Московский физико-технический институт
Физтех-школа прикладной математики и информатики

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ

II СЕМЕСТР

Лектор: *Райгородский Андрей Михайлович*

$h\nu$

КОНСПЕКТ НЕ ОКОНЧЕН
СООБЩИТЬ ОБ ОШИБКЕ

Автор: *Даниил Максимов*
Проект на Github

весна 2022

Содержание

Замечание автора. В этом конспекте введены следующие обозначения для облегчения жизни:

$$\mathbb{N}_1 = \mathbb{N} = \{1, 2, 3, \ldots\}$$
$$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$$

1 Основы комбинаторики и теории чисел

1.1 Распределение простых чисел

Определение 1.1. *Пи-функцией от натурального числа x* будем называть количество простых чисел, меньших либо равных x:

$$\pi(x) = \sum_{p \leqslant x} 1$$

Определение 1.2. *Тета-функцией от натурального числа x* будем называть сумму натуральных логарифмов простых чисел, меньших либо равных x:

$$\Theta(x) = \sum_{p \leqslant x} \ln p$$

Определение 1.3. *Пси-функцией от натурального числа x* будем называть сумму натуральных логарифмов от простых чисел p по парам (p, α) так, что верно соотношение $p^\alpha \leqslant x$:

$$\psi(x) = \sum_{(p,\alpha)\colon\, p^\alpha \leqslant x} \ln p$$

Теорема 1.1. *(Чебышёва, 1848-1850гг.) Для всех достаточно больших x при фиксированном ε верно, что*

$$\pi(x) \in \left[(1-\varepsilon) \cdot \ln 2 \frac{x}{\ln x}; (1+\varepsilon) \cdot 4 \ln 2 \frac{x}{\ln x}\right]$$

Доказательство. Обозначим следующие пределы через λ и μ:

$$\lambda_1 := \overline{\lim_{x\to\infty}} \frac{\Theta(x)}{x}; \qquad \mu_1 := \underline{\lim_{x\to\infty}} \frac{\Theta(x)}{x}$$
$$\lambda_2 := \overline{\lim_{x\to\infty}} \frac{\psi(x)}{x}; \qquad \mu_2 := \underline{\lim_{x\to\infty}} \frac{\psi(x)}{x}$$
$$\lambda_3 := \overline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\ln x}; \qquad \mu_3 := \underline{\lim_{x\to\infty}} \frac{\pi(x)}{x/\ln x}$$

Лемма 1.1. *Утверждается, что*

$$\lambda_1 = \lambda_2 = \lambda_3; \quad \mu_1 = \mu_2 = \mu_3$$

Доказательство. Докажем данное утверждение лишь для λ, так как для μ всё происходит

абсолютно аналогично. Совершенно очевидно, что

$$\Theta(x) \leqslant \psi(x) \Rightarrow \frac{\Theta(x)}{x} \leqslant \frac{\psi(x)}{x} \Rightarrow \lambda_1 \leqslant \lambda_2$$

Теперь, распишем $\psi(x)$. Сколько существует пар для фиксированного p? Ровно $\left\lfloor \log_p x \right\rfloor = \left\lfloor \frac{\ln x}{\ln p} \right\rfloor$. Отсюда получаем

$$\psi(x) = \sum_{(p,\alpha)\colon p^\alpha \leqslant x} \ln p = \sum_{p \leqslant x} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \ln p \leqslant \ln x \cdot \sum_{p \leqslant x} 1 = \pi(x) \ln x$$

Таким образом, находим соотношение между вторым и третьим пределами:

$$\frac{\psi(x)}{x} \leqslant \frac{\pi(x)\ln x}{x} = \frac{\pi(x)}{x/\ln x} \Rightarrow \lambda_1 \leqslant \lambda_2 \leqslant \lambda_3;$$

Осталось доказать, что $\lambda_1 \geqslant \lambda_3$. Зафиксируем $\alpha \in (0;1)$. Тогда

$$\sum_{p \leqslant x} \ln p \geqslant \sum_{x^\alpha < p \leqslant x} \ln p > \sum_{x^\alpha < p \leqslant x} \ln(x^\alpha)$$

Последнюю сумму можно записать в следующем виде:

$$\sum_{x^\alpha < p \leqslant x} \ln(x^\alpha) = \alpha \ln x \sum_{x^\alpha < p \leqslant x} 1 = \alpha \ln x \cdot (\pi(x) - \pi(x^\alpha))$$

При этом понятно, что $\pi(x) \leqslant x$. Отсюда получаем новое неравенство:

$$\frac{\Theta(x)}{x} > \frac{\alpha \ln x}{x}(\pi(x) - \pi(x^\alpha)) \geqslant \frac{\alpha \ln x}{x}(\pi(x) - x^\alpha) = \alpha \cdot \left(\frac{\pi(x)}{x/\ln x} - \frac{x^\alpha \ln x}{x} \right)$$

Перейдём к пределу в неравенстве:

$$\lambda_1 \geqslant \alpha(\lambda_3 - 0) \Longrightarrow \forall \alpha \in (0;1)\ \lambda_1 \geqslant \alpha\lambda_3 \Longrightarrow \lambda_1 \geqslant \lambda_3$$

□

▷ Начнём доказательство с верхней оценки. Рассмотрим C_{2n}^n:

$$C_{2n}^0 + \ldots + C_{2n}^n + \ldots + C_{2n}^{2n} = 2^{2n} \Rightarrow C_{2n}^n < 2^{2n}$$

Более того, заметим следующее неравенство. Оно следует из того, что простые числа в диапазоне от $n < p \leqslant 2n$ никак не могли сократиться из-за знаменателя, ибо он сам не содержит чисел в разложении больше n:

$$C_{2n}^n \geqslant \prod_{n < p \leqslant 2n} p$$

Прологарифмируем полученное выражение и увидим ещё одну деталь:

$$\Theta(2n) - \Theta(n) = \sum_{n<p\leqslant 2n} \ln p \leqslant \ln C_{2n}^n < 2n \ln 2$$

Мы можем записать такие неравенства для всех $n = 2^k$, $k = 0, \ldots, m$. Сложив их, в итоге получим следующее:

$$\Theta(2^{m+1}) - \Theta(1) < \sum_{k=1}^{m+1} (2^k \ln 2) = \ln 2 \cdot \sum_{k=1}^{m+1} 2^k$$

При этом $\Theta(1) = 0$, а сумма степеней равна $2^{m+2} - 1 - 2^0 < 2^{m+2}$. То есть

$$\Theta(2^{m+1}) < 2^{m+2} \ln 2$$

Выберем произвольный натуральный x. Найдём m такое, что $2^m < x \leqslant 2^{m+1}$. Тогда

$$\Theta(x) \leqslant \Theta(2^{m+1}) < 2^{m+2} \ln 2 < 4 \ln 2 \cdot x \Rightarrow \frac{\Theta(x)}{x} < 4 \ln 2 \Rightarrow \lambda_3 = \lambda_1 \leqslant 4 \ln 2$$

По свойству верхнего предела получаем необходимое:

$$\exists \varepsilon > 0, X(\varepsilon) \in \mathbb{N} \;\big|\; \forall x \geqslant X \quad \frac{\pi(x)}{x/\ln x} \leqslant 4 \ln 2 \cdot (1 + \varepsilon)$$

▷ Теперь докажем нижнюю оценку. Для этого вспомним, что C_{2n}^n - наибольшее число в строке треугольника Паскаля. То есть

$$C_{2n}^0 + \ldots + C_{2n}^n + \ldots + C_{2n}^{2n} = 2^{2n}$$

Отсюда среднее число суммы - это $\frac{2^{2n}}{2n+1}$, и при этом верно соотношение

$$C_{2n}^n > \frac{2^{2n}}{2n+1} \text{ (будем рассматривать } n \geqslant 1)$$

Логарифмируя данное неравенство, получим оценку снизу на биномиальный коэффициент:

$$\ln C_{2n}^n > 2n \ln 2 - \ln(2n+1)$$

При этом есть и другое соотношение, связанное с записью факториала:

$$(n)! = \prod_{p\leqslant n} p^{\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \ldots}$$

Откуда оно взялось? Степень простого числа при разложении факториала - это вклад чисел от 1 до n, где данное простое число встретится 1 раз, 2 раза и так далее. Стало

быть

$$C_{2n}^n = \frac{\prod\limits_{p\leqslant 2n} p^{\left\lfloor \frac{2n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \dots}}{\prod\limits_{p\leqslant n} p^{2\left(\left\lfloor \frac{n}{p}\right\rfloor + \left\lfloor \frac{n}{p^2}\right\rfloor + \dots\right)}} = \prod_{p\leqslant 2n} p^{\left(\left\lfloor \frac{2n}{p}\right\rfloor - 2\left\lfloor \frac{n}{p}\right\rfloor\right) + \dots} \leqslant \prod_{p\leqslant 2n} p^{\left\lfloor \frac{\ln(2n)}{\ln p}\right\rfloor}$$

Утверждение 1.1. *Последний переход имеет место, так как* $\lfloor 2x\rfloor - 2\lfloor x\rfloor \leqslant 1$

Доказательство. Представим x как сумму целой и дробной частей:

$$x = a + b,\ 0 \leqslant b < 1$$

Тогда $2x = 2a + 2b$. Целая часть никак не влияет на округление, поэтому

$$\lfloor 2x\rfloor - 2\lfloor x\rfloor = 2a + \lfloor 2b\rfloor - 2a = \lfloor 2b\rfloor \leqslant 1$$

□

Логарифмируя полученное неравенство, получаем уже оценку сверху на биномиальный коэффициент:

$$\ln C_{2n}^n \leqslant \sum_{p\leqslant 2n} \ln p \cdot \left\lfloor \frac{\ln(2n)}{\ln p}\right\rfloor = \sum_{p\leqslant 2n} \ln p \cdot \left\lfloor \log_p(2n)\right\rfloor = \psi(2n)$$

Снова выберем произвольный натуральный x. Найдём для него такое n, что он окажется зажат между двумя соседними чётными числами: $2n \leqslant x < 2n + 2$. Отсюда

$$\psi(x) \geqslant \psi(2n) \geqslant 2n\ln 2 - \ln(2n+1) \geqslant 2n\ln 2 - \ln(x) \geqslant (x-2)\ln 2 - \ln(x)$$

В итоге имеем, что

$$\frac{\psi(x)}{x} > \ln 2 - \frac{2\ln 2}{x} - \frac{\ln(x)}{x}$$

Переходя к нижнему пределу, получаем необходимую оценку:

$$\mu_3 = \mu_2 \geqslant \ln 2 \Longrightarrow \exists \varepsilon > 0,\ X(\varepsilon) \in \mathbb{N} \mid \forall x \geqslant X \quad \frac{\pi(x)}{x/\ln x} \geqslant (1-\varepsilon)\ln 2$$

□

Теорема 1.2. *(без доказательства, Адамара и Валле-Пуссена, 1896г.) На бесконечности для* $\pi(x)$ *справедливо следующее утверждение:*

$$\pi(x) \sim \frac{x}{\ln x},\ x \to \infty$$

Теорема 1.3. *(без доказательства, Постулат Бертрана) Для любого натурального числа* $x \geqslant 1$ *всегда найдётся простое число* p *такое, что* $p \in [x; 2x]$.

