:

$\times$	1	x	$x+1$
1	1	x	$x+1$
x	x	$x+1$	1
$x+1$	$x+1$	1	x

2. Постройте поля $\mathbb{F}_8$ и $\mathbb{F}_9$ из 8 и 9 элементов, указав соответствующие неприводимые многочлены и таблицы умножения в этих полях.

3. Здесь и всюду далее, если не оговорено противное, мы полагаем $q = p^m$ и $f \in \mathbb{Z}_p[x]$ — неприводимый многочлен степени m.
(a) Пусть $\mathbb{F}$ — конечное поле характеристики p. Докажите, что $(a + b)^q = a^q + b^q$ для любых элементов $a, b \in \mathbb{F}$.
(b) Пусть $g \in \mathbb{Z}_p[x]$ — многочлен над полем $\mathbb{Z}_p$. Докажите, что $g(x)^q = g(x^q)$.
(c) Малая теорема Ферма для многочленов. Докажите, что для любого многочлена $g \in \mathbb{Z}_p[x]/(f)$ выполнено равенство $g^{q-1} = 1$.

4. **(a)** Докажите, что для любого многочлена $g \in \mathbb{Z}_p[x]$ многочлен $g(x)^q - g(x)$ делится на многочлен $x^q - x$.
(b) Докажите, что если для некоторого многочлена $g \in \mathbb{Z}_p[x]/(f)$ выполнено равенство $g^p = g$, то этот многочлен является константой.

5. Пусть $N_p(m)$ — множество приведенных неприводимых многочленов над $\mathbb{Z}_p$ степени m. Имеет место следующая формула:

$$x^q - x = \prod_{d|m} \prod_{g \in N_p(d)} g(x).$$

(a) Докажите, что многочлен $x^q - x$ делится на многочлен $g \in N_p(d)$ тогда и только

тогда, когда $m \vdots d$.

(b) Докажите, что многочлен $x^q - x$ не делится на многочлен $g^2(x)$, где $g \in N_p(d)$, ни для какого $d \mid m$.

6. Докажите, что если $M_p(m) := |N_p(m)|$, то справедливо равенство $q = \sum\limits_{d|m} d \cdot M_p(d)$.

7* Докажите, что $M_p(m) \geqslant 1$.

Мультипликативные функции в теории чисел

Мы продолжаем доказывать существование неприводимого над $\mathbb{Z}_p$ многочлена степени m для любого простого числа p и натурального числа m. Напомним, что ранее нами была выведена следующая формула:

> если $M_p(m)$ — количество приведенных неприводимых многочленов над $\mathbb{Z}_p$ степени m, то $\sum\limits_{d|m} d \cdot M_p(d) = p^m$.

Из этой формулы непосредственно следует явная формула для числа $M_p(m)$. В частности, отсюда также легко будет следовать, что $M_p(m) \geqslant 1$ для всех p и m. Однако вывести эту явную формулу без дополнительных соображений весьма непросто. Для этого нам потребуются знания о *мультипликативных функциях в теории чисел*, а говоря точнее, знания о *функции Мебиуса*.

Определение. Функция $f : \mathbb{N} \to \mathbb{C}$ называется *мультипликативной*, если для любых взаимно простых чисел a, b выполнено равенство $f(ab) = f(a)f(b)$ и $f \not\equiv 0$. Обычно рассматривают мультипликативные функции $f : \mathbb{N} \to \mathbb{Z}$.

Примеры мультипликативных функций. φ (функция Эйлера), τ (количество натуральных делителей), σ (сумма натуральных делителей), $\left(\frac{\cdot}{p}\right)$ (символ Лежандра), n^s (степенная функция).

Важнейшим примером мультипликативной функции является *функция Мебиуса*.

Определение. Пусть n — натуральное число и $k = \omega(n)$ — количество его простых делителей. Тогда функция Мебиуса от числа n определяется следующим обраом:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ не свободно от квадратов}, \\ (-1)^k, & \text{если } n \text{ свободно от квадратов}. \end{cases}$$

Именно функция Мебиуса будет играть центральную роль при выводе формулы для величины $M_p(m)$.

1. Докажите, что функция Мебиуса мультипликативна.
2. Пусть f — мультипликативная функция и $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ — разложение числа n на простые сомножители. Докажите, что
$$\sum_{d|n} f(d) = \prod_{i=1}^{k} \left(1 + f(p_i) + f(p_i^2) + \dots + f(p_i^{\alpha_i})\right).$$
3. Пусть f — мультипликативная функция и $F(n) = \sum\limits_{d|n} f(d)$. Докажите, что функция F также мультипликативна.

4. **(a)** Докажите, что если $n \geqslant 2$, то $\sum\limits_{d|n} \mu(d) = 0$.

(b) Пусть f — мультипликативная функция и $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ — разложение числа n на простые сомножители. Докажите, что

$$\sum_{d|n} \mu(d) f(d) = \prod_{i=1}^{k} \big(1 - f(p_i)\big).$$

(c) **Формула обращения Мебиуса для сумм.** Докажите, что если $F, f : \mathbb{N} \to \mathbb{Z}$ — такие функции, что $F(n) = \sum\limits_{d|n} f(n)$, то $f(n) = \sum\limits_{d|n} \mu(d) F(n/d)$.

(d) **Формула обращения Мебиуса для произведений.** Докажите, что если $F, f : \mathbb{N} \to \mathbb{Z}$ — такие функции, что $F(n) = \prod\limits_{d|n} f(n)$, то $f(n) = \sum\limits_{d|n} F(n/d)^{\mu(d)}$.

