Наш семинар: математические сюжеты

Мотивированное изложение комбинаторной теоремы о нулях

М. А. Ложкин, А. Б. Скопенков

О применениях линейной алгебры и многочленов в комбинаторике хорошо известно (см., например, [R1, R2, S]). Менее известные в школьном образовании применения *комбинаторной теоремы о нулях* (теорем Алона 7.b и 7′.b) описаны в [A, C, D, KS]. Мы покажем, как эта теорема постепенно и естественно возникает при решении «олимпиадных» задач. Простейшие идеи (утверждения 2, 2′, 4, 4′, 6 и 6′) естественно появляются при решении задач 1, 3 и 5, чем подводят читателя к обобщениям (теоремам 7 и 7′). Явная формулировка промежуточных частных случаев позволяет читателю проделать самостоятельно возможно большее количество этих постепенных обобщений.

Многие излагаемые здесь результаты близки к переднему краю науки. Однако эти результаты «олимпиадные»: для понимания формулировок и придумывания доказательств не требуется знаний, выходящих за пределы «кружковской» программы (или программы первого курса).

Заметка возникла из обсуждений семинаров по курсу «дискретный анализ» А. Райгородского на ФПМИ МФТИ, а также занятий кружка ЦПМ, проводимых М. Ложкиным. Благодарим А. Волостнова за предоставление его материалов по § 2, а также А. Волостнова, Д. Гринберга, Н. Ленскую и Ф. Петрова и анонимного рецензента за полезные обсуждения.

Подумайте самостоятельно над доказательством каждого утверждения! Доказательства приведены после формулировки или в конце заметки. *Если условие задачи является утверждением, то задача состоит в том, чтобы это утверждение доказать* (*тогда мы пишем «доказательство утверждения», а не «решение задачи»*).

§1. Приходим к комбинаторной теореме о нулях

Степенью одночлена $x_1^{d_1} \dots x_n^{d_n}$ называется число $d_1 + \dots + d_n$. *Степенью* $\deg f$ ненулевого многочлена f называется максимальная степень входящих в него одночленов. *Степенью* нулевого многочлена называется минус бесконечность.

Задача 1. Даны два многочлена по модулю 2 от n переменных, сумма степеней которых меньше n. Если они имеют общий корень, то они имеют хотя бы два общих корня.

Доказательство основано на следующем утверждении 2.

Через $\mathbb{Z}_p$ обозначается множество вычетов по модулю p. Напомним, что

$$A_1 \times \dots \times A_n := \{(a_1, \dots, a_n) \colon a_1 \in A_1, \dots, a_n \in A_n\}.$$

В утверждениях 2 и $2'$ суммирование и равенства рассматриваются по модулю 2.

Утверждение 2. *Дан многочлен f по модулю 2 от n переменных степени меньше n.*

(*a*) *Имеем* $\sum_{\alpha \in \mathbb{Z}_2^n} f(\alpha) = 0$.

(*b*) *Если f имеет корень, то он имеет хотя бы два корня.*

Назовём многочлен (с любыми коэффициентами) от нескольких переменных **неполным**, если в каждом его одночлене одна из переменных отсутствует.

Доказательство утверждения 2. (a) Так как $\deg f < n$, то f неполный. Если f не содержит x_1, то $f(0, \beta) = f(1, \beta)$ при любом $\beta \in \mathbb{Z}_2^{n-1}$, поэтому равенство из утверждения верно. Значит, оно верно для любого неполного многочлена f.

(b) Применим п. (a). Так как сумма чётного количества слагаемых равна нулю и одно из них равно нулю, то ещё одно равно нулю. □

Доказательство утверждения 1. Обозначим данные многочлены через f_1, f_2. Обозначим

$$g := f_1 f_2 + f_1 + f_2 = 1 + (1 + f_1)(1 + f_2).$$

Набор $\alpha \in \mathbb{Z}_2^n$ является корнем многочлена g тогда и только тогда, когда α является общим корнем многочленов f_1, f_2. Имеем

$$\deg g \leqslant \deg f_1 + \deg f_2 < n.$$

Значит, по утверждению 2.b многочлены f_1, f_2 имеют хотя бы два общих корня. □

Утверждение $2'$. *Дан многочлен f по модулю 2 от n переменных степени не более n.*

(*a*) *Коэффициент при $x_1 \cdots x_n$ равен $\sum_{\alpha \in \mathbb{Z}_2^n} f(\alpha)$.*

(*b*) *Если f зануляется в каждой точке, то его коэффициент при одночлене $x_1 \cdots x_n$ равен нулю.*

Доказательство. (a) Утверждение 2.a доказано для неполных многочленов (не обязательно имеющих степень менее n). Поэтому достаточно доказать утверждение $2'$.a для $f(x_1, \ldots, x_n) = kx_1 \cdots x_n$. Для него сумма из условия равна k.