Замечание. Обобщение Постулата Бертрана является на сегодняшний день (февраль 2022) открытой проблемой: для каких функций $f : \mathbb{N} \to \mathbb{R}$ таких, что $f(x) < x$, для любого $x \in \mathbb{N}$ будет всегда содержаться простое число p в диапазоне $[x; x + f(x)]$?

Известно, что лучшая оценка сейчас - это $f(x) = C \cdot x^{0.525}$, где C - подобранная константа. Доказано, что если гипотеза Римана о нулях дзета-функции верна, то в таком случае показатель степени можно свести к 0.5, но есть также гипотеза следующего вида:

$$\exists C \mid \forall x \in \mathbb{N}\ \exists p \in [x; x + C \ln^2 x]$$

1.2 Квадратичные вычеты

Определение 1.4. Пусть $m \in \mathbb{N}$. Число $a \in \mathbb{N}$ называется *квадратичным вычетом* по модулю m, если выполнены условия:

1. $(a, m) = 1$
2. $x^2 \equiv a \pmod{m}$

Замечание. Все остальные числа, для которых не выполнено второе условие, называются *невычетами.*

Теорема 1.4. *(Лагранжа) Пусть $f(x)$ - многочлен степени m с целыми коэффициентами, а p - произвольное простое число. Тогда из сравнения*

$$f(x) \equiv 0 \pmod{p}$$

может следовать лишь 2 факта:

- ▷ *Либо у $f(x)$ не более m корней в данном сравнении (с точностью до класса вычета);*
- ▷ *Либо все коэффициенты $f(x)$ кратны p.*

Доказательство. Так как p - простое число, то $\mathbb{Z}_p$ - поле. Предположим, что существует $m + 1$ различное решение, которые обозначим за $x_1, \ldots, x_{m+1}$. Тогда, $f(x)$ может быть записано в виде

$$f(x) = k_m(x - x_1) \cdot \ldots \cdot (x - x_m) + k_{m-1}(x - x_1) \cdot \ldots \cdot (x - x_{m-1}) + \ldots + k_1(x - x_1) + k_0$$

где $k_0, \ldots, k_m$ - целые числа (по условию, степень многочлена m, а потому данная запись имеет место быть). Теперь будем последовательно подставлять корни многочлена и выяснять коэффициенты:

$$\begin{aligned} &f(x_1) \equiv 0 \pmod{p} \Rightarrow k_0 \equiv 0 \pmod{p} \\ &f(x_2) \equiv 0 \pmod{p} \Rightarrow k_1 \equiv 0 \pmod{p} \\ &\vdots \\ &f(x_{m+1}) \equiv 0 \pmod{p} \Rightarrow k_m \equiv 0 \pmod{p} \end{aligned}$$

Если какой-то коэффициент не кратен p, то получим противоречие с предположением. В ином случае, многочлен будет сравним с нулевым и, стало быть, любой x будет решением. □

Следствие. У сравнения $x^2 \equiv a \pmod{p}$ не более двух решений.

Замечание. Более того, у сравнения $x^2 \equiv a \pmod p$ если и есть решение, то их ровно два: действительно, если x - решение, то и $(-x)$ - тоже:

$$(-x)^2 = x^2 \equiv a \pmod p$$

Отдельно отметим, для разных квадратичных вычетов a_1 и a_2 всегда получаются разные решения $\pm x_1,\ \pm x_2$.

Замечание. Далее и до конца параграфа мы считаем, что $m = p$ - простое число, причём $p > 2$.

Утверждение 1.2. *(о квадратичных вычетах и Малой Теореме Ферма) Если в сравнении $a^{p-1} \equiv 1 \pmod p$ a является квадратичным вычетом, то также верно сравнение*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

Доказательство. Распишем сравнение Малой Теоремы Ферма в следующем виде:

$$a^{p-1} \equiv 1 \pmod p \quad \Leftrightarrow \quad a^{p-1} - 1 \equiv 0 \equiv (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \pmod p$$

Если a - квадратичный вычет, то $\exists x_1 \in \mathbb{Z}_p$ такой, что

$$x_1^2 \equiv a \pmod p$$

Отсюда получаем

$$a^{\frac{p-1}{2}} \equiv (x_1^2)^{\frac{p-1}{2}} = x_1^{p-1} \equiv 1 \pmod p$$

□

Следствие. Для всех квадратичных вычетов по модулю p верно, что

$$a^{\frac{p-1}{2}} \equiv 1 \pmod p$$

а для всех невычетов (то есть оставшихся чисел) верно другое

$$a^{\frac{p-1}{2}} \equiv -1 \pmod p$$

Определение 1.5. *Символом Лежандра* $\left(\frac{a}{p}\right)$ называется функция от целого числа a и простого числа p, определяемая следующим образом:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, \text{ если } a \text{ - квадратичный вычет} \\ 0, \ a \equiv 0 \pmod p \\ -1, \text{ если } a \text{ - квадратичный невычет} \end{cases}$$

Замечание. Фактически символ Лежандра является значением сравнения

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$$

Из этого также следует как минимум 2 значения этого символа:

$$\left(\frac{1}{p}\right) = 1; \quad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Утверждение 1.3.

$$\sum_{a=1}^{p} \left(\frac{a}{p}\right) = 0$$

Доказательство. Уже доказано, что число невычетов и вычетов совпадает. Отсюда напрямую следует заявленное равенство. □

Утверждение 1.4. *Символ Лежандра мультипликативен, то есть*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Доказательство. Напрямую следует из замечания. □

Теорема 1.5.

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Доказательство. Зафиксируем любое a такое, что $(a, p) = 1$.

Утверждение 1.5.

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}} \pmod{p}$$

где $\varepsilon_i = \pm 1$ *- знак представителя числа* $a \cdot i$ *в системе вычетов* $\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$

Доказательство. Рассмотрим множество чисел $\{a \cdot 1, a \cdot 2, \ldots, a \cdot p_1\}$, где $p_1 = \frac{p-1}{2}$. Эти числа сравнимы со следующими:

$$\begin{aligned} a \cdot 1 &\equiv \varepsilon_1 r_1 \pmod{p} \\ &\vdots \\ a \cdot p_1 &\equiv \varepsilon_{p_1} r_{p_1} \pmod{p} \end{aligned}$$

где $\varepsilon_i = \pm 1$, $r_i \in \{1, \ldots, p_1\}$. Почему это так? Потому что увидим, что всевозможные произведения данных чисел дают систему вычетов $\left[-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\right]$. Теперь, перемножим все имеющиеся сравнения. Получим новое:

$$a^{\frac{p-1}{2}}(1 \cdot \ldots \cdot p_1) \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{p_1} \cdot (r_1 \cdot \ldots \cdot r_{p_1}) \pmod{p}$$

Заметим, что произведения в скобках слева и справа должны совпадать, так как никакие 2 числа из правой скобки не совпадают:

- ▷ Если $a \cdot x \equiv \varepsilon r$, $a \cdot y \equiv \varepsilon r \pmod{p}$, то очевидным образом $x = y$.
- ▷ Если $a \cdot x \equiv \varepsilon r$, $a \cdot y \equiv -\varepsilon r \pmod{p}$, то $a(x + y) \equiv 0 \pmod{p}$, где $(a, p) = 1$ и $x + y < p$. Такого быть не может.

Получили утверждение следующего вида:

$$a^{\frac{p-1}{2}} \equiv \varepsilon_1 \cdot \ldots \cdot \varepsilon_{p_1} \pmod{p}$$

□

Следствие.

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{\frac{p-1}{2}}$$

Утверждение 1.6.

$$\varepsilon_x = (-1)^{\left\lfloor \frac{2ax}{p} \right\rfloor}$$

Доказательство. Разобьём числовую прямую на системы вычетов:

$$\ldots \cup \{0, 1, \ldots, p-1\} \cup \{p, \ldots, 2p-1\} \cup \ldots$$

Далее возможно 2 случая, где окажется ax:

- ▷ ax в первой половине некоторой системы вычетов. То есть для некоторого k верно неравенство:

  $$kp + 1 \leqslant ax \leqslant kp + \frac{p-1}{2}$$

  Домножим на 2 и посмотрим, что получится

  $$2kp + 2 \leqslant 2ax \leqslant 2kp + p - 1$$

  То есть число $2ax$ лежит в системе, начинающаяся с $2kp$. Отсюда уже получаем

  $$2k + \frac{2}{p} \leqslant \frac{2ax}{p} \leqslant 2k + \frac{p-1}{p}$$

  В итоге добились требуемого:

  $$\left\lfloor \frac{2ax}{p} \right\rfloor = 2k \Rightarrow \varepsilon_x = 1 = (-1)^{2k}$$

- ▷ a во второй половине некоторой системы вычетов. Поступаем аналогично предыдущему пункту.

□

Следствие.