5. **(a)** Выведите с помощью формулы обращения Мебиуса явную формулу для чисел $M_p(m)$.

(b) Докажите, что $M_p(m) \geqslant 1$.

Формула обращения Мебиуса

Определение. Пусть n — натуральное число и $k = \omega(n)$ — количество его простых делителей. Тогда функция Мебиуса от числа n определяется следующим образом:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ не свободно от квадратов}, \\ (-1)^k, & \text{если } n \text{ свободно от квадратов}. \end{cases}$$

1. **(a)** Пусть $F_1, F_2 : \mathbb{N} \to \mathbb{Z}$ — арифметические функции. Докажите, что

$$\sum_{d|n} F_1(d) \cdot \sum_{d'|n/d} F_2(d') = \sum_{d,d' \,:\, dd'|n} F_1(d)F_2(d').$$

(b) **Формула обращения Мебиуса для сумм.** Докажите, что если $F, f : \mathbb{N} \to \mathbb{Z}$ — такие функции, что $F(n) = \sum\limits_{d|n} f(n)$, то $f(n) = \sum\limits_{d|n} \mu(d)F(n/d)$.

(c) **Формула обращения Мебиуса для произведений.** Докажите, что если $F, f : \mathbb{N} \to \mathbb{Z}$ — такие функции, что $F(n) = \prod\limits_{d|n} f(n)$, то $f(n) = \sum\limits_{d|n} F(n/d)^{\mu(d)}$.

2. **(a)** Выведите с помощью формулы обращения Мебиуса явную формулу для чисел $M_p(m)$.
(b) Докажите, что $M_p(m) \geqslant 1$.

3. Пусть $\varphi(n)$ — функция Эйлера.
(a) Докажите, что $\sum_{d|n} \varphi(d) = n$.
(b) Запишите, чему равна сумма $\sum_{d|n} \dfrac{\mu(d)}{d}$ через $\varphi(n)$.

4. Докажите, что если $F, f : \mathbb{N} \to \mathbb{Z}$ — такие функции, что $F(n) = \sum\limits_{k=1}^{n} f\Big(\big[n/k\big]\Big)$, то $f(n) = \sum\limits_{\ell=1}^{n} \mu(\ell)F\Big(\big[n/\ell\big]\Big)$.

Кубики

Определение. Многочлен $F(x, y)$ степени d задает на (комплексной) плоскости *алгебраическую кривую порядка* d (как множество решений уравнения $F(x, y) = 0$). Так, алгебраические кривые степени 1 — это прямые. Алгебраические кривые порядка 2 называют также соответственно *квадриками* или *кониками*. Алгебраические кривые порядка 3 называют *кубиками*.
Также алгебраические кривые рассматривают как множества точек на (комплексной) проективной плоскости; при этом уравнение $F(x, y) = 0$ степени d в однородных координатах $(x : y : z)$ переписывается в виде $P(x, y, z) = 0$, где $P(x, y, z) = z^d F(x/z, y/z)$ — однородный многочлен степени d, так что $F(x, y) = P(x, y, 1)$.

Теорема Безу. *Две алгебраические кривые порядка m и n, задаваемые взаимно-простыми многочленами, пересекаются ровно в mn точках (комплексной проективной плоскости) с учетом кратности.*
Формальное определение кратности непросто. Отметим только, что случай касания кривых в их общей точке соответствует тому, что эта точка — точка пересечения кратности не меньше 2.

Из теоремы Безу следует, что любая прямая пересекает невырожденную кубику в трех точках, любая коника — в шести точках (с учетом кратности), а две различные невырожденные кубики имеют ровно девять общих точек (с учетом кратности). Из теории СЛУ следует, что через 9 точек (проективной) плоскости можно провести хотя бы одну кубику. Причем эта кубика заведомо невырожденная, если данные 9 точек «достаточно общего» положения (скажем, если никакие 3 из данных точек не лежат на одной прямой и никакие 6 не лежат на одной конике).

Теорема Шаля. *Пусть даны две кубики, пересекающиеся в девяти точках. Тогда любая кубика, проходящая через восемь из них, проходит и через девятую.*
В отличие от девятки точек «общего положения», девятка точек из теоремы Шаля — особенная, и через нее проходит не единственная кубика: кубики, проходящие через такую особенную девятку, образуют пучок. Несложно понять, что в таком пучке найдутся невырожденные кубики. Отметим еще, что в особенной девятке точек из теоремы Шаля никакие 4 точки не лежат на одной прямой и никакие 7 из этих 9 точек не лежат на одной конике (иначе вся прямая или коника принадлежала бы каждой кубике, содержащей эту девятку точек).

Сложение точек. Наиболее важным фактом для нас в геометрии кубик является наличие на множестве точек невырожденной кубики операции сложения, превращающей кубику в нечто, аналогичное векторному пространству (точнее, кубика является $\mathbb{Z}$-модулем). Зафиксируем на кубике $\mathcal{C}$ произвольную точку O (аналог числа 0) и выберем на ней две произвольные точки A и B. Пусть X — третья точка пересечения прямой AB с $\mathcal{C}$, тогда точка $A + B$ — это третья точка пересечения прямой OX с $\mathcal{C}$). Эта операция удовлетворяет естественным свойствам операции сложения $A + B = B + A$; $(A + B) + C = A + (B + C)$;

$O + A = A$; если O — точка перегиба, то для любой точки A найдется точка $-A$, такая, что $(-A) + A = O$.