(b) Следует из п. (a). □

Далее число p простое. В утверждениях 3, 4, $4'$, 6 и $6'$ суммирование и равенства рассматриваются по модулю p.

Задача 3 (теорема Шевалле). Даны многочлены по простому модулю p от n переменных, сумма степеней которых меньше n. Если они имеют общий корень, то они имеют хотя бы два общих корня.

Доказательство основано на следующем естественном обобщении утверждения 2. Из него вытекает более сильный факт: количество корней делится на p (теорема Варнинга).

Утверждение 4. *Дан многочлен f по модулю p от n переменных степени меньше $n(p-1)$.*

(*a*) *Имеем $\sum_{\alpha \in \mathbb{Z}_p^n} f(\alpha) = 0$.*

(*b*) *Если f не зануляется хотя бы в одной точке, то он не зануляется хотя бы в двух точках.*

Доказательство. (a) Ввиду линейности достаточно доказать утверждение для $f(x_1, \ldots, x_n) = x_1^{k_1} \cdots x_n^{k_n}$. В этом случае выражение в формуле можно разложить на множители:

$$\sum_{\alpha \in \mathbb{Z}_p^n} f(\alpha) = \sum_{\alpha_1 \in \mathbb{Z}_p} \alpha_1^{k_1} \cdot \ldots \cdot \sum_{\alpha_n \in \mathbb{Z}_p} \alpha_n^{k_n}.$$

Так как $k_1 + \ldots + k_n < n(p-1)$, то, не уменьшая общности, $k_1 < p-1$. Тогда[1)], беря первообразный корень g по модулю p, получаем:

$$\sum_{\alpha_1 \in \mathbb{Z}_p} \alpha_1^{k_1} = \sum_{0 \leqslant n < p-1} g^{nk_1} = \frac{g^{k_1(p-1)} - 1}{g^{k_1} - 1} = 0,$$

где

- первое равенство верно, поскольку g — первообразный корень;
- второе равенство верно, поскольку $g^{k_1} \neq 1$;
- последнее равенство верно, поскольку по малой теореме Ферма $g^{k_1(p-1)} = 1$.

(b) Применим п. (a). Так как сумма равна нулю и одно из слагаемых не равно нулю, то ещё одно не равно нулю. □

Доказательство утверждения 3. Обозначим данные многочлены через $f_1, f_2, \ldots, f_k$. Обозначим

$$g := \prod_{j=1}^{k} (f_j^{p-1} - 1).$$

Ввиду малой теоремы Ферма, $g(\alpha) \neq 0$ тогда и только тогда, когда α является общим корнем многочленов $f_1, \ldots, f_k$. Так как многочлены $f_1, \ldots, f_k$ имеют общий корень, то многочлен g не зануляется в некоторой точке. Имеем

$$\deg g = (p-1)\left(\deg f_1 + \deg f_2 + \ldots + \deg f_k\right) < n(p-1).$$

Значит, по утверждению 4.b многочлен g не зануляется хотя бы в двух точках. Поэтому у многочленов $f_1, \ldots, f_k$ есть хотя бы два общих корня. □

Утверждение 4′. *Дан многочлен f по модулю p от n переменных степени не более $n(p-1)$.*

(*a*) *Коэффициент при $x_1^{p-1} \cdots x_n^{p-1}$ равен $(-1)^n \sum_{\alpha \in \mathbb{Z}_p^n} f(\alpha)$.*

(*b*) *Если f зануляется в каждой точке, то его коэффициент при одночлене $x_1^{p-1} \cdots x_n^{p-1}$ равен нулю.*

Доказательство. (a) Утверждение 4.a доказано для одночленов, у которых степень вхождения хотя бы одной переменной меньше $p-1$ (но не обязательно имеющих степень менее $n(p-1)$). Поэтому достаточно доказать утверждение 4′.a для $f(x_1, \ldots, x_n) = kx_1^{p-1} \cdots x_n^{p-1}$. Для него по малой теореме Ферма сумма из условия есть $(-1)^n (p-1)^n k = k$.

(b) Следует из п. (a). □

[1)] Равенство $\sum_{\alpha_1 \in \mathbb{Z}_p} \alpha_1^{k_1} = 0$ следует также из леммы 8.b для $A = \mathbb{Z}_p$ и $m = k_1$.

Задача 5 (Всероссийская олимпиада 2007/11.5). В каждой вершине 100-угольника записаны два различных числа. Тогда из каждой вершины можно удалить одно число так, чтобы оставшиеся числа в любых двух соседних вершинах были различны.