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{2ax}{p} \right\rfloor}$$

Утверждение 1.7. *Если a - нечётное число, то*

$$\left(\frac{2a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor + \frac{p^2-1}{8}}$$

Доказательство. Распишем символ Лежандра, описываемый в теореме:

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4((a+p)/2)}{p}\right) = \left(\frac{4}{p}\right) \cdot \left(\frac{(1/2)\cdot(a+p)}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{(a+p)x}{p} \right\rfloor}$$

Осталось лишь немного преобразовать степень:

$$\sum_{x=1}^{p_1} \left\lfloor \frac{(a+p)x}{p} \right\rfloor = \sum_{x=1}^{p_1} \left(\left\lfloor \frac{ax}{p} \right\rfloor + x \right) = \sum_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor + \frac{p_1(p_1+1)}{2} = \sum_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor + \frac{p^2-1}{8}$$

□

В выражение последнего утверждения остаётся подставить $a = 1$ и получить требуемое:

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{x}{p} \right\rfloor + \frac{p^2-1}{8}} = (-1)^{\frac{p^2-1}{8}}$$

□

Следствие. Если a - нечётно, то

$$\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor}$$

Доказательство. Пользуясь уже доказанным, распишем символ Лежандра для $2a$:

$$\left(\frac{2a}{p}\right) = (-1)^{\sum\limits_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor + \frac{p^2-1}{8}} = \left(\frac{2}{p}\right) \cdot \left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}} \cdot \left(\frac{a}{p}\right)$$

Откуда уже следует нужное равенство. □

Теорема 1.6. *(Квадратичный закон взаимности) Если p, q - нечётные простые числа, то*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{p_1 \cdot q_1}$$

где $p_1 = \frac{p-1}{2}$, $q_1 = \frac{q-1}{2}$

Доказательство. По уже доказанному, распишем произведение символов из теоремы:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\sum\limits_{x=1}^{q_1} \left\lfloor \frac{qx}{p} \right\rfloor + \sum\limits_{y=1}^{p_1} \left\lfloor \frac{py}{q} \right\rfloor}$$

То есть всё сводится к доказательству того, что

$$\sum_{x=1}^{q_1} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{p_1} \left\lfloor \frac{py}{q} \right\rfloor = p_1 \cdot q_1$$

Для этого воспользуемся комбинаторикой: подсчитаем количество пар чисел (x, y) таких, что $1 \leqslant x \leqslant p_1$, $1 \leqslant y \leqslant q_1$. Их всего $p_1 \cdot q_1$. Заметим, что среди них нет пар таких, что $py = qx$:

Если бы это было не так, то без умаления общности положим $p > q$. Равенство возможно лишь тогда, когда $x \geqslant p > q$ - противоречие.

Из этого следует, что все пары делятся на 2 группы, которые мы тоже посчитаем:

▷ $qx < py \Leftrightarrow x \leqslant \left\lfloor \frac{py}{q} \right\rfloor$. Отсюда получаем возможность посчитать количество K_1 пар в данной группе:

$$K_1 = \sum_{y=1}^{q_1} \left\lfloor \frac{py}{q} \right\rfloor$$

Почему все y будут корректными? То есть не случится такого, что $\left\lfloor \frac{py}{q} \right\rfloor > p_1$?

$$y \leqslant q_1 = \frac{q-1}{2} \Rightarrow \frac{py}{q} \leqslant \frac{p(q-1)}{2q} = \frac{p-1}{2} + \frac{q-p}{2q}$$

Несложно проверить арифметическими операциями, что $\frac{q-p}{2q} < 1$. То есть всё хорошо округлится и никаких выходов за границы не случится.

▷ Аналогично предыдущему случаю. Число этих пар - K_2 получается равным

$$K_2 = \sum_{x=1}^{p_1} \left\lfloor \frac{qx}{p} \right\rfloor$$

По уже обоснованной причине имеем следующее равенство:

$$K_1 + K_2 = \sum_{x=1}^{q_1} \left\lfloor \frac{qx}{p} \right\rfloor + \sum_{y=1}^{p_1} \left\lfloor \frac{py}{q} \right\rfloor = p_1 \cdot q_1$$

□

1.3 Матрицы Адамара

Определение 1.6. *Матрицей Адамара* порядка n называется квадратная матрица A такая, что $A_{ij} \in \{\pm 1\}$ и любые 2 не одинаковые строки ортогональны (сумма произведений элементов строк постолбцово даёт 0).

Утверждение 1.8. *Если матрица Адамара $A \in M_n$ существует, то у неё и столбцы попарно ортогональны.*

Доказательство. Заметим следующее равенство:

$$A \cdot A^T = nE_n$$

Коль скоро $\det(A \cdot A^T) = \det A \cdot \det A^T$, то A и A^T не вырождены. Домножим слева на A^T и справа на A:

$$A^T \cdot (A \cdot A^T) \cdot A = (A^T \cdot A)^2 = A^T \cdot nE_n \cdot A = nE_n \cdot (A^T \cdot A)$$

Осталось домножить на $(A^T \cdot A)^{-1} = A^{-1} \cdot (A^T)^{-1}$ и получить равенство:

$$A^T \cdot A = nE_n$$

□

Следствие. Если домножить строку или столбец матрицы Адамара на -1, то она останется матрицей Адамара. Отсюда получаем, что если для некоторого n нашлась матрица Адамара, то найдётся и другая, которая имеет вид:

$$H_n = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ 1 & & & \\ \vdots & & \pm 1 & \\ 1 & & & \end{pmatrix}$$

Матрицу Адамара в таком виде будем называть *нормальной*.

Пример.

▷ $n = 1$

$$H_1 = (1)$$

▷ $n = 2$

$$H_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

▷ $n = 3 \Rightarrow \varnothing$

Утверждение 1.9. *Если $n \geqslant 2$, то матрица Адамара может существовать только для чётного n.*

Доказательство. Рассмотрим произвольную не верхнюю строку в H_n. Тогда, в произведении с верхней она должна давать 0. Такое возможно тогда и только тогда, когда количество -1 и 1 в строке совпадают, отсюда следует чётность n. □

Утверждение 1.10. *Если $n \geqslant 4$, то матрица Адамара может существовать только для n, кратного 4.*

Доказательство. В любой матрице H_n можно переставить столбцы так, чтобы где-то собралась строка вида

$$\underbrace{1 \ \ldots \ 1}_{n/2} \underbrace{-1 \ \ldots \ -1}_{n/2}$$

Такая строка при «умножении» с любой другой должна давать 0. Пусть x - это количество единиц другой строки, которые попали под позиции, где у полученной строки стоят 1. Тогда, $x > 0$ и на остальных $n/2 - x$ позициях стоят, естественно, -1. Так как количеств 1 и -1 поровну, то позициям -1 полученной строки соответствует $n/2 - x$ единиц и x минус единиц. Отсюда имеем равенство:

$$1 \cdot x - \left(\frac{n}{2} - x\right) - \left(\frac{n}{2} - x\right) + x = 0; \quad n = 4x$$

□

Гипотеза 1. *(Адамара, не доказана/опровергнута) Матрица Адамара существует для $n \geqslant 4$ тогда и только тогда, когда $n = 4k$, $k \geqslant 1$.*

Замечание. Для чисел, меньших 1000, гипотеза не доказана только для 668, 716 и 892.

Пример. Матрицу H_4 можно построить по подобию H_2:

$$H_4 = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} = \begin{pmatrix} H_2 & H_2 \\ H_2 & -H_2 \end{pmatrix}^{\square}$$

Этот же метод работает и для любого $n = 2^k$, $k \geqslant 1$.

Определение 1.7. *Кронекеровским произведением* $A * B$ матриц $A \in M_{n\times m}$, $B \in M_{p\times q}$ называется матрица вида

$$A * B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1m}B \\ \vdots & \vdots & \vdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nm}B \end{pmatrix}^{\square} \in M_{np\times mq}$$

Утверждение 1.11. *Если A и B - матрицы Адамара, то и $A * B$ - тоже матрица Адамара.*

Доказательство. Достаточно доказать, что строки полученной матрицы ортогональны. Посмотрим, как бы выглядели произвольные строки, которые мы выбрали для умножения:

$$\begin{matrix} a_{i1}B_{l*} & a_{i2}B_{l*} & \cdots & a_{im}B_{l*} \\ a_{t1}B_{r*} & a_{t2}B_{r*} & \cdots & a_{tm}B_{r*} \end{matrix}$$

При умножении можно собрать некоторые слагаемые в скобки при $b_{lx} \cdot b_{ry}$. Выражение, которое находится внутри, получается аналогичным тому, что получается при умножении строк матрицы A. $\square$

Определение 1.8. *Матрицей Якобсталя* порядка p, где p - простое число, называется матрица Q вида

$$Q_{ij} := \left(\frac{i-j}{p}\right)$$

Утверждение 1.12. *Произведение любых двух строк матрицы Якобсталя равно -1. То есть*

$$\sum_{j=1}^{p} \left(\frac{i_1-j}{p}\right)\left(\frac{i_2-j}{p}\right) = -1$$

Доказательство. Так как j пробегает всю систему вычетов, то и $i_1 - j$ делает так же. Сделаем замену $b = i_1 - j$. В таком случае, $i_2 - j = i_1 - j + (i_2 - i_1) = b + (i_2 - i_1) = b + c$, а сумма запишется в следующем виде:

$$\sum_{j=1}^{p} \left(\frac{i_1-j}{p}\right)\left(\frac{i_2-j}{p}\right) = \sum_{b=1}^{p} \left(\frac{b}{p}\right)\left(\frac{b+c}{p}\right)$$

Если $i_1 \neq i_2$, то $c \not\equiv 0 \pmod p$ и наоборот. Сделаем некоторые преобразования над суммой:

$$\sum_{b=1}^{p} \left(\frac{b}{p}\right)\left(\frac{b+c}{p}\right) = \sum_{b=1}^{p-1} \left(\frac{b}{p}\right)\left(\frac{1\cdot(b+c)}{p}\right) = \sum_{b=1}^{p-1} \left(\frac{b}{p}\right)\left(\frac{b\cdot b^{-1}(b+c)}{p}\right) =$$

$$\sum_{b=1}^{p-1} \left(\frac{b}{p}\right)^2 \left(\frac{1+b^{-1}c}{p}\right) = \sum_{b=1}^{p-1} \left(\frac{1+b^{-1}c}{p}\right) = -1$$

□

Утверждение 1.13. *(Первая конструкция Пэли) Рассмотрим $p = 4k+3$ (считаем известным, что данных простых чисел бесконечно много и они распределены $\pm$ равномерно). Если $n = p+1$, то существует матрица Адамара этого порядка, имеющая вид*

$$H_n = \begin{pmatrix} 1 & 1 & \cdots\cdots & 1 \\ 1 & & & \\ \vdots & & Q_p - E_p & \\ 1 & & & \end{pmatrix}$$

где Q_p - матрица Якобсталя порядка p.