Удобно обозначать $nA = A + A + \ldots + A$ (n раз букв A) и $-nA = -A - A - \ldots - A$ (n раз букв A). Также полагаем $0 \cdot A = O$. Так, для любых целых m и k выполнены естественные свойства дистрибутивности $(m+k)A = mA + kA$ и $m(A+B) = mA + mB$. Отметим, что из равенства $nA = O$ не следует, что $A = O$. Точки A, такие, что $A \neq 0$, $2A \neq O$, ..., $(n-1)A \neq O$, но $nA = O$, называют *точками порядка n*. Ниже нам будут многократно встречаться точки порядка 2.

Часто бывает удобно выбирать за O *точку перегиба* кубики; в леммах о 3 точках на прямой и 6 точках на конике сделан именно такой выбор. *Точка перегиба* O — это точка, касательная к $\mathcal{C}$ в которой пересекает кубику $\mathcal{C}$ ровно в одной точке — самой точке O.

1. Пусть O и O' — две различные точки на кубике $\mathcal{C}$. Определим две операции сложения: «+» — относительно точки O и «$+'$» — относительно точки O'. Докажите, что $A +' B = A + B - O'$.

2. Докажите ассоциативность операции сложения, т.е. что $(A + B) + C = A + (B + C)$. (*Указание*: воспользуйтесь теоремой Шаля.)

3. **Точки порядка 2.** Пусть O — точка перегиба и $C \neq O$ — такая точка, что $2C = O$ (точка порядка 2).
   (a) Докажите, что прямая OC является касательной к кубике $\mathcal{C}$ в точке C.
   (b) Докажите, что на кубике $\mathcal{C}$ с фиксированной нулевой точкой O существует ровно три точки порядка 2.
   (c) Рассмотрим сдвиг $T_C : X \mapsto X' = X + C$. Докажите, что сдвиг T_C является инволюцией (т.е. $T_C \circ T_C = \mathrm{id}$ — тождественное преобразование), а касательные в точках X и X' к кубике $\mathcal{C}$ пересекаются на $\mathcal{C}$.

4. **Лемма о 3 точках на прямой.** Пусть на невырожденной кубике $\mathcal{C}$ точка O — это точка перегиба. Докажите, что точки X_1, X_2, X_3 лежат на одной прямой тогда и только тогда, когда $X_1 + X_2 + X_3 = O$.

5. Пусть точки X, Y, X', Y', $P = XY \cap X'Y'$ и $P' = XY' \cap X'Y$ лежат на невырожденной кубике $\mathcal{C}$. Докажите, что найдется точка C порядка 2, такая, что $X' = X + C$, $Y' = Y + C$ и $P' = P + C$.

6. **Лемма о 6 точках на конике.** Пусть на невырожденной кубике $\mathcal{C}$ точка O — это точка перегиба. Докажите, что точки $X_1, \ldots, X_6$ лежат на одной конике тогда и только тогда, когда $X_1 + \ldots + X_6 = O$. (*И вновь поможет теорема Шаля.*)

7. Зафиксируем точки A, B, C и D, лежащие на кубике $\mathcal{C}$. Каждой точке $X \in \mathcal{C}$ поставим в соответствие точку Y — шестую (с учетом кратности) точку пересечения коники, проходящей через A, B, C, D, X, с $\mathcal{C}$. Докажите, что прямые XY проходят через фиксированную точку.

Циркулярные кубики

Напомним, что мы работаем с *кубическими кривыми* (*кубиками*), которые задаются уравнением $\{F(x,y) = 0\}$ степени 3. В дальнейшем мы будем считать кубику заданной на комплексной проективной плоскости, т.е. рассматривать вместо многочлена $F(x,y)$ однородный многочлен $P(x,y,z) = z^3F(x/z, y/z)$. На невырожденных кубиках определена операция сложения точек, которая задается выбором нулевой точки O (являющейся точкой перегиба). Три точки X_1, X_2, X_3 кубики $\mathcal{C}$ лежат на одной прямой тогда и только тогда, когда $X_1 + X_2 + X_3 = O$, а шесть точек X_1, ..., X_6 кубики $\mathcal{C}$ лежат на одной конике тогда и только тогда, когда $X_1 + ... + X_6 = O$.

Пример 1. Зафиксируем точки P, C и D на кубике $\mathcal{C}$. Проведем через точку P всевозможные секущие, каждая из которых пересекает кубику $\mathcal{C}$ в точках X и Y. Проведем через точки C, D, X и Y всевозможных коники, и пусть они пересекают $\mathcal{C}$ еще в паре точек Z и T. Тогда прямые ZT проходят через фиксированную точку Q, лежащую на кубике $\mathcal{C}$.
Доказательство. Действительно, $P + X + Y = O$ и $C + D + X + Y + Z + T = O$, тогда $Z + T = P - C - D$, т.е. прямые ZT проходят через точку $C + D - P$.

Пример 2 (обобщенные радикальные оси). Если три коники проходят через две данные точки, то три прямые, соединяющие пары остальных общих точек каждых двух коник, пересекаются в одной точке.
Доказательство. Пусть C и D — общие точки трех коник, а A_{ij} и B_{ij} — оставшиеся две точки пересечения коник с номерами i и j. Через эти восемь точек проведем кубику. Так как точки $C, D, A_{12}, B_{12}, A_{13}$ и B_{13} лежат на одной конике, то их сумма равна O. Тогда сумма всех восьми рассматриваемых точек равна $A_{23} + B_{23}$. Аналогично, она равна $A_{12} + B_{12}$ и $A_{13} + B_{13}$. Из равенств $A_{12} + B_{12} = A_{13} + B_{13} = A_{23} + B_{23}$ следует, что прямые $A_{12}B_{12}$, $A_{13}B_{13}$ и $A_{23}B_{23}$ пересекают кубику в третий раз в одной и той же точке.