Доказательство основано на следующем естественном обобщении вышеприведённых утверждений $4'$, в котором вместо значений многочлена на $\mathbb{Z}_2^n$ и $\mathbb{Z}_p^n$ рассматриваются значения многочлена на произведении $A_1 \times \ldots \times A_n \subset \mathbb{Z}_p^n$.

Замечание. У утверждений 5 и 10 имеется несложное прямое комбинаторное доказательство (см. доказательство утверждения 10 в решениях). Однако для большей части утверждений этого текста доказательство, не использующее комбинаторную теорему о нулях, неизвестно (или сложно).

Далее в этом тексте $\mathbb{F}$ есть $\mathbb{Z}_p$ или $\mathbb{R}$ (случай произвольного *поля* доказывается так же, но не применяется в комбинаторных задачах из § 2).

Утверждение 6. *Даны двухэлементные подмножества $A_1, \ldots, A_n$ множества $\mathbb{F}$ и многочлен f с коэффициентами в $\mathbb{F}$ от n переменных степени меньше n.*

(*a*) *Обозначим $\{a_{i0}, a_{i1}\} := A_i$. Тогда*

$$\sum_{\alpha \in \mathbb{Z}_2^n} (-1)^{\alpha(1)+\ldots+\alpha(n)} f(a_{1\alpha(1)}, \ldots, a_{n\alpha(n)}) = 0.$$

(*b*) *Если f не зануляется хотя бы в одной точке из $A_1 \times \ldots \times A_n$, то он не зануляется хотя бы в двух его точках.*

Доказательство. (a) Так как $\deg f < n$, то f неполный. Если f не содержит x_1, то

$$f(a_{10}, a_{2\alpha(2)}, \ldots, a_{n\alpha(n)}) = f(a_{11}, a_{2\alpha(2)}, \ldots, a_{n\alpha(n)})$$

для любых $\alpha(2), \ldots, \alpha(n) \in \mathbb{Z}_2$, поэтому нужное равенство верно. Тогда оно верно и для любого неполного многочлена f.

(b) Следует из п. (a). □

С помощью утверждения 6 доказываются утверждения 12.b и 13.

Утверждение $6'$. *Даны двухэлементные подмножества $A_1, \ldots, A_n$ множества $\mathbb{F}$ и многочлен f с коэффициентами в $\mathbb{F}$ от n переменных степени не более n.*

(*a*) *Обозначим* $\{a_{i0}, a_{i1}\} := A_i$. *Тогда коэффициент при одночлене* $x_1 \cdots x_n$ *равен*

$$\frac{\sum_{\alpha\in\mathbb{Z}_2^n}(-1)^{\alpha(1)+\ldots+\alpha(n)} f(a_{1\alpha(1)}, \ldots, a_{n\alpha(n)})}{\prod_{i=1}^n (a_{i,0} - a_{i,1})}.$$

(*b*) *Если* f *зануляется на* $A_1 \times \ldots \times A_n$, *то коэффициент при одночлене* $x_1 \cdots x_n$ *равен нулю.*

Доказательство. (a) Утверждение 6.a доказано для неполных многочленов (не обязательно имеющих степень менее n). Поэтому достаточно доказать утверждение 6′.a для $f(x_1, \ldots, x_n) = kx_1 \cdots x_n$. Имеем

$$\sum_{\alpha\in\mathbb{Z}_2^n}(-1)^{\alpha(1)+\ldots+\alpha(n)} a_{1\alpha(1)} \cdot \ldots \cdot a_{n\alpha(n)} = \prod_{i=1}^n (a_{i,0} - a_{i,1}).$$

Поэтому сумма из условия равна k.

(b) Следует из п. (a). □

Доказательство утверждения 5. Обозначим $n = 100$. Определим многочлен

$$f(x_1, \ldots, x_n) = \prod_{i=1}^n (x_i - x_{i+1}), \quad \text{где } x_{n+1} = x_1.$$

Имеем $\deg f = n$. Так как n чётно, то в многочлене f коэффициент при одночлене $x_1 \cdots x_n$ равен $2 \neq 0$. Применим утверждение 6′.b для множеств чисел, записанных в вершинах. Получим, что найдутся такие числа $a_1, \ldots, a_n$, записанные в вершинах, что $f(a_1, \ldots, a_n) \neq 0$. Это и есть искомые числа. □

Теорема 7 (Алон). *Даны конечные подмножества* $A_1, \ldots, A_n$ *множества* $\mathbb{F}$ *и многочлен* f *с коэффициентами в* $\mathbb{F}$ *от* n *переменных степени менее* $|A_1| + \ldots + |A_n| - n$.