Доказательство. Проверим ортогональность строк

- ▷ Умножение какой-то строки с первой, очевидно, даст 0: у нас было поровну единиц и минус единиц в Q_p, но ещё мы добавили единицу слева и минус единицу вместо нуля на диагонали.
- ▷ Рассмотрим произведение строк i_1 и i_2, где ни одна не является первой. Распишем слагаемые слева-направо:

$$1 + \sum_{j=1}^{p} \left(\frac{i_1 - j}{p}\right)\left(\frac{i_2 - j}{p}\right) + (-1)\cdot\left(\frac{i_2 - i_1}{p}\right) + (-1)\cdot\left(\frac{i_1 - i_2}{p}\right) = 0$$

  Последние 2 слагаемых - это то, что получается, когда мы попадаем на диагональ матрицы.

□

Замечание. Нам нужно $p = 4k+3$ потому, что иначе не выполнится равенство

$$\left(\frac{i_2 - i_1}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{i_1 - i_2}{p}\right)$$

и полученная матрица не будет иметь порядок, делящийся на 4.

Следствие. Зная распределение простых чисел и конструкцию Пэли, теперь можно заявить следующее:

$\forall \varepsilon > 0\ \exists N \in \mathbb{N} \mid \forall n \geqslant N$ на отрезке $[n; (1+\varepsilon)n]$ найдётся порядок матрицы Адамара

Доказательство второй конструкции Пэли по А. Мирошникову

Утверждение 1.14. *(Свойства кронекеровского произведения) Кронекерово произведение обладает двумя замечательными свойствами:*

1. $$\forall A \in M_{n\times m}, B \in M_{k\times d} \quad (A \oplus B)^T = A^T \oplus B^T$$

2. $$\forall A, B, C, D \in M_n \quad (A \oplus B)(C \oplus D) = (AC) \oplus (BD)$$

Доказательство.

1. Обозначим $C = A \oplus B$, $D = C^T$. Посмотрим на произвольную ячейку d_{ij}. Распишем координаты в следующем виде:

$$i = t \cdot d + l,\ l < d$$
$$j = q \cdot k + p,\ p < k$$

   Теперь можно приступить к рассмотрению ячейки более подробно:

$$d_{ij} = d_{td+l,\ qk+p} = c_{qk+p,\ td+l} = a_{qt} \cdot b_{pl} = (A^T)_{tq} \cdot (B^T)_{lp} = (A^T \oplus B^T)_{td+l,\ qk+p}$$

2. Распишем левую часть равенства:

$$(A \oplus B)(C \oplus D) = \begin{pmatrix} a_{11}B & \cdots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix}^{\square} \begin{pmatrix} c_{11}D & \cdots & c_{1n}D \\ \vdots & \ddots & \vdots \\ c_{n1}D & \dots & c_{nn}D \end{pmatrix}^{\square} = \begin{pmatrix} R_{11} & \cdots & R_{1n} \\ \vdots & \ddots & \vdots \\ R_{n1} & \dots & R_{nn} \end{pmatrix}^{\square}$$

   В силу блочного умножения матриц, несложно увидеть следующую формулу:

$$R_{ij} = \sum_{k=1}^{n} (a_{ik}B)(c_{kj}D)$$

   Расписывая её, получим требуемое равенство:

$$R_{ij} = \sum_{k=1}^{n} (a_{ik}B)(c_{kj}D) = \left(\sum_{k=1}^{n} a_{ik}c_{kj}\right) \cdot BD = (AC)_{ij} \cdot BD$$

□

Лемма 1.2. *(Свойства матрицы Якобсталя) Если $p \equiv 1 \pmod 4$, то верны следующие факты:*

1. *Q_p симметрична*
2. *$Q_p \cdot Q_p^T = pE_p - I_p$, где I_p - матрица, состоящая полностью из единиц*

Доказательство.

1. Просто посмотрим на элемент матрицы Якобсталя:

$$\left(\frac{i-j}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{j-i}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{j-i}{p}\right) = \left(\frac{j-i}{p}\right)$$

2. Из первой конструкции мы знаем, что произведение любых различных строк матрицы Якобсталя даёт -1, а одной и той же даст $p-1$. В силу симметрии и того факта, что $Q_p \cdot Q_p^T$ выдаёт в ячейке как раз произведение двух строк, заключаем искомое выражение:

$$Q_p \cdot Q_p^T = pE_p - I_p$$

□

Утверждение 1.15. *(Вторая конструкция Пэли) Если $p = 4m+1$, $n = 2p+2$ для некоторого $m \in \mathbb{N}_0$, то существует матрица Адамара порядка n, получаемая следующим путём:*

1. *Запишем следующую матрицу*

$$A = \begin{pmatrix} 0 & e^T \\ e & Q_p \end{pmatrix}^{\square} \in M_{p+1}$$

где e - единичный столбец высоты p.

2. *Получим искомую матрицу, заменив элементы A следующим образом:*

$$0 \longrightarrow M_0 = \begin{pmatrix} 1 & -1 \\ -1 & -1 \end{pmatrix}$$
$$\pm 1 \longrightarrow \pm M_1 = \pm \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

Доказательство. Произведём доказательство в несколько стадий:

1. Вычислим AA^T. Понятно, что в левом верхнем углу будет стоять $p-1$. В остальных ячейках первой строки/столбца будут стоять нули, так как их выражения представляют собой сумму символов Лежандра. Методом пристального взгляда заметим, что в оставшемся пространстве получится $Q_p \cdot Q_p^T + I_p = pE_p$. Итого имеем

$$A \cdot A^T = A^2 = pE_{p+1}$$

2. Отметим отдельно, что матрицы M_0, M_1 - это матрицы Адамара. Более того, верны все следующие утверждения:

$$M_i^T = M_i$$
$$M_i^2 = M_i^T \cdot M_i = 2E_2$$
$$M_1 M_0 = -M_0 M_1$$

3. Обозначим за H искомую матрицу, получаемую подстановкой M_0 и M_1. Тогда, её можно записать в следующем виде:

$$H = A \oplus M_1 + E_{p+1} \oplus M_0$$

Докажем теперь, что она действительно является матрицей Адамара. Для этого вычислим HH^T:

$$\begin{aligned} HH^T = (A \oplus M_1 + E_{p+1} \oplus M_0)(A \oplus M_1 + E_{p+1} \oplus M_0)^T = \\ (A \oplus M_1 + E_{p+1} \oplus M_0)(A^T \oplus M_1^T + E_{p+1} \oplus M_0^T) = \\ (A \oplus M_1)(A^T \oplus M_1) + (A \oplus M_1)(E_{p+1} \oplus M_0) + \\ (E_{p+1} \oplus M_0)(A^T \oplus M_1) + (E_{p+1} \oplus M_0)(E_{p+1} \oplus M_0) = \\ (AA^T) \oplus M_1^2 + A \oplus (M_1 M_0) + A^T \oplus (M_0 M_1) + E_{p+1} \oplus M_0^2 = \\ pE_{p+1} \oplus 2E_2 + E_{p+1} \oplus 2E_2 = (2p+2)E_{2p+2} \end{aligned}$$

□

Применение матриц Адамара

1. Задача об уклонении

Определим множество $V_n = \{1, \ldots, n\}$. В нём выбрано s подмножеств $M_1, \ldots, M_s \subseteq V_n$. Обозначим за $\mathcal{M} = \{M_1, \ldots, M_s\}$. Введём функцию *раскраски*:

$$\chi \colon V_n \to \{\pm 1\}$$

Дополнительно с тем же обозначением введём значение функции для подмножества:

$$\chi(M_i) = \sum_{j \in M_i} \chi(j)$$

Разбросом $\mathcal{M}$ по χ назовём величину

$$\operatorname{disc}(\mathcal{M}, \chi) = \max_{i \in \{1,\ldots,s\}} |\chi(M_i)|$$

А разбросом $\mathcal{M}$ обозначим величину

$$\operatorname{disc}(\mathcal{M}) = \min_{\chi} \operatorname{disc}(\mathcal{M}, \chi)$$

Фактически, мы хотим раскрасить множество так, что по выбранным подмножествам баланс цветов стремится к идеальному, то есть синих и красных почти (или вообще) поровну.

Теорема 1.7. *Пусть $s = n$, где n - порядок матрицы Адамара. Тогда существует набор подмножеств $\mathcal{M} = \{M_1, \ldots, M_s\}$ такой, что*

$$\operatorname{disc}(\mathcal{M}) \geqslant \frac{\sqrt{n}}{2}$$

Более того, маски M_i являются строками в матрице $\frac{H_n+J}{2}$, где J - матрица, состоящая полностью из единиц.

Доказательство. Фактически надо доказать, что $\forall \vec{v} = (v_1, \ldots, v_n)^T$, $v_i \in \{\pm 1\}$ у вектора вида

$$\vec{u} = \left(\frac{H_n + J}{2}\right) \cdot \vec{v}$$

есть координата, модуль которой $\geqslant \frac{\sqrt{n}}{2}$. Иначе говоря, $\vec{v}$ - это раскраска V_n, и так совпало, что произведение будет давать в координатах разброс каждого подмножества.