Определение. Точки $\iota^{\pm}$, имеющие однородные координаты $(1 : \pm i : 0)$, называются *круговыми*. Формально это бесконечно удаленные точки комплексной проективной плоскости $\mathbb{C}P^2$.
Заметим, что любая окружность проходит через круговые точки, поэтому любая кубика, состоящая из окружности и прямой, является циркулярной.
Пусть четыре точки A, B, C и D лежат на невырожденной циркулярной кубике и отличны от $\iota^{\pm}$. Из леммы о 6 точках на конике следует, что они лежат на одной окружности тогда и только тогда, когда $A + B + C + D + \iota^+ + \iota^- = O$.

Принцип. Если в конструкции участвуют только прямые, окружности и отношение инцидентности (принадлежности), то возможно, существует переформулировка или обобщение этой конструкции в терминах циркулярных кубик. Для этого полезно выбрать подходящие точки и провести через них и круговые точки $\iota^{\pm}$ цикрулярную кубику, после чего использовать лемму о трех точках на прямой и лемму о четырех точках на окружности, комбинируя равенства и получая из них различные следствия.

1. Пусть на циркулярной кубике $\mathcal{C}$ зафиксированы точки A и P. Через точку P проводят прямые, пересекающие кубику $\mathcal{C}$ в точках X и Y.
(a) Докажите, что окружности (AXY) проходят через одну точку A'.
(b) Пусть теперь на кубике выбраны еще точки B и Q. Аналогично, через Q проводят прямые, пересекающие кубику $\mathcal{C}$ в точках Z и T. Окружности (BZT) проходят через фиксированную точку B'. Докажите, что $A' = B'$ тогда и только тогда, когда прямые PB и QA пересекаются на кубике $\mathcal{C}$.

2. **(a) Антипараллельность относительно кубики.** Пусть P и Q — точки на циркулярной кубике $\mathcal{C}$. Через точку P проведем всевозможные секущие и получим пары точек пересечения X и Y. Через точку Q проведем всевозможные секущие и получаем пары точек пересечения Z и T. Докажите, что если точки X, Y, Z, T лежат на одной окружности для одного положения секущих, то это будет выполнено и для любого положения секущих.
(b) Антипараллельность относительно коники. Окружность пересекает конику в точках A, B, C и D. Прямая, параллельная CD, пересекает конику в точках X и Y. Докажите, что точки A, B, X и Y лежат на одной окружности.

3. **Сопряжение Клоуссона.** **(a)** В четырехугольнике $ABCD$ точки E и F таковы, что окружности (ABE), (CDE), (BCF) и (ADF) пересекаются в одной точке. Докажите, что окружности (ADE), (BCE), (ABF) и (CDF) также пересекаются в одной точке.
(b) В выпуклом четырехугольнике $ABCD$ лучи AB и DC пересекаются в точке P, а лучи AD и BC — в точке Q. Точки E и F внутри четырехугольника $ABCD$ таковы, что окружности (ABE), (CDE), (BCF), (ADF) пересекаются в одной точке K. Докажите, что окружности (PKF) и (QKE) вторично пересекаются на прямой PQ.

4. Пусть точки A', B' и C' лежат на прямых BC, CA и AB соответственно.
(a) Пусть $\mathcal{C}$ — любая циркулярная кубика, проходящая через точки A, B, C, A', B' и C'. Докажите, что кубика $\mathcal{C}$ содержит точку T пересечения окружностей $(AB'C')$, $(BC'A')$ и $(CA'B')$.
(b) Докажите, что прямые AA', BB' и CC' пересекаются в одной точке тогда и только тогда, когда окружности $(AA'T)$, $(BB'T)$ и $(CC'T)$ соосны (т.е. имеют, помимо T, еще одну общую точку, либо касаются в точке T).

5. В шестиугольнике $A_1A_2A_3A_4A_5A_6$ никакие четыре вершины не лежат на одной окружности, а диагонали A_1A_4, A_2A_5 и A_3A_6 пересекаются в одной точке X. Обозначим через ℓ_i радикальную ось окружностей $(A_iA_{i+1}A_{i-2})$ и $(A_iA_{i-1}A_{i+2})$ (мы считаем индексы по модулю 6). Докажите, что прямые ℓ_1, ..., ℓ_6 пересекаются в одной точке.

6. В треугольнике ABC проведены чевианы AA_1, BB_1 и CC_1, пересекающиеся в точке X. Окружности (BB_1A_1) и (CC_1A_1) вторично пересекаются в точке A_2, аналогично определены точки B_2 и C_2.
(a) Докажите, что окружности (BCA_2), (CAB_2) и (ABC_2) пересекаются в одной точке.
(b) Докажите, что окружности (XAA_2), (XBB_2) и (XCC_2) пересекаются в той же точке.
(c) Докажите, что прямые AA_2, BB_2 и CC_2 пересекаются в одной точке.