(*a*) *Тогда существуют (не зависящие от* f*)* $P(\alpha) \in \mathbb{F}\backslash\{0\}$, *где* $\alpha \in \in A_1 \times \ldots \times A_n$, *для которых*

$$\sum_{\alpha\in A_1\times\ldots\times A_n} \frac{f(\alpha)}{P(\alpha)} = 0.$$

(*b*) *Если* f *не зануляется хотя бы в одной точке из* $A_1 \times \ldots \times A_n$, *то он не зануляется хотя бы в двух его точках.*

Пункт (b) следует из п. (a). Для доказательства теорем 7.a и 7′.a требуется лемма 8.b.

Теорема 7′ (Алон). *Даны конечные непустые подмножества $A_1, \ldots, A_n$ множества $\mathbb{F}$ и многочлен f с коэффициентами в $\mathbb{F}$ от n переменных степени не более $|A_1| + \ldots + |A_n| - n$.*

(*a*) *Тогда существуют (не зависящие от f) $P(\alpha) \in \mathbb{F}\setminus\{0\}$, где $\alpha \in A_1 \times \ldots \times A_n$, для которых коэффициент при одночлене $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$ равен*

$$\sum_{\alpha \in A_1 \times \ldots \times A_n} \frac{f(\alpha)}{P(\alpha)}.$$

(*b*) *Если f зануляется на $A_1 \times \ldots \times A_n$, то коэффициент при одночлене $x_1^{|A_1|-1} \cdots x_n^{|A_n|-1}$ равен нулю.*

Далее $A \subset \mathbb{F}$ — любое конечное подмножество. Для $a \in A$ обозначим

$$Aa = \prod_{b \in A,\, b \neq a} (a - b).$$

Лемма 8. (*a*) (*Интерполяционная формула Лагранжа*) *Для любых подмножества $A \subset \mathbb{F}$ и многочлена f с коэффициентами в $\mathbb{F}$ от одной переменной степени менее $|A|$ имеем*

$$f(x) = \sum_{a \in A} \frac{f(a) \prod_{b \in A,\, b \neq a} (x - b)}{Aa}.$$

(*b*) *Для любого подмножества $A \subset \mathbb{F}$ имеем*

$$\sum_{a \in A} \frac{a^m}{Aa} = \begin{cases} 0, & m < |A| - 1; \\ 1, & m = |A| - 1. \end{cases}$$

Доказательство. (a) В обеих частях равенства написаны многочлены степени менее $|A|$. Они совпадают во всех точках множества A, следовательно, они равны. (Заметим, что $|A| < p + 1$ при $\mathbb{F} = \mathbb{Z}_p$.)

(b) Подставим в п. (a) многочлен $f(x) = x^m$ при $m < |A|$:

$$x^m = \sum_{a \in A} \frac{a^m \prod_{b \in A \setminus \{a\}} (x - b)}{Aa}.$$

Приравняв коэффициенты обеих частей при $x^{|A|-1}$, получаем требуемое равенство. □

Доказательство теорем 7.a и 7′.a. Положим $P(\alpha) := A_1\alpha_1 \cdot \ldots \cdot A_n\alpha_n$. Ввиду линейности достаточно доказать каждую из теорем для

$$f(x_1, \ldots, x_n) = x_1^{k_1} \cdots x_n^{k_n}.$$

В этом случае выражение в формуле можно разложить на множители:

$$\sum_{\alpha_1\in A_1}\cdots\sum_{\alpha_n\in A_n}\frac{\alpha_1^{k_1}\cdots\alpha_n^{k_n}}{P(\alpha)}=\sum_{\alpha_1\in A_1}\frac{\alpha_1^{k_1}}{A_1\alpha_1}\cdot\ldots\cdot\sum_{\alpha_n\in A_n}\frac{\alpha_n^{k_n}}{A_n\alpha_n}.$$

Используем формулу 8.b. Если $k_i<|A_i|-1$ для некоторого i, то один из множителей равен нулю. Иначе $k_i=|A_i|-1$ для любого i, тогда каждый из множителей равен 1. □

Замечания. (a) Приведённое доказательство теорем Алона 7 и $7'$ отлично от имеющегося в [A, C, D].

(b) Теоремы Алона являются естественным обобщением интерполяционной формулы Лагранжа 8.a. В [KP] это подмечено, и теорема Алона $7'$.a применена к вычислению коэффициентов некоторого многочлена. В [P] обобщается следующее «качественное следствие» интерполяционной формулы Лагранжа 8.a: *многочлен степени n от одной переменной задаётся своими значениями в $n+1$ точке* (ср. теорему $7'$.b); обобщение применяется к комбинаторным *тождествам*.