Распишем произведение из определения вектора $\vec{u}$:

$$\vec{u} = \left(\frac{H_n + J}{2}\right) \cdot \vec{v} = \frac{1}{2} \cdot (H_n\vec{v} + J\vec{v})$$

Отдельно разберёмся с первым слагаемым в скобках. Обозначим $H\vec{v} = (L_1, \ldots, L_n)^T$ и рассмотрим скалярный квадрат:

$$\langle H_n\vec{v}, H_n\vec{v}\rangle = L_1^2 + \ldots + L_n^2$$

Дополнительно скажем, что $H_n = (\vec{h}_1 \cdots \vec{h}_n)$ и h_{ij} - это элемент матрицы Адамара. Тогда

$$\langle H_n\vec{v}, H_n\vec{v}\rangle = \left\langle v_1\vec{h}_1 + \ldots + v_n\vec{h}_n, v_1\vec{h}_1 + \ldots + v_n\vec{h}_n \right\rangle = v_1^2 \underbrace{\left\langle \vec{h}_1, \vec{h}_1 \right\rangle}_{n} + \ldots + v_n^2 \underbrace{\left\langle \vec{h}_n, \vec{h}_n \right\rangle}_{n} + \sum_{i\neq j} v_i v_j \underbrace{\left\langle \vec{h}_i, \vec{h}_j \right\rangle}_{0} = n^2$$

Отсюда следует, что $\exists i\colon |L_i| \geqslant \sqrt{n}$. Теперь распишем всё произведение, за исключением домножения на скаляр:

$$(H + J)\vec{v} = \left(L_1 + \sum_{i=1}^{n} v_i, \ldots, L_n + \sum_{i=1}^{n} v_i\right)^T$$

где $\sum\limits_{i=1}^{n} v_i = \lambda$, причём λ должна быть чётным числом. Снова возьмём скалярный квадрат от всего выражения, получим следующее:

$$\langle (H + J)\vec{v}, (H + J)\vec{v}\rangle = L_1^2 + \ldots + L_n^2 + 2\lambda \sum_{i=1}^{n} L_i + \lambda^2 n = n^2 + 2\lambda \sum_{i=1}^{n} L_i + \lambda^2 n$$

Отдельно посчитаем оставшуюся сумму:

$$\sum_{i=1}^{n} L_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{n} h_{ij} v_j\right) = \sum_{j=1}^{n} v_j \left(\sum_{i=1}^{n} h_{ij}\right) = v_1 \cdot n$$

Подставим полученное в выражение выше:

$$n^2 + 2\lambda \sum_{i=1}^{n} L_i + \lambda^2 n = n^2 + 2nv_1\lambda + n\lambda^2$$

Для оценки модулей координат нам надо оценить минимум скалярного квадрата. Это сделать мы можем, так как имеем дело с параболой ветвями вверх относительно λ:

$$\lambda_{min} = \frac{-2nv_1}{2n} = -v_1 \in \{\pm 1\}$$

Из-за того, что λ - чётное число, то необходимо произвести разбор случаев:

$$\lambda_{min} \in \begin{cases} \{-2, 0\},\ v_1 = 1 \\ \{0, 2\},\ v_1 = -1 \end{cases}$$

В обоих случаях есть вариант с $\lambda = 0$, поэтому

$$\langle (H+J)\vec{v}, (H+J)\vec{v} \rangle = n^2 + 2nv_1\lambda + n\lambda^2 \geqslant n^2$$

Отсюда уже следует существование координаты с модулем $\geqslant \sqrt{n}$, ну а стало быть в исходном виде $\geqslant \frac{\sqrt{n}}{2}$. □

Следствие. Если $s = n$ (уже не обязательно порядок матрицы Адамара), то $\mathrm{disc}(\mathcal{M}) \geqslant (1 - \varepsilon_n)\frac{\sqrt{n}}{2}$, где $\varepsilon_n \to 0$ при $n \to \infty$

Теорема 1.8. *(без доказательства) Если $s = n$, то*

$$\forall \mathcal{M}\ \ \mathrm{disc}(\mathcal{M}) \leqslant 6\sqrt{n}$$

2. Задача о кодах, исправляющих ошибки.

Есть источник и приёмник. Между ними установлен канал связи, по которому можно передавать слова в виде двоичного кода, однозначно сопоставленного каждому слову. К сожалению, при передаче возникают помехи, из-за которых в произвольном месте кода 1 может замениться на 0 и наоборот. Какое максимальное количество слов можно передать?

Определение 1.9. *Расстоянием Хэмминга* между двумя двоичными кодами длины n назовём число позиций, в которых они различаются (или же квадрат евклидова расстояния между точками n-мерного пространства).

Пример. Для кодов 01110 и 11001 расстояние Хэмминга будет 4.

Утверждение 1.16. *Рассмотрим произвольный код длины n. Число кодов такой же длины, для которых расстояние Хэмминга с исходным не превышает d, будет $C_n^0 + \ldots + C_n^d$*

Доказательство. В сумме C_n^i символизирует количество способов выбрать i позиций, на местах которых мы изменим число в исходном коде. □

Определение 1.10. *Кодом, исправляющим ошибки* (n, M, d) будем называть код, который может передать M слов, каждое закодировано при помощи n нулей и единиц (то есть длина кода) и d - минимальное расстояние Хэмминга между словами.

Замечание. Если такой код существует, то он исправляет не более чем $\left\lfloor \frac{d-1}{2} \right\rfloor$ ошибок, чтобы иметь возможность однозначно раскодировать слова.

Теорема 1.9. *(Граница Плоткина) Пусть* $2d > n$. *Тогда* $M \leqslant \left\lfloor \frac{2d}{2d-n} \right\rfloor$.

Доказательство. Пусть $a_1, \ldots, a_M$ - кодовые слова, то есть последовательности из 0 и 1 длины n. Запишем их в виде матрицы A:

$$A = (a_{ij}) = \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_M \end{pmatrix}^{\square} \in M_{M \times n}$$

Посчитаем суммарное количество ошибок в кодовых словах, если рассмотреть пары с точностью до перестановки слов:

$$\sum_{1 \leqslant i < j \leqslant M} \left(\sum_{k=1}^{n} \mathbb{I}_{\{a_{ik} \neq a_{jk}\}} \right) \geqslant \frac{M(M-1)}{2} \cdot d$$

где $\mathbb{I}$ - это функция-индикатор, то есть

$$\mathbb{I}_{\{\text{условие}\}} = \begin{cases} 1, & \text{условие истинно} \\ 0, & \text{условие ложно} \end{cases}$$

А теперь попробуем посчитать сумму с другой стороны, поменяв знаки суммирования местами. Пусть в столбце было x_k единиц. Тогда

$$\sum_{1 \leqslant i < j \leqslant M} \mathbb{I}_{\{a_{ik} \neq a_{jk}\}} = x_k \cdot (M - x_k)$$

Снова столкнулись с параболой, но уже ветвями вниз. Её можно оценить сверху как $\frac{M^2}{4}$. Отсюда

$$\sum_{k=1}^{n} \left(\sum_{1 \leqslant i < j \leqslant M} \mathbb{I}_{\{a_{ik} \neq a_{jk}\}} \right) \leqslant n \cdot \frac{M^2}{4}$$

В итоге получили следующую оценку:

$$\frac{M(M-1)}{2} \cdot d \leqslant n\frac{M^2}{4}; \quad 2(M-1)d \leqslant nM; \quad M(2d-n) \leqslant 2d$$

$\square$

Утверждение 1.17. *Граница Плоткина достигается, если рассмотреть код* $(n-1, n, n/2)$. *Кодовые слова записаны в матрице Адамара* H_n, *если удалить левый столбец и заменить все* -1 *на 0.*

Доказательство. При удалении левого столбца число -1 не изменяется, а потому расстояние между первой и любой другой строкой будет в аккурат $n/2$. Подставим все величины кода в оценку Плоткина:

$$n \leqslant \left\lfloor \frac{n}{n-(n-1)} \right\rfloor = n$$

□

1.4 Первообразные корни и индексы

Определение 1.11. Пусть $m \in N$, $a \in \mathbb{Z}$: $(a, m) = 1$. *Показателем элемента* a по модулю m (или же *порядком элемента* a в группе $\mathbb{Z}_m$) называется минимальное положительное целое число δ такое, что

$$a^\delta \equiv 1 \pmod{m}$$

Замечание. Согласно теореме Эйлера

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

поэтому $\delta \leqslant \varphi(m)$ точно.

Замечание. Отсюда и до конца параграфа мы будем сохранять введённые выше обозначения a, m, δ, если не сказано обратного.

Утверждение 1.18. $\delta \mid \varphi(m)$ *всегда.*

Доказательство. Предположим обратное. Тогда, $\varphi(m)$ делится на δ с остатком:

$$\varphi(m) = \delta q + r,\ 0 < r < \delta$$

Но в таком случае заметим, что

$$1 \equiv a^{\varphi(m)} \equiv a^{\delta q + r} = a^r \cdot (a^\delta)^q \equiv a^r$$

Получили противоречие с выбором δ. □

Утверждение 1.19. *Все числа* $\{1, a, a^2, \ldots, a^{\delta-1}\}$ *различны.*

Доказательство. Предположим, что $a^i \equiv a^j \pmod{m}$, $i \geqslant j$. Однако, это означает, что если домножить обе части на $a^{\delta-i}$, то получится следующее:

$$1 \equiv a^\delta \equiv a^{\delta-(i-j)} \pmod{m}$$

Такое возможно тогда и только тогда, когда $i = j$. □

Определение 1.12. Назовём a *первообра́зным корнем* по модулю m, если $\delta(a) = \varphi(m)$, то есть показатель элемента a по модулю m совпадает со значением функции Эйлера от m.

Замечание. Степени первообразного корня образуют всю приведённую систему вычетов.

Определение 1.13. *Дискретным логарифмом* (*индексом*) числа b, взаимно простого с m, по основанию a будем называть число

$$\operatorname{ind}_a b := \log_a b := i \Leftrightarrow a^i \equiv b \pmod m$$

Замечание. Особенность индекса заключается в том, что на данный момент не существует алгоритма с приемлемой асимптотикой, который позволяет быстро вычислить индекс произвольного допустимого числа. На этой загвоздке основан один из методов шифрования.

Шифрование сообщений

Задача. *Алиса и Боб хотят произвести обмен сообщениями по некоторому каналу связи. При этом они желают, чтобы любой человек, который перехватит сообщение, не смог его прочитать. Для этого они используют шифрование, основанное на степенях первообразного корня по некоторому модулю m. (Например, $m \approx 10^{100}$)*

Решение. Алиса и Боб фиксируют числа a и b соответственно, которые знают только они. Всем известен модуль m и то, что у него есть первообразный корень g. Далее Алиса высчитывает число $g^a \pmod m$, а Боб - $g^b \pmod m$ и передают их друг-другу по каналу. Теперь, если Алиса возведёт число Боба в степень a по модулю, а Боб возведёт её число в степень b, то они получат *ключ* ab, который не будет известен никому кроме них. (В предположении, что вычисление индекса - крайне трудоёмкая задача). Далее с этим ключом они уже могут делать что угодно.