Сложение точек на вырожденной кубике

Ранее мы научились использовать сложение точек на циркулярных невырожденных кубиках, чтобы решать задачи из классической геометрии. Однако в некоторых ситуациях бывает полезно использовать в качестве циркулярной кубики *вырожденную кубику*, которая является объединением прямой и окружности. Для такой кубики нужно несколько иначе определить операцию сложения точек, поскольку, например, изначальное определение не работает в ситуации, когда две точки лежат на прямой.

Определение. Пусть $\mathcal{C}$ — вырожденная циркулярная кубика, состоящая из прямой ℓ и окружности ω. Выберем в качестве нулевой точки бесконечно удаленную точку O прямой ℓ и обозначим через h ось симметрии кубики $\mathcal{C}$, т.е. прямую, перпендикулярную прямой ℓ и проходящую через центр окружности ω. Определим сложение точек A и B кубики $\mathcal{C}$ следующим образом:

- если $A, B \in \omega$, то $A+B$ — это точка, симметричная точке $X_{AB} = AB \cap \ell$ относительно прямой h;
- если $A \in \omega$, $B \in \ell$ (или наоборот), то $A + B$ — это точка, симметричная точке $X_{AB} = AB \cap \omega$ относительно прямой h;
- если A, $B \in \ell$, то $A + B$ — это такая точка C, что $\deg_\omega C = CA \cdot CB$ (иными словами, точка C — это точка пересечения прямой ℓ и радикальной оси окружности ω и любой окружности, проходящей через точки A и B).

Так определенная операция сложения точек удовлетворяет всем естественным свойствам операции сложения: коммутативность, ассоциативность, наличие нулевого и обратного элементов. Самым трудным (как и в общем случае) является доказательство ассоциативности, и, в отличие от невырожденного случая, здесь используется частный случай теоремы Шаля, который называется *теоремой Паскаля*. Посмотрим, как это происходит, на примере следующего расположения точек.

Ассоциативность операции сложения. Пусть точки A, B и C лежат на окружности ω. Тогда $(A + B) + C = A + (B + C)$.
Доказательство. Обозначим через X_{PQ} третью точку пересечения прямой PQ с нашей вырожденной кубикой $\mathcal{C}$. Тогда достаточно доказать, что точка P пересечения прямых $X_{AB}C$ и $X_{BC}A$ лежит на окружности ω. Но это в точности теорема Паскаля, примененная к шестивершиннику $AA'B'C'CP$, где A', B' и C' — точки, симметричные точкам A, B и C относительно оси симметрии h.

Поскольку нулевая точка O в нашей кубике $\mathcal{C}$ является бесконечно удаленной, $\iota^+ + \iota^- + O = O$, поэтому лемма о четырех точках на окружности приобретает совсем простой вид:

> *точки A, B, C, $D \in \mathcal{C}$ лежат на одной окружности тогда и только тогда, когда $A + B + C + D = O$.*

1. **(a)** Докажите ассоциативность операции сложения для случая, когда A, $C \in \omega$ и $B \in \ell$.

(b) Докажите ассоциативность операции сложения для случая, когда $A \in \ell$, B, $C \in \omega$. (*Указание*: в этом случае теоремы Паскаля нет, достаточно описанных окружностей и уголков.)

2. Дан произвольный треугольник ABC, точка O — центр его описанной окружности, а точка L — его точка Лемуана.

(a) Докажите, что касательные к окружностям (AOL), (BOL), (COL) в точках A, B, C конкурентны.

(b) Обозначим через A_1 точку пересечения касательной к окружности (ABC) со стороной BC, а через A_2 — точку пересечения прямых $A_1B_1C_1$ и AL. Аналогично определим точки B_1, B_2 и C_1, C_2. Докажите, что окружности (AA_1A_2), (BB_1B_2), (CC_1C_2) и (ABC) пересекаются в одной точке.

Вокруг круговых многочленов – 1

При знакомстве с простейшими задачами теории чисел мы сразу же сталкиваемся с понятием *простого числа* (т.е. натурального числа, которое нельзя представить в виде произведения двух меньших натуральных чисел). В старших классах мы знакомимся с многочленами. Среди многочленов можно выделить многочлены, которые нельзя разложить в произведение многочленов меньшей степени. Такие многочлены называются *неприводимыми* и могут считаться аналогами простых чисел среди многочленов.

Однако при определении неприводимых многочленов большую роль играет вопрос о том, какими можно брать коэффициенты этих многочленов. Если разрешить коэффициентам быть произвольными комплексными числами, то описание неприводимых многочленов совсем просто — это в точности линейные многочлены (это не что иное как основная теорема алгебры). Если разрешить коэффициентам быть вещественными, то описание становится немного сложнее — это все линейные многочлены и квадратные трехчлены с отрицательным дискриминантом.

А как устроены неприводимые многочлены с целыми коэффициентами? Несмотря на простую формулировку вопроса, полный ответ на него вряд ли можно сформулировать (по крайней мере в достаточно простых терминах). Поэтому мы сосредоточим свое внимание на казалось бы совсем частном случае:

> *как устроено разложение многочлена $x^n - 1$ на неприводимые над $\mathbb{Z}$ множители?*

Вот примеры некоторых подобных разложений:

$$\begin{aligned} x^6 - 1 &= (x-1)\cdot(x+1)\cdot(x^2+x+1)\cdot(x^2-x+1),\\ x^{15} - 1 &= (x-1)\cdot(x^2+x+1)\cdot(x^4+x^3+x^2+x+1)\cdot\\ &\quad\cdot(x^8-x^7+x^6-x^5+x^4-x^3+x^2-x+1),\\ x^{25} - 1 &= (x-1)\cdot(x^4+x^3+x^2+x+1)\cdot(x^{20}+x^{15}+x^{10}+x^5+1). \end{aligned}$$

Оказывается, неприводимые многочлены, возникающие в этих разложениях, обладают большим количеством интересных свойств, делающих эти многочлены полезными в различных вопросах теории чисел. Таким многочлены называются *круговыми*, и именно о них пойдет речь в этом сюжете.