(c) Многочлен f от переменных $x_1,\ldots,x_n$ назовём $(d_1,\ldots,d_n)$-*многочленом*, если среди его одночленов $x_1^{k_1}\cdots x_n^{k_n}$, отличных от $x_1^{d_1}\cdots x_n^{d_n}$, нет таких, что $k_i\geqslant d_i$ для всех $i\in\{1,\ldots,n\}$. В теоремах Алона 7 и $7'$ обозначим $d_i=|A_i|-1$ для $i=1,\ldots,n$. Тогда условия на степень многочлена можно ослабить соответственно до следующих:

- f является $(d_1,\ldots,d_n)$-многочленом и коэффициент при $x_1^{d_1}\cdots x_n^{d_n}$ равен нулю;
- f является $(d_1,\ldots,d_n)$-многочленом.

(d) Утверждение 8.b можно доказать напрямую, используя разложение по строке определителя Вандермонда (см. определение в решении задачи 14.b).

§ 2. Применяем комбинаторную теорему о нулях

Здесь мы приводим комбинаторные применения. Об алгебраических обобщениях теорем Алона, Шевалле и Варнинга (теоремы 7, $7'$ и утверждение 3) в разных направлениях см., например, [BS, C14, CGS].

Задача 9 (теорема Эрдёша — Гинзбурга — Зива). Для всякого простого p любой набор из $2p-1$ целых чисел содержит p чисел, сумма которых делится на p.

Этот забавный факт вытекает из следующего общего результата (хотя может быть доказан и независимо).

Задача 10 (теорема Коши — Давенпорта). Пусть p простое, и пусть $A, B \subset \mathbb{Z}_p$ непусты. Обозначим $A+B = \{a+b\colon a \in A,\ b \in B\}$. Тогда

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

Указание. Обозначим

$$f(x,y) = \prod_{c \in A+B} (x+y-c).$$

Тогда $f(x,y) = 0$ при всех $x \in A$, $y \in B$.

Задача 11. Пусть p простое и $A, B \subset \mathbb{Z}_p$ непусты. Обозначим

$$A \dot{+} B = \{a+b\colon a \in A,\ b \in B,\ a \neq b\}.$$

(a) (Гипотеза Эрдёша — Хайльбронна.) Имеем

$$|A \dot{+} A| \geqslant \min(2|A|-3, p).$$

(b) Если $A \neq B$, то $|A \dot{+} B| \geqslant \min(|A|+|B|-2, p)$.

Указание. Пункт (a) сводится к п. (b). Пункт (b) сводится к случаю $|A| \neq |B|$, который доказывается при помощи теоремы $7'$.b.

Задача 12. (a) (Международная олимпиада 2007.) Найдите наименьшее целое k, такое что в пространстве $\mathbb{R}^3$ имеется k плоскостей, объединение которых не содержит точку $(0,0,0)$, но содержит все остальные точки $(a,b,c) \in \mathbb{Z}^3$, такие что $0 \leqslant a, b, c \leqslant n$.

(b) (Теорема Олсона.) Пусть p простое. Найдите наименьшее целое m, для которого среди любых m векторов из $\mathbb{Z}_p^k$ (не обязательно различных) найдутся несколько векторов с нулевой суммой.

Задача 13. Пусть p простое, степень каждой вершины графа меньше $2p$, а средняя степень больше $2p-2$. Тогда имеется непустой подграф, степень каждой вершины которого равна p.

Задача 14. Пусть k и n — целые положительные числа.

(a) Если $2k \leqslant n+1$, то для любых $a_1, \ldots, a_k \in \mathbb{Z}_n$ (не обязательно различных) существует перестановка σ множества $\{1, \ldots, k\}$ такая, что вычеты $a_1+\sigma(1), \ldots, a_k+\sigma(k) \in \mathbb{Z}_n$ попарно различны.

(b) Найдите коэффициент при одночлене $x_1^{k-1} \cdots x_k^{k-1}$ многочлена

$$\prod_{1 \leqslant i < j \leqslant n} (x_j - x_i)^2.$$

(c) (Гипотеза Сневиля, доказанная Алоном.) Пусть p — нечётное простое число, $k < p$ и вычеты $b_1, \ldots, b_k \in \mathbb{Z}_p$ попарно различны. Тогда для любых $a_1, \ldots, a_k \in \mathbb{Z}_p$ (не обязательно различных) найдётся перестановка σ множества $\{1, \ldots, k\}$ такая, что вычеты $a_1+b_{\sigma(1)}, \ldots, a_k+b_{\sigma(k)} \in \mathbb{Z}_p$ попарно различны.

Здесь п. (b) — подсказка к п. (a), а п. (c) — обобщение п. (a) для нечётного простого n.

Задача 15. Каждое из данных 2^n+1 конечных множеств покрашено в один из двух цветов. Оба цвета имеются. Тогда найдётся не менее 2^n попарно различных множеств (не обязательно из данных), каждое из которых является симметрической разностью двух множеств разных цветов. (Напомним, что *симметрическая разность* двух множеств есть множество всех элементов, принадлежащих ровно одному из них.)