Теорема 1.10. *Если $m = 2^\alpha$, $\alpha \geqslant 3$, то первообразного корня для такого модуля m не существует.*

Замечание. Для $m = 2$ естественно корнем будет 1, а для $m = 4$ корнем будет 3.

Доказательство. Заметим, что при таком модуле все взаимно простые с модулем числа - это все нечётные числа. Рассмотрим любое такое a:

$$\begin{aligned} &a = 1 + 2t_0 \\ &a^2 = (1+2t_0)^2 = 1 + 4t_0 + 4t_0^2 = 1 + 4\underbrace{t_0(1+t_0)}_{\text{делится на 2}} = 1 + 8t_1 \\ &\vdots \\ &a^{2^k} = 1 + 2^{k+2} \cdot t_k \end{aligned}$$

Подставим $k = \alpha - 2$:

$$a^{2^{\alpha-2}} = 1 + 2^\alpha \cdot t_{\alpha-2} \equiv 1 \pmod m$$

А взаимно простых с m чисел $\varphi(m) = 2^{\alpha-1} > 2^{\alpha-2}$. □

Теорема 1.11. *По модулю любого нечётного простого числа p существует первообразный корень.*

Доказательство. Рассмотрим приведённую систему вычетов $\{1, \ldots, p-1\}$. У каждого числа в ней есть свой показатель, которые мы обозначим за $\{\delta_1, \ldots, \delta_{p-1}\}$. Определим

число τ - НОК этих показателей:

$$\tau := [\delta_1, \ldots, \delta_{p-1}] \leqslant p-1$$

Теперь наша цель - построить некоторое число с показателем τ и доказать, что τ в точности равно $p-1$.

1. Разложим число τ на простые сомножители:

   $$\tau = q_1^{k_1} \cdot \ldots \cdot q_s^{k_s}$$

   Из свойств НОКа известно, что любой k_i - это максимум степеней у $\{\delta_1, \ldots, \delta_{p-1}\}$. Следовательно

   $$\forall i \in \{1, \ldots, s\}\ \exists \delta \in \{\delta_1, \ldots, \delta_s\} \mid \delta = a \cdot q_i^{k_i}$$

   То есть можно определить некоторую функцию, которая по i будет выдавать соответствующие δ и a.

   На время зафиксируем некоторое такое i и соответствующие ему δ и a. Рассмотрим тот $x \in \{1, \ldots, p-1\}$, у которого δ служит показателем. Тогда заметим следующие вещи:

   Утверждение 1.20. *x^a имеет показатель $q_i^{k_i}$.*

   Доказательство. Посмотрим на x^a в данной степени:

   $$(x^a)^{q_i^{k_i}} = x^{aq_i^{k_i}} = x^{\delta} \equiv 1 \pmod{p}$$

   При этом понятно, что меньшего показателя найтись не могло - было бы противоречие с тем, что само δ является показателем числа x. □

   Утверждение 1.21. *Если у некоторых чисел u, v показатели δ_u, δ_v взаимно просты, то показателем uv будет $\delta_u \cdot \delta_v$ (В предположении модуля p).*

   Доказательство. Для начала удостоверимся, что такая степень сойдёт за показатель:

   $$(uv)^{\delta_u \delta_v} = (u^{\delta_u})^{\delta_v} \cdot (v^{\delta_v})^{\delta_u} \equiv 1 \pmod{p}$$

   Пока дальше не пошло, а затехать остальное надо. □

   Из этих утверждений следует, что произведение x по всем i даёт число, у которого показатель ровно τ.

2. Рассмотрим сравнение следующего вида:

   $$y^{\tau} \equiv 1 \pmod{p}$$

   По уже доказанной теореме Лагранжа, у него не более τ корней. Но при этом известно, что любое число из $\{1, \ldots, p-1\}$ является его корнем, так как τ - НОК их показателей. Отсюда имеем, что $p-1 \leqslant \tau \leqslant p-1$, то есть $\tau = p-1$.

□

Теорема 1.12. *Для любого $\alpha \geqslant 1$ первообразный корень по модулю p^α тоже существует, если p - нечётное простое число.*

Доказательство. Рассмотрим g - первообразный корень по модулю p.

Лемма 1.3. *Существует такое t и $u(t)$, что выполнено равенство*

$$(g+pt)^{p-1} = 1 + pu,\ (u,p) = 1$$

Доказательство. Распишем степень $g+pt$ по биному Ньютона:

$$(g+pt)^{p-1} = g^{p-1} + (p-1)g^{p-2} \cdot pt + p^2 v$$

где v просто обозначает части оставшихся слагаемых. При этом

$$g^{p-1} \equiv 1 \pmod{p} \Leftrightarrow g^{p-1} = 1 + pw$$

Подставим это равенство в первое:

$$(g+pt)^{p-1} = 1 + p(w + (p-1)g^{p-2}t + pv)$$

Заметим, что $(p-1)g^{p-2}$ - взаимно просто с p, так как g^{p-2} это фактически обратное число к g по модулю p, а стало быть точно не кратно ему. Отсюда получаем метод нахождения u:

1. Если $w \equiv 0 \pmod{p}$, то положим $t = 1$.
2. Иначе возьмём $t = 0$.

Оба случая дают требуемое условие на u. □

Утверждение 1.22. *$g+pt$ - искомый первообразный корень по модулю p^α (то есть он одинаков для всех α).*

Доказательство. Показатель первообразного корня всегда совпадает с функцией Эйлера от модуля по определению. В нашем случае это будет

$$\delta = \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$$

Понятно, что раз $(g+pt)^\delta \equiv 1 \pmod{p^\alpha}$, то и $(g+pt)^\delta \equiv 1 \pmod{p}$. Отсюда следует, что $(p-1) \mid \delta$, то есть δ может иметь лишь вид

$$\delta = p^k(p-1),\ k \in \{0, \ldots, \alpha-1\}$$

Остаётся посмотреть на степени $g+pt$, соответствующие кандидатам на δ:

$$(g+pt)^{p-1} = 1 + pu,\ (p,u) = 1$$
$$(g+pt)^{p(p-1)} = (1+pu)^p = 1 + p^2u + p^3v = 1 + p^2 \underbrace{(u+pv)}_{\equiv u \pmod{p}} = 1 + p^2u_1,\ (u_1,p) = 1$$
$$\vdots$$
$$(g+pt)^{p(p^{k-1}(p-1))} = (1+p^k u_{k-1})^p = 1 + p^{k+1}u_k,\ (u_k,p) = 1$$

Подставим $k = \alpha - 1$. Тогда

$$(g + pt)^{p^{\alpha-1}(p-1)} = 1 + p^{\alpha} u_{\alpha-1},\ (u_{\alpha-1}, p) = 1$$

Следовательно, только начиная с $k = \alpha - 1$ будет возможно, что

$$(g + pt)^k \equiv 1 \pmod{p}$$

□

□

Теорема 1.13. *Для любого $\alpha \geqslant 1$ первообразный корень по модулю $2p^{\alpha}$ тоже существует, если p - нечётное простое число.*

Доказательство. Заметим, что $\varphi(2p^{\alpha}) = \varphi(p^{\alpha})$. Пусть g - первообразный корень по модулю p^{α}. Тогда есть 2 варианта:

1. Если g - нечётное число, то $(g, 2p^{\alpha}) = 1$ и применима теорема Эйлера:
$$g^{\varphi(2p^{\alpha})} \equiv 1 \pmod{2p^{\alpha}}$$
2. Иначе нам подойдёт число $g + p^{\alpha}$, которое остаётся первообразным корнем по модулю p^{α} и к нему уже применима теорема Эйлера.

□

Теорема 1.14. *(не входит в программу) Первообразные корни существуют только по модулям 2, 4, p^{α} и $2p^{\alpha}$ для $\alpha \geqslant 1$ и p - простого нечётного числа.*

1.5 Диофантовы приближения

Замечание. В этом параграфе натуральные числа считаются от единицы, если не указано

Диофантовы приближения - это область математики, которая изучает приближение иррациональных чисел при помощи рациональных. Более точно, то для числа $\alpha \in \mathbb{R}\backslash\mathbb{Q}$ мы исследуем дроби p/q и функции $\psi\colon \mathbb{N} \to \mathbb{N}$ такие, что выполнено неравенство

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{\psi(q)}$$

Теорема 1.15. *(Дирихле) Для $\forall \alpha \in \mathbb{R}\backslash\mathbb{Q}$ существует последовательность рациональных дробей $\frac{p}{q}$ таких, что*

1. $\left|\alpha - \frac{p_i}{q_i}\right| < \frac{1}{q_i^2}$
2. $\left|\alpha - \frac{p_{i+1}}{q_{i+1}}\right| < \left|\alpha - \frac{p_i}{q_i}\right|$

Доказательство.