Напомним, что *корнем n-й степени из единицы* называется такое комплексное число ξ, что $\xi^n = 1$. Корней n-й степени из 1 существует ровно n штук, и равны они

$$\xi_k := \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n} = e^{\frac{2\pi i k}{n}}, \quad \text{где } k = 0, 1, \ldots, n-1.$$

Определение. *Круговым многочленом порядка n* называется многочлен

$$\Phi_n(x) = \prod_{(k,n)=1} (x - \xi_k),$$

где ξ_k — корни n-й степени из 1.

Именно эти, на первый взгляд, странные многочлены оказываются очень полезны при решении различных задач по теории чисел. Начнем с того, что докажем основные свойства круговых многочленов.

Утверждение 1. Имеет место равенство $\prod\limits_{d|n} \Phi_d(x) = x^n - 1$. В частности, $\Phi_n(x) \mid x^n - 1$ и $\sum\limits_{d|n} \varphi(d) = n$.

Доказательство. Заметим, что старшие коэффициенты многочленов слева и справа совпадают, поэтому достаточно доказать, что совпадают множества их корней. Пусть ξ — произвольный корень n-й степени из 1. Тогда рассмотрим наименьшее натуральное d, такое, что $\xi^d = 1$. Ясно, что $d \mid n$ (в противном случае остаток r числа n по модулю d был бы меньше d, и было бы выполнено равенство $\xi^r = 1$). Тогда ξ — корень многочлена $\Phi_d(x)$. Обратно, каждый корень ξ многочлена $\Phi_d(x)$ при $d \mid n$ является корнем степени n из 1, т.к. $\xi^n = (\xi^d)^{(n/d)} = 1$. Таким образом, множества корней многочленов слева и справа совпадают, а раз так, то совпадают и сами многочлены.
При $d = n$ получаем, что $\Phi_n(x) \mid x^n - 1$.
Заметим, что $\deg \Phi_d(x) = \varphi(d)$ для любого натурального d. Приравнивая степени многочленов слева и справа, получаем $\sum\limits_{d|n} \varphi(d) = n$.

Утверждение 2. Пусть p — произвольное простое число. Тогда

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p), & \text{если } p \mid n, \\ \dfrac{\Phi_n(x^p)}{\Phi_n(x)}, & \text{если } p \nmid n \end{cases} \qquad \text{и} \quad \Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}), & \text{если } p \mid n, \\ \dfrac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, & \text{если } p \nmid n. \end{cases}$$

Доказательство. Ясно, что второе равенство следует из первого, поэтому достаточно доказать лишь первое равенство. Пусть $p \mid n$. Заметим, что корни многочленов $\Phi_{pn}(x)$ и $\Phi_n(x^p)$ совпадают: если ξ — корень многочлена $\Phi_n(x^p)$, показатель которого равен T (т.е. наименьшее натуральное t, такое, что $\xi^t = 1$, равно T), то $T \mid np$ и $T \geqslant n$, поэтому $T = n$ или $T = np$. Но если $T = n$, то $\xi^n = (\xi^p)^{n/p} = 1$, поэтому показатель числа ξ^p меньше n, что невозможно. Значит, $T = np$, т.е. ξ является корнем многочлена $\Phi_{np}(x)$. Аналогично доказывается обратное включение. Т.к. эти многочлены являются приведенными, то и сами они также совпадают.
Пусть теперь $p \nmid n$. Докажем равенство $\Phi_n(x^p) = \Phi_{np}(x) \cdot \Phi_n(x)$. Опять пусть ξ — корень многочлена $\Phi_n(x^p)$, показатель которого равен T. Тогда $T \mid np$ и $T \geqslant n$, поэтому $T = n$ или $T = np$. Если $T = n$, то ξ является корнем многочлена $\Phi_n(x)$, а если $T = np$, то ξ является корнем многочлена $\Phi_{np}(x)$. Т.к. все многочлены являются приведенными, и множества корней левой и правой частей совпадают, отсюда следует требуемое.

1. **(a)** Докажите, что если p — простое, то $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$.
(b) Вычислите $\Phi_4(x)$, $\Phi_{2^k}(x)$.
(c) Вычислите $\Phi_{20}(x)$.

2. Докажите, что если $n \geqslant 3$ — нечетно, то $\Phi_{2n}(x) = \Phi_n(-x)$.

3. Докажите, что при $(n, k) = 1$ имеет место равенство $\Phi_n(x^k) = \prod\limits_{d|k} \Phi_{nd}(x)$.

4. Докажите, что все числа вида 100010001…00010001 являются составными.

5. Докажите, что $\Phi_n(x) \mid \dfrac{x^n - 1}{x^k - 1}$ при $k \mid n$ и $k \neq n$.

6. Пусть p — простой делитель числа $\Phi_n(a)$, где a — целое число. Тогда $n = p^\alpha q$, где $\alpha \geqslant 0$ и q — показатель числа a по модулю p. (*Указание*: это очень важное, но вместе с тем довольно трудное свойство круговых многочленов. В доказательстве вам может пригодиться лемма об уточнении показателя и предыдущая задача. Если не получается доказать этот факт, можно без доказательства использовать его при решении последующих задач; на следующем занятии мы докажем это утверждение вместе.)