Решения задач

В решениях задач 9, 10, 11, 12.*b*, 13 *равенства являются равенствами вычетов по модулю p или многочленов с коэффициентами в $\mathbb{Z}_p$.*

9. Если среди данных $2p-1$ чисел найдутся p чисел, дающих одинаковые остатки от деления на p, то возьмём их. Иначе упорядочим остатки $x_1 \geqslant x_2 \geqslant \ldots \geqslant x_{2p-1}$ от деления данных чисел на p. Обозначим $M_p = \{x_p\}$ и $M_i = \{x_i, x_{p+i}\}$ для $i = 1, \ldots, p-1$. Индукцией по n с помощью теоремы Коши — Давенпорта 10 нетрудно получить, что

$$|A_1 + \ldots + A_n| \geqslant \min(|A_1| + \ldots + |A_n| - n + 1, p)$$

для любых непустых подмножеств $A_1, \ldots, A_n \subset \mathbb{Z}_p$. Поэтому

$$|M_1 + \ldots + M_p| = p.$$

Значит, $0 \in M_1 + \ldots + M_p$.

10. *Набросок доказательства, не использующего теоремы* $7'$. Можно считать, что $|A| \leqslant |B|$. Проведём индукцию по $|A|$. База $|A| = 1$ очевидна.

Переход. Пусть $|A| > 1$. Если $B = \mathbb{Z}_p$, то теорема очевидна. Иначе, ввиду простоты числа p, существует такое $x \in \mathbb{Z}_p$, что для $A' := A + x$ выполнено $A' \cap B \neq \varnothing$ и $A' \not\subset B$. Тогда по индукции можно перейти к паре множеств $(A' \cap B, A' \cup B)$.

10. Обозначим $a := |A|$, $b := |B|$, $C := A + B$.

Пусть сначала $a + b - 1 > p$. Тогда существуют непустые подмножества $A' \subset A$ и $B' \subset B$, для которых $|A'| + |B'| = p + 1$. Поскольку $A' + B' \subset C$ и $\min(a + b - 1, p) = p = \min(|A'| + |B'| - 1, p)$, то утверждение сведено к случаю $a + b - 1 = p$.

Пусть теперь[2] $a + b - 1 \leqslant p$. Пусть, напротив, $|C| \leqslant a + b - 2$.

[2] Аналогично предыдущему абзацу утверждение сводится к частному случаю $a + b - 1 = p$. Вместо этого мы включаем в нижеприведённую формулу множитель $(x + y)^{a+b-2-|C|}$.

Положим

$$f(x,y)=(x+y)^{a+b-2-|C|}\prod_{c\in C}(x+y-c).$$

Ясно, что $f(x,y)=0$ при всех $x\in A$, $y\in B$. Тогда по теореме 7′.b коэффициент при $x^{a-1}y^{b-1}$ равен нулю. Но он равен $\binom{a+b-2}{a-1}$. Так как $a+b-2\leqslant p-1$, то он не делится на p. Противоречие.

11. (a) Возьмём произвольный элемент $a\in A$. Тогда получаем $A\dot{+}A=A\backslash\{a\}\dot{+}A$, и мы свели задачу к п. (b).

(b) Обозначим $a:=|A|$, $b:=|B|$, $C:=A\dot{+}B$. Если $a+b-2>p$, то аналогично доказательству теоремы Коши — Давенпорта 10 удалим из множеств A или B какие-нибудь элементы и сведём утверждение к случаю $a+b-2=p$.

Пусть теперь $a+b-2\leqslant p$. Пусть, напротив, $|C|\leqslant a+b-3$. Положим

$$f(x,y)=(x-y)(x+y)^{a+b-3-|C|}\prod_{c\in C}(x+y-c).$$

Ясно, что $f(x,y)=0$ при всех $x\in A$, $y\in B$. Тогда по теореме 7′.b коэффициент при $x^{a-1}y^{b-1}$ равен нулю. Но он равен $\binom{a+b-3}{a-2}-\binom{a+b-3}{a-1}$.

Так как $a+b-3\leqslant p-1$, то при $a\neq b$ эта разность не делится на p. Противоречие. (Этого достаточно для п. (a).)

Пусть теперь $a=b$. Если $A\cap B=\varnothing$, то применим теорему Коши — Давенпорта 10. Иначе перейдём ко множествам $(A',B')=(A\cap B,\ A\cup B)$. Нетрудно видеть, что

$$A'+B'\subset A+B,\quad |A'|+|B'|-2=|A|+|B|-2\quad\text{и}\quad |A'|<|B'|.$$

Таким образом, утверждение сведено к случаю $a\neq b$.

12. (a) Ответ: $3n$.