1. Зафиксируем число $Q \in \mathbb{N}$. Разобьём отрезок $[0;1]$ на Q отрезков, то есть длина каждого - $1/Q$. Рассмотрим **дробные доли** $\{\alpha x\}$ при $x \in \{0, \dots, Q\}$. По принципу Дирихле
$$\exists x_1, x_2 \colon x_1 > x_2,\ |\{\alpha x_1\} - \{\alpha x_2\}| \leqslant \frac{1}{Q}$$
Распишем дробные части через целые:
$$|\alpha x_1 - [\alpha x_1] - \alpha x_2 + [\alpha x_2]| \leqslant \frac{1}{Q}$$
Перепишем модуль в несколько ином виде:
$$|\alpha(x_1 - x_2) - ([\alpha x_1] - [\alpha x_2])| \leqslant \frac{1}{Q}$$
Теперь обозначим $q := x_1 - x_2 \leqslant Q$, $p := [\alpha x_1] - [\alpha x_2]$. В новых обозначениях неравенство принимает вид
$$|\alpha q - p| \leqslant \frac{1}{Q}$$
Поделим обе части на q:
$$\left|\alpha - \frac{p}{q}\right| \leqslant \frac{1}{qQ} \leqslant \frac{1}{q^2}$$
2. Покажем наличие следующей дроби для данной. Рассмотрим $Q_1 \in \mathbb{N}$: $1/Q_1 < |\alpha - p/q|$. По нему найдём соответствующие p_1, q_1 ($q_1 \geqslant 1$). Отсюда
$$\left|\alpha - \frac{p_1}{q_1}\right| \leqslant \frac{1}{q_1 Q_1} \leqslant \frac{1}{Q_1} < \left|\alpha - \frac{p}{q}\right|$$

□

Конечные цепные дроби

Определение 1.14. Пусть есть числа $\{a_0, a_1, \dots, a_n\}$, где $a_0 \in \mathbb{Z}, a_i \in \mathbb{N}$. Тогда назовём *конечной цепной дробью* следующее выражение:
$$[a_0; a_1, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}}$$

Числа $a_0, \dots, a_n$ называются *элементами цепной дроби*, они же *неполные частные*. Более формально, можно определить цепную дробь через индукцию:

- $[a_0] = \dfrac{a_0}{1}$
- $[a_0; a_1, \dots, a_n] = a_0 + \dfrac{1}{[a_1; a_2, \dots, a_n]} = a_0 + \dfrac{1}{p/q} = \dfrac{a_0 p + q}{p}$

Определение 1.15. Назовём дробь, соответствующую цепной дроби $[a_0; a_1, \ldots, a_k] = p_k/q_k$ - *подходящей*.

Замечание. В процессе приведения цепной дроби к виду p/q мы **ничего не сокращаем**. Такой шаг позволяет нам точно приравнивать числители и знаменатели, исходя из определения подходящей дроби.

Теорема 1.16. *Для подходящих дробей числа* $[a_0; a_1, \ldots, a_k]$ *верны рекуррентные соотношения:*

$$\begin{cases} p_{k+2} = a_{k+2}p_{k+1} + p_k \\ q_{k+2} = a_{k+2}q_{k+1} + q_k \end{cases}$$

Доказательство. Проведём индукцию по k:

▷ База $k = 0$: для дроби $[a_0; a_1, \ldots, a_n]$ должны быть выполнены соотношения:

$$\begin{cases} p_2 = a_2p_1 + p_0 \\ q_2 = a_2q_1 + q_0 \end{cases}$$

где $p_0 = a_0, q_0 = 1$, а p_1, q_1 найдём из записи числа $[a_0; a_1]$:

$$[a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0a_1 + 1}{a_1}$$

Отсюда $p_1 = a_0a_1 + 1$, $q_1 = a_1$. Осталось разобраться с p_2, q_2:

$$[a_0; a_1, a_2] = a_0 + \frac{1}{[a_1; a_2]} = a_0 + \frac{a_2}{a_1a_2 + 1} = \frac{a_0a_1a_2 + a_0 + a_2}{a_1a_2 + 1} = \frac{p_2}{q_2}$$

Подставим все найденные величины в потенциальные равенства:

$$\begin{cases} a_0a_1a_2 + a_0 + a_2 = a_2(a_0a_1 + 1) + a_0 \\ a_1a_2 + 1 = a_2a_1 + 1 \end{cases}$$

Верность очевидна.

▷ Переход $k > 0$:

$$[a_0; a_1, \ldots, a_k] = a_0 + \frac{1}{[a_1; a_2, \ldots, a_k]}$$

К дроби $[a_1; a_2, \ldots, a_k]$ примени́мо предположение индукции. Будем обозначать подходящие к ней, через p'/q'. Более точно

$$[a_1; a_2, \ldots, a_i] =: \frac{p'_{i-1}}{q'_{i-1}}$$

Подставим дробь вместо $[a_1; a_2, \ldots, a_k]$:

$$[a_0; a_1, \ldots, a_k] = a_0 + \frac{q'_{k-1}}{p'_{k-1}} = \frac{a_0p'_{k-1} + q'_{k-1}}{p'_{k-1}} = \frac{p_k}{q_k}$$

Отсюда можно получить другую рекуррентную систему, которая тоже верна

$$\begin{cases} p_i = a_0 p'_{i-1} + q'_{i-1} \\ q_i = p'_{i-1} \end{cases}$$

По предположению индукции имеем

$$\begin{cases} p'_{k-1} = a_k p'_{k-2} + p'_{k-3} \\ q'_{k-1} = a_k q'_{k-2} + q'_{k-3} \end{cases}$$

Подставляя p'_{i-1}, q'_{i-1}, выраженные через первую систему, во вторую, получим требуемое:

$$\begin{cases} q_k = a_k q_{k-1} + q_{k-2} \\ p_k = a_k p_{k-1} + p_{k-2} + a_0(q_k - a_k q_{k-1} - q_{k-2}) = a_k p_{k-1} + p_{k-2} \end{cases}$$

□

Следствие. Домножим первое выражение на q_{k+1}, а второе на p_{k+1} и вычтем одно из другого:

$$q_{k+1}p_{k+2} - p_{k+1}q_{k+2} = p_k q_{k+1} - q_k p_{k+1}$$

Попробуем последовательно вычислить данное соотношение:

$$\begin{aligned} &p_0 q_1 - q_0 p_1 = a_0 a_1 - 1(a_0 a_1 + 1) = -1 \\ &p_1 q_2 - q_1 p_2 = -(p_0 q_1 - q_0 p_1) = 1 \\ &\vdots \end{aligned}$$

Или же сразу

$$p_k q_{k+1} - q_k p_{k+1} = (-1)^{k+1}$$

Следствие. Из доказанного выше следует, что $\forall k \in \mathbb{N} \cup \{0\}$ p_k/q_k - несократимая дробь. Действительно, ведь если $(p_k, q_k) \neq 1$, то $(-1)^{k+1}$ должно делиться на этот НОД. Значит, возможен лишь один вариант - они взаимно просты.

Замечание. Перепишем равенство из следствия с следующем виде:

$$\frac{p_k}{q_k} - \frac{p_{k+1}}{q_{k+1}} = \frac{(-1)^{k+1}}{q_k q_{k+1}}$$

А теперь то же самое сделаем для дробей, отличающихся по номеру на 2:

$$p_{k+2}q_k - q_{k+2}p_k = a_{k+2}(p_{k+1}q_k - q_{k+1}p_k) \Leftrightarrow \frac{p_{k+2}}{q_{k+2}} - \frac{p_k}{q_k} = \frac{(-1)^k a_k}{q_k q_{k+2}}$$

Если k - нечётный номер, то в первом равенстве справа стоит положительное число, то есть дробь p_k/q_k больше следующей. Из второго равенства следует, что дроби с чётными номерами возрастают, а с нечётными - убывают. В общей картине это означает, что чётные дроби приближаются к α строго слева, а нечётные - строго справа.

Сюда бы картинку числовой прямой, где слева отмечены дроби с чётными номерами, а справа - с нечётными.

Если рассмотреть подходящие дроби как приближение к числу α (пока рациональному, но то же верно и для иррациональных), то для разности верна оценка:

$$\left|\alpha - \frac{p_k}{q_k}\right| \leqslant \left|\frac{p_{k+1}}{q_{k+1}} - \frac{p_k}{q_k}\right| = \left|\frac{p_{k+1}q_k - q_{k+1}p_k}{q_k q_{k+1}}\right| = \frac{1}{q_k q_{k+1}} \leqslant \frac{1}{q_k^2}$$

Бесконечные цепные дроби

Определение 1.16. Назовём число $\alpha = [a_0; a_1, \ldots, a_n, \ldots]$ *бесконечной цепной дробью*, если

$$\exists \lim_{k\to\infty} [a_0; a_1, \ldots, a_k] = \alpha$$

Теорема 1.17. *Если $\forall i \in \mathbb{N}_0$ $a_i \in \mathbb{N}$, то предел всегда существует.*

Доказательство. Так как мы имеем дело с последовательностью подходящих дробей, то верны все утверждения и теоремы, которые мы доказали выше. В частности, последовательность подходящих дробей с чётными номерами возрастает, но ограничена сверху через $p1/q1$. Значит, по теореме Вейерштрасса о монотонной последовательности существует предел. Аналогично с нечётными, и из обоих утверждений уже следует требуемое. □

Утверждение 1.23. *Любое число $\alpha \in \mathbb{R}$ можно представить в виде цепной дроби.*

Доказательство. Представим число α как сумму целой и дробной частей:

$$\alpha = \lfloor\alpha\rfloor + \{\alpha\}$$

Возможно 2 варианта:

1. $\{\alpha\} = 0$. В таком случае алгоритм разложения закончен.
2. $\{\alpha\} \neq 0$. Тогда сделаем шаг рекурсии:

$$\alpha = \lfloor\alpha\rfloor + \frac{1}{1/\{\alpha\}}$$

Теперь нужно рекурсивно разложить $1/\{\alpha\}$.

□

Замечание. Если какая-то последовательность подходящих дробей имеет предел, равный α, то эти дроби совпадают с построенным в утверждении разложением. Доказывается индукцией по k.

Определение 1.17. *Периодической цепной дробью* назовём дробь α вида

$$\alpha = [a_0; a_1, \ldots, a_n, (b_1, \ldots, b_k)]$$

где $(b_1, \ldots, b_k)$ - период, который бесконечно повторяется.

Пример. Рассмотрим периодическую цепную дробь $\alpha = [1;(1)] > 1$. Что это за число?

$$[1;(1)] = 1 + \frac{1}{[1;(1)]} \Rightarrow \alpha = 1 + \frac{1}{\alpha}$$

Решив это уравнение, получим следующее значение:

$$\alpha = \frac{1+\sqrt{5}}{2} = \varphi$$

Определение 1.18. *Квадратичной иррациональностью* называется иррациональное число, которое является корнем квадратного уравнения.

Пример. $\sqrt{2}$ - квадратичная иррациональность. Является одним из корней уравнения $x^2 = 2$.