7. Докажите, что если числа $\Phi_n(a)$ и $\Phi_m(a)$ не взаимно просты, то $\dfrac{m}{n}$ является степенью некоторого простого числа (возможно отрицательной).

8. Пусть a и n — целые числа и p — простой делитель $\Phi_n(a)$. Докажите, что либо $p \mid n$, либо $n \mid p - 1$.

Вокруг круговых многочленов – 2

Начнем с того, что докажем важное свойство круговых многочленов, сформулированное в прошлом листке в задаче под номером 6.

Утверждение. Пусть p — простой делитель числа $\Phi_n(a)$. Тогда $n = p^\alpha q$, где $\alpha \geqslant 0$ и q — показатель числа a по модулю p.

Доказательство. Пусть T — показатель числа a по модулю p и $n = p^\alpha q$, где $p \nmid q$. Сначала предположим, что $p = 2$. Докажем, что тогда $n = 2^\alpha$. В самом деле, если $2 \mid \Phi_n(a)$, то a нечетно, и если у n есть нечетный делитель d, то

$$2 \mid \Phi_n(a) \mid \frac{a^n - 1}{a^{n/d} - 1} = a^{(n/d)(d-1)} + a^{(n/d)(d-2)} + \ldots + 1$$

— нечетное число. Противоречие.

Теперь рассмотрим случай $p \geqslant 3$. Имеем $p \mid \Phi_{p^\alpha q}(a) \mid \Phi_q(a^{p^\alpha})$. Далее, по малой теореме Ферма $\Phi_q(a^{p^\alpha}) \equiv \Phi_q(a) \pmod p$. Тогда $p \mid \Phi_q(a)$, и

$$p \mid \Phi_q(a) \mid \frac{a^q - 1}{a^T - 1}.$$

Если $q \neq T$, то по LTE-лемме $\|a^q - 1\|_p - \|a^T - 1\|_p + \|q/T\|_p = 0$ — противоречие. Значит, $q = T$ — показатель числа a по модулю p.

Теперь посмотрим, как круговые многочлены помогают решать различные задачи. Ключевыми обычно являются следующие соображения:

- если в условии присутствует выражение вида $m^n - 1$, то нужно рассмотреть число $\Phi_n(m)$, являющееся его делителем, и простые числа, делящие $\Phi_n(m)$. Об этих простых числах у нас есть существенная информация, которую можно использовать. При этом часто бывает полезно воспользоваться алгоритмом Евклида для степеней: $(a^n - 1, a^m - 1) = a^{(n,m)} - 1$;
- Если в условии задачи что-то говорится про делители, то полезно разложить выражение из условия на множители. В этом помогает грамотная подстановка переменной в подходящий круговой многочлен.

Еще раз отметим наиболее важные их свойства:

- $\Phi_{p^k n}(x) = \begin{cases} \Phi_n(x^{p^k}), & \text{если } p \mid n, \\ \frac{\Phi_n(x^{p^k})}{\Phi_n(x^{p^{k-1}})}, & \text{если } p \nmid n, \end{cases}$, $\Phi_n(x^k) = \prod_{d \mid k} \Phi_{nd}(x)$ при $(n, k) = 1$,
- $\Phi_n(x) \;\Big|\; \frac{x^n - 1}{x^k - 1}$ при $k \mid n$ и $k \neq n$,
- если числа $\Phi_n(a)$ и $\Phi_m(a)$ не взаимно просты, то $\frac{m}{n}$ является степенью некоторого простого числа (возможно отрицательной),
- если p — простой делитель числа $\Phi_n(a)$, то либо $p \mid n$, либо $n \mid p - 1$.

1. Докажите, что для любого натурального n существует бесконечно много простых чисел p, таких, что $n \mid p-1$.

2. Решить уравнение $\dfrac{x^7-1}{x-1} = y^5 - 1$ в целых числах.

3. Пусть $p_1, \ldots, p_k$ — различные простые числа, большие 3, и $N = 2^{p_1 \cdots p_k} + 1$.

(a) Придумайте, как разложить это число на множители с помощью круговых многочленов.

(b) Используя одно из свойств круговых многочленов, докажите, что у числа N есть хотя бы $2^{2^{k-1}}$ делителей.

4. Существует бесконечно много натуральных n, таких, что все простые делители числа n^2+1 меньше $\sqrt{n}$.

(a) Будем искать $n = a^k$ для подходящих k. С помощью круговых многочленов разложите число n^2+1 на множители.

(b) Докажите, что для решения задачи достаточно найти бесконечно много таких k, что $\varphi(4d) < \dfrac{k}{2}$ при всех $d \mid k$.

(c) Будем искать $k = p_1 \ldots p_m$, где p_i — различные простые числа, не равные 3. Докажите, что при $d < k$ и $d \mid k$ выполнено неравенство $\varphi(4d) < \dfrac{k}{2}$.

(d) Докажите, что при $d = k$ и достаточно больших m выполнено неравенство $\varphi(4d) < \dfrac{k}{2}$ и таким образом решите исходную задачу.