В качестве примера возьмём

- n плоскостей $x=a$, $1\leqslant a\leqslant n$;
- n плоскостей $y=b$, $1\leqslant b\leqslant n$;
- n плоскостей $z=c$, $1\leqslant c\leqslant n$.

Пусть теперь $k<3n$ и множество $\{0,1,\dots,n\}^3-\{(0,0,0)\}$ покрыто k плоскостями с уравнениями $a_ix+b_iy+c_iz+d_i=0$. Обозначим

$$f(x,y,z)=\prod_{i=1}^{k}(a_ix+b_iy+c_iz+d_i).$$

Тогда $\deg f=k<3n$. Этот многочлен равен нулю во всех точках множества $\{0,1,\dots,n\}^3$, кроме, быть может, точки $(0,0,0)$. Тогда по тео-

реме 7.b он равен нулю и в точке $(0,0,0)$. Значит, некоторая плоскость содержит точку $(0,0,0)$.

(b) Ответ: $k(p-1)+1$.

Ясно, что $m>k(p-1)$, поскольку можно выбрать базисные векторы e_1, e_2, …, e_k по $p-1$ раз.

Рассмотрим произвольные $m=k(p-1)+1$ векторов $v_1,\dots,v_m\in\mathbb{Z}_p^k$. Покажем, что можно выбрать несколько из них с нулевой суммой. Сумма нескольких из этих векторов равна $\varepsilon_1v_1+\ldots+\varepsilon_mv_m$ для некоторых $\varepsilon_1,\dots,\varepsilon_m\in\{0,1\}$. Обозначим j-ю координату вектора v_i через v_{ij} для $i\in\{1,\dots,m\}$, $j\in\{1,\dots,k\}$. Если $\varepsilon_1v_1+\ldots+\varepsilon_mv_m\neq 0$, то существует такое $j\in\{1,\dots,m\}$, что $\varepsilon_1v_{1j}+\ldots+\varepsilon_mv_{mj}\neq 0$. В пространстве $\mathbb{Z}_p^k$ с координатами $\varepsilon_1,\dots,\varepsilon_m$ рассмотрим $m-1=k(p-1)$ гиперплоскостей, заданных уравнениями

$$\varepsilon_1v_{1j}+\ldots+\varepsilon_mv_{mj}=\lambda,\quad\text{где}\quad i\in\{1,\dots,k\}\quad\text{и}\quad\lambda\in\mathbb{Z}_p\setminus\{0\}.$$

Аналогично версии п. (a) по модулю p эти гиперплоскости не могут покрывать все точки куба $\{0,1\}^m$, кроме точки $(0,\dots,0)$. Значит, существует точка $(\varepsilon_1,\dots,\varepsilon_m)\in\{0,1\}^m$, не лежащая ни в одной из построенных $k(p-1)$ гиперплоскостей. Тогда $\varepsilon_1v_1+\ldots+\varepsilon_mv_m=0$.

13. Обозначим через V и E множества вершин и рёбер данного графа. Для каждого ребра $e\in E$ введём переменную x_e. Определим многочлен с коэффициентами в $\mathbb{Z}_p$ формулой

$$f(x)=\prod_{v\in V}\left(\left(\sum_{e\in E\colon v\in e}x_e\right)^{p-1}-1\right).$$

Имеем $f(0,\dots,0)\neq 0$. Кроме того, $\deg f\leqslant|V|(p-1)<|E|$ (если граф имеет изолированную вершину, то в определении многочлена f суммирование ведётся по пустому множеству, поэтому степень многочлена f не равна $|V|(p-1)$). Значит, по теореме 7.b многочлен принимает ненулевое значение ещё хотя бы в одной точке $z\in\{0,1\}^{|E|}$. Удалим из графа все те рёбра e, для которых $z_e=1$. Если появились изолированные вершины, то удалим их. Получим искомый подграф.

14. (a) Для $x_i,x_j\in\{1,\dots,k\}$ имеем

$$|x_i-x_j|\leqslant k-1\leqslant\frac{n-1}{2}<\frac{n}{2}$$

и

$$x_i+a_i\not\equiv x_j+a_j\pmod n\quad\Leftrightarrow\quad x_j-x_i\not\equiv a_i-a_j\pmod n\quad\Leftrightarrow\quad x_j-x_i\neq r_{ij},$$

где r_{ij} обозначает число, сравнимое с $a_i - a_j$ по модулю n, из интервала $(-n/2, n/2]$. Таким образом, достаточно показать, что существуют различные $x_1, \dots, x_k \in \{1, \dots, k\}$ такие, что $x_j - x_i \neq r_{ij}$ для любых $1 \leqslant i < j \leqslant k$. Ввиду теоремы 7′.b достаточно показать, что коэффициент при мономе $x_1^{k-1} \cdots x_k^{k-1}$ многочлена

$$\prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)(x_j - x_i - r_{ij})$$

не равен нулю. Так как этот коэффициент совпадает с коэффициентом при том же мономе многочлена

$$\prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2,$$

то нужное вытекает из ответа на п. (b).

(b) Ответ: $k!(-1)^{\binom{k}{2}}$.

Для доказательства воспользуемся формулой (для определителя Вандермонда)

$$\prod_{1 \leqslant i < j \leqslant k} (x_j - x_i) = \sum_{\sigma} \operatorname{sgn} \sigma \cdot x_{\sigma(1)}^0 \cdots x_{\sigma(k)}^{k-1},$$

где σ пробегает все перестановки множества $\{1, \dots, k\}$, а $\operatorname{sgn} \sigma$ — знак перестановки. Тогда

$$\prod_{1 \leqslant i < j \leqslant k} (x_j - x_i)^2 = \left(\sum_{\sigma} \operatorname{sgn} \sigma \cdot x_{\sigma(1)}^0 \cdots x_{\sigma(k)}^{k-1} \right) \cdot \left(\sum_{\pi} \operatorname{sgn} \pi \cdot x_{\pi(1)}^0 \cdots x_{\pi(k)}^{k-1} \right).$$

При раскрытии скобок моном $x_1^{k-1} \cdots x_k^{k-1}$ присутствует только в произведении слагаемых, соответствующих всем тем перестановкам σ и π, для которых $\pi = \sigma\alpha$, где $\alpha(j) = k + 1 - j$ при любом j. Для таких перестановок $\operatorname{sgn} \sigma \cdot \operatorname{sgn} \pi = \operatorname{sgn} \alpha = (-1)^{\binom{k}{2}}$. Поэтому искомый коэффициент равен $k!(-1)^{\binom{k}{2}}$.

Список литературы

[A] *Alon N.* Combinatorial Nullstellensatz // Combin. Probab. Comput. 1999. Vol. 8, № 1–2. P. 7–29. https://www.cs.tau.ac.il/~nogaa/PDFS/null2.pdf.

[BS] *Bishnoi A., Clark P. L.* Restricted variable Chevalley — Warning theorems. http://alpha.math.uga.edu/~pete/Bishnoi-Clark22.pdf.

[C] *Chen E.* Combinatorial Nullstellensatz, 2013. https://web.evanchen.cc/handouts/BMC_Combo_Null/BMC_Combo_Null.pdf.

[C14] *Clark P. L.* The Combinatorial Nullstellensätze Revisited // The Electr. J. of Comb. 2014. Vol. 21, №. 4. Paper 4.15, 17. https://www.combinatorics.org/ojs/index.php/eljc/article/view/v21i4p15.

[CGS] *Clark P. L.*, *Genao T.*, *Saia F.* Chevalley — Warning at the Boundary, Expositiones Math., to appear. http://alpha.math.uga.edu/~pete/Chevalley_Warning_on_the_Boundary.pdf.

[D] *Димитров В.* Combinatorial Nullstellensatz // Петербургские олимпиады школьников по математике 2003–2005. СПб.: Невский Диалект; БХВ-Петербург, 2007. С. 416–425.

[KP] *Карасёв Р. Н.*, *Петров Ф. В.* Ещё раз о комбинаторной теореме о нулях // Задачи Санкт-Петербургской олимпиады по математике 2010 года. СПб.: Невский Диалект; БХВ-Петербург, 2007. С. 116–120.

[KS] *Kezdy A.*, *Snevily H.* Distinct Sums Modulo n and Tree Embeddings // Combin. Probab. Comput. 2002. Vol. 11, № 1. P. 35–42. https://www.math.ucdavis.edu/~deloera/MISC/LA-BIBLIO/trunk/Kezdy/kezdy.pdf.

[P] *Петров Ф. В.* Восстановление многочлена по его значениям // Задачи Санкт-Петербургской олимпиады школьников по математике 2015 года. М.: МЦНМО, 2015. С. 98–106.

[R1] *Райгородский А. М.* Проблема Борсука. М.: МЦНМО, 2015.

[R2] *Райгородский А. М.* Линейно-алгебраический метод в комбинаторике. М.: МЦНМО, 2015.

[S] *Скопенков А.* Короткое опровержение гипотезы Борсука // Математическое просвещение. Сер. 3. Вып. 17. М.: МЦНМО, 2013. С. 88–92. http://arxiv.org/abs/0712.4009.

Михаил Алексеевич Ложкин, НИУ ВШЭ
lozhkin.mixail@gmail.com

Аркадий Борисович Скопенков, МФТИ, НМУ
https://users.mccme.ru/skopenko; skopenko@mccme.ru