5. Для каждого натурального k рассмотрим операцию f_k, определенную следующим образом:

$$f_k(n) = \Big[\sqrt[k]{\text{наибольший простой делитель числа } (n^{2024k}+1)}\Big].$$

Докажите, что с помощью нескольких таких операций каждое натуральное число можно привести к 1 (в качестве k можно взять любое натуральное число и менять его при необходимости).

6. **Задача на исследование.** Можно ли обобщить результаты, доказанные выше, на круговые многочлены, определенные над расширениями вида $\mathbb{Z}[\alpha]$? Например, на гауссовы целые числа? Какими свойствами обладают многочлены $\Phi_n(a+bi)$ и $(a-bi)^{\varphi(n)} \cdot \Phi\Big(\dfrac{a+bi}{a-bi}\Big)$? Можно ли использовать такие многочлены для исследования простых чисел в арифметических прогрессиях вида $-1+nd$ (или, более общо, вида $k+nd$)?

Теорема Зигмонди

Теорема, которую мы сейчас докажем, является, возможно, самой мощной теоремой в олимпиадной теории чисел, связанной со степенями натуральных чисел. Эта теорема позволяет решать задачи, казалось бы, невероятной сложности, практически сразу. Разумеется, за такую легкость придется заплатить. В данном случае платой будет чрезвычайная сложность доказательства, а также понимание того, что составители олимпиад знают об этой теореме, а потому стараются предлагать задачи, в которых эта теорема неприменима. Тем не менее, знать ее необходимо.

Теорема Зигмонди. *1. Пусть $a > b$ — натуральные числа. Тогда для любого натурального $n \geqslant 2$ число $a^n - b^n$ содержит в своем разложении на простые сомножители такое простое, которого нет в разложении чисел $a^k - b^k$ для всех $k < n$. Исключения составляют следующие два случая*: (1) $n = 2$, $a + b = 2^m$; (2) $n = 6$, $a = 2$, $b = 1$.
2. Пусть $a > b$ — натуральные числа. Тогда для любого натурального $n \geqslant 2$ число $a^n + b^n$ содержит в своем разложении на простые сомножители такое простое, которого нет в разложении чисел $a^k + b^k$ для всех $k < n$. Исключение составляет следующий случай: (3) $n = 3$, $a = 2$, $b = 1$.

Мы разобьем доказательство этой теоремы на несколько шагов. Прежде всего докажем теорему Зигмонди для случая $b = 1$. Назовем простое число p, делящее $a^n - 1$ и не делящее $a^k - 1$ при всех $k < n$, *примитивным*. Мы хотим доказать, что при всех a и n, за исключением случаев, указанных в теореме, у числа $\Phi_n(a)$ есть примитивный простой делитель (т.к. $\Phi_n(a) \mid a^n - 1$, этот же простой делитель будет и у числа $a^n - 1$). Основной идеей доказательства является оценка числа $\Phi_n(a)$ снизу через его простой делитель, не являющийся примитивным: мы докажем, что $\Phi_n(a) > p$ и $\|\Phi_n(a)\|_p = 1$, за исключением двух случаев, указанных в теореме.
Итак, предположим, что у числа $\Phi_n(a)$ нет примитивных простых делителей. Пусть $p \mid \Phi_n(a)$ — некоторый простой делитель. Тогда существует число $k \mid n$, такое, что $p \mid a^k - 1$.

1. Пусть $n = p^\alpha q$, где $p \nmid q$. Докажите, что $\alpha > 0$. Отсюда следует, что p — *наибольший простой делитель* числа n.

2. Докажите, что если $p = 2$, то $n = 2$ и $a + b$ — степень двойки.

3. Докажите, что если $p > 2$, то $\|\Phi_n(a)\|_p = 1$.

Из последней задачи следует, что для доказательства теоремы Зигмонди достаточно доказать, что $\Phi_n(a) > p$. В самом деле, $\Phi_n(a)$ не может быть кратно p^2, т.к. $\|\Phi_n(a, b)\|_p = 1$, поэтому у числа $\Phi_n(a)$ должен найтись еще один простой делитель. Он также обязан быть непримитивным, а значит, по задаче 6 он должен быть наибольшим простым делителем n, что невозможно.

4. Пусть $n = p^\alpha q$, где $p \nmid q$.
(a) Докажите, что $\Phi_n(a) > p$ при $\alpha > 1$.
(b) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a > 2$.
(c) Докажите, что $\Phi_n(a) > p$ при $\alpha = 1$ и $a = 2$, за исключением случая $n = 6$.

5. Докажите п.1 теоремы Зигмонди для произвольных a и b.

6. Докажите п.2 теоремы Зигмонди.

Теперь посмотрим, как теорема Зигмонди позволяет решать, казалось бы, очень трудные и громоздкие задачи.

7. Найти все решения уравнения

$$a^n - 1 = (a^p - 1)(a^q - 1)(a^r - 1)$$

в натуральных числах.

8. Найти все натуральные числа a, m, n, такие, что $a^m + 1 \mid (a+1)^n$.

9. Найти все такие натуральные числа x, p, n, r, такие, что p простое, $n, r > 1$ и $x^r - 1 = p^n$.

10. Найти все натуральные решения уравнения $p^x - y^p = 1$, где p — простое.

11. Решить уравнение $5^x - 3^y = z^2$ в натуральных числах.

12. Найти все натуральные решения уравнения $p^a - 1 = 2^n(p-1)$, где p — простое.

13. Решить уравнение $(a+1)(a^2+a+1)\ldots(a^n+a^{n-1}+\ldots+a+1) = a^m + a^{m-1} + \ldots + a + 1$ в натуральных числах.