Утверждение 1.24. *Если α - квадратичная иррациональность, $v \in \mathbb{N}$, то α^{-1}, $\alpha + v$ - тоже квадратичные иррациональности.*

Доказательство. Для доказательства достаточно предъявить квадратные уравнения, где эти числа являются корнями. По условию есть $a, b, c \in \mathbb{R}$ такие, что

$$a\alpha^2 + b\alpha + c = 0$$

Для $1/\alpha$ нужно найти аналогичные $d, e, f \in \mathbb{R}$ такие, что

$$d\frac{1}{\alpha^2} + e\frac{1}{\alpha} + f = \frac{d + e\alpha + f\alpha^2}{\alpha^2} = 0$$

То есть видно, что нужно положить $f = a$, $e = b$, $c = d$ соответственно. Аналогичным образом поступаем и с $\alpha + v$:

$$d'(\alpha+v)^2 + e'(\alpha+v) + f' = d'\alpha^2 + \alpha(2d'v + e') + d'v^2 + e'v + f' = 0$$

Отсюда получаем систему уравнений, которая очевидным образом разрешима:

$$\begin{cases} d' = a \\ 2d'v + e' = b \\ d'v^2 + e'v + f' = c \end{cases}$$

□

Утверждение 1.25. *Периодическая цепная дробь α является квадратичной иррациональностью.*

Доказательство. Пусть $\alpha = [a_0; a_1, \ldots, a_m, (b_1, \ldots, b_k)]$. Обозначим за β следующее число:

$$\beta = [0; (b_1, \ldots, b_k)] = \cfrac{1}{b_1 + \cfrac{1}{\ldots + \cfrac{1}{b_k + \beta}}}$$

Несложно показать по индукции, что эту дробь можно развернуть и получить уравнение

с некоторыми известными $a, b, c, d \in \mathbb{Z}$:

$$\frac{a\beta + b}{c\beta + d} = \beta$$

Его существования уже достаточно, чтобы заключить, что β - квадратичная иррациональность, откуда следует по тем же индуктивным соображениям квадратичная иррациональность α. □

Теорема 1.18. *(без доказательства) α - квадратичная иррациональность тогда и только тогда, когда α раскладывается в периодическую цепную дробь.*

Открытой проблемой остаётся вопрос о кубической иррациональности - об устройстве таких цепных дробей известно крайне мало.

Гипотеза 2. *$\forall p$ - простого числа, существует $a \leqslant p-1$ такое, что все неполные частные цепной дроби $\frac{a}{p}$ ограничены константой 5.*

Замечание. Данная гипотеза имеет большое значение в вычислении определённых интегралов «по сеточкам». Компьютерные данные говорят, что она работает, но доказать пока удалось лишь ограниченность сверху через $\ln p$.

Определение 1.19. Число называется *алгебраическим*, если оно является корнем уравнения, задаваемого многочленом с целыми коэффициентами.

Множество этих чисел обозначается как $\mathbb{A}$

$$a \in \mathbb{A} \Leftrightarrow \exists P \in \mathbb{Z}[x] \;\Big|\; P(a) = 0$$

Замечание. Без доказательства отметим, что множество алгебраических чисел $\mathbb{A}$ образует поле.

Определение 1.20. Любое число, не являющееся алгебраическим, называется *трансцендентным.*

Замечание. Алгебраических чисел в рамках действительных крайне мало - счётное число.

Определение 1.21. *Степень алгебраического числа* - это минимальная степень уравнения, корнем которого это число является.

Теорема 1.19. *(Лиувилля) Для любого $\alpha \in (\mathbb{A}\backslash\mathbb{Q}) \cap \mathbb{R}$ степени $d(\alpha)$ существует $c = c(\alpha) > 0$ такое, что*

$$\forall p, q \in \mathbb{Z} \;\; \left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q^d}$$

Замечание. Суть теоремы состоит в том, что алгебраические числа нельзя слишком хорошо аппроксимировать.

Доказательство. Разберём несколько случаев:

1. Пусть p и q таковы, что $|\alpha - p/q| \geqslant 1$. Тогда очевидным образом

$$\left|\alpha - \frac{p}{q}\right| \geqslant \frac{1}{q^d}$$

2. Теперь $|\alpha - p/q| < 1$. Пусть многочлен $f(x)$, имеющий вид

$$f(x) = a_d x^d + \ldots + a_0$$

является минимальным многочленом, корнем которого служит α. Согласно основной теореме алгебры, у $f(x) = 0$ будет ровно d корней $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_d$ (при этом α_i может быть комплексным, без проблем).

Утверждение 1.26. *У $f(x)$ нет рациональных корней*

Доказательство. Действительно, если он есть, то, разложив многочлен на линейные сомножители, скобка с таким корнем при подстановке α не обнулится - следовательно, на неё можно «сократить» и останется многочлен степени $d-1$, что противоречит с условием. □

Ради интереса, подставим p/q в f:

$$0 \neq f(p/q) = a_d(p/q)^d + \ldots + a_1(p/q) + a_0 = \frac{h}{q^d}$$

где h - целое число. То есть $|f(p/q)| \geqslant 1/q^d$. С другой стороны, распишем это же значение, но в разложенном виде:

$$f(p/q) = a_d(p/q - \alpha) \cdot \prod_{\tau=2}^{d}(p/q - \alpha_\tau)$$

Снова оценим модуль:

$$\frac{1}{q^d} \leqslant |f(p/q)| = |a_d| \cdot \left|\alpha - \frac{p}{q}\right| \cdot \prod_{\tau=2}^{d}\left(\left|\alpha_\tau - \frac{p}{q}\right|\right) \leqslant$$

$$|a_d| \cdot |\alpha - p/q| \cdot \prod_{\tau=2}^{d}(|\alpha_\tau - \alpha| + \underbrace{|\alpha - p/q|}_{<1}) < |\alpha - p/q| \cdot \underbrace{\left(|a_d| \cdot \prod_{\tau=2}^{d}(|\alpha_\tau - \alpha| + 1)\right)}_{1/c(\alpha)}$$

□

Теорема 1.20. *Для любой функции $\psi(q)$ такой, что ψ монотонно стремится к бесконечности, существует число α такое, что найдётся последовательность $\{p_n/q_n\}_{n=1}^{\infty}$ со свойством:*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n \cdot \psi(q_n)}$$

Замечание. Теорема описывает собою конструкцию трансцендентного числа для любой скорости приближения.

Доказательство. Будем строить цепную дробь α индуктивно при помощи подходящих дробей.

1. База - произвольное рациональное число, разложенное в цепную дробь $[a_0; a_1, \ldots, a_k]$, для подходящих дробей которого выполнено условие (такое точно есть, ибо можно просто взять целое число).

2. Переход $n > k$ - пусть мы узнали $n+1$ число в разложении α, то есть

$$\alpha = [a_0; a_1, \ldots, a_n, \ldots]$$

Понятно, что $p_n/q_n = [a_0; a_1, \ldots, a_n]$. При этом мы можем гарантировать индуктивное неравенство Дирихле, следующее из свойств подходящих дробей:

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q_n q_{n+1}} = \frac{1}{q_n(a_{n+1}q_n + q_{n-1})}$$

где a_{n+1} - число, которое мы хотим найти. При этом мы хотим соблюсти другое неравенство:

$$\frac{1}{q_n(a_{n+1}q_n + q_{n-1})} < \frac{1}{q_n\psi(q_n)}$$

Отсюда можно получить явное неравенство на a_{n+1} и, соответственно, можно выбрать a_{n+1} из подходящих чисел.

□

Теорема 1.21. *(без доказательства, Рота, 50-е годы XX в.)* $\forall \alpha \in (\mathbb{A}\backslash\mathbb{Q}) \cap \mathbb{R}$ *выполнено утверждение:*

$$\forall \varepsilon > 0 \ \exists c > 0 \colon \left|\alpha - \frac{p}{q}\right| \geqslant \frac{c}{q^{2+\varepsilon}}$$

Теорема 1.22. *(без доказательства)* $\forall \alpha \in \mathbb{R}$ *существует* $\{p_n/q_n\}_{n=1}^{\infty}$ *такая, что*

$$\left|\alpha - \frac{p_n}{q_n}\right| \leqslant \frac{1}{q^2\sqrt{5}}$$

Замечание. То есть последняя теорема представляет собой улучшение результата Дирихле на коэффициент $\sqrt{5}$. Если при этом убрать из рассмотрения числа, которые линейно выражаются через $\varphi = [1; (1)]$, то оценку можно улучшить до $\sqrt{8}$. Улучшать можно и дальше, если выкидывать числа, для которых оценка достигается. Доказано, что тогда выражение справа будет стремиться к $1/3$.

Теорема 1.23. *Число Эйлера* e *- иррациональное.*

Доказательство. Пока поверим, что

$$e = \sum_{k=0}^{\infty} \frac{1}{k!}$$

Предположим, что $e = a/n$ для некоторых $a \in \mathbb{Z}$, $n \in \mathbb{N}$. С одной стороны, очевидно,

$en! \in \mathbb{Z}$. С другой стороны,

$$en! = A + \frac{n!}{(n+1)!} + \frac{n!}{(n+2)!} + \ldots = A + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \ldots = A + \frac{1}{n+1}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots\right)$$

где $A \in \mathbb{Z}$, а сумма в скобках

$$1 < 1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots < 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$$

То есть

$$0 < \frac{1}{n+1}\left(1 + \frac{1}{n+2} + \frac{1}{(n+2)(n+3)} + \ldots\right) < \frac{2}{n+1} \leqslant \frac{2}{2} = 1$$

Получили, что $en!$ не целое число. Противоречие. □

Теорема 1.24. *Числа Эйлера e - трансцендентное.*

Лемма 1.4. *(тождество Эрмита) Пусть $f(t) = b_\nu t^\nu + \ldots + b_1 t + b_0$, где $b_i \in \mathbb{R}$. Утверждается, что*

$$\int_0^x f(t)e^{-t}dt = F(0) - F(x)e^{-x}$$

где $F(x) = f(x) + f'(x) + \ldots + f^{(\nu)}(x)$

Доказательство. Рассмотрим следующий интеграл от многочлена $f(t)$:

$$\int_0^x f(t)e^{-t}dt = -\int_0^x f(t)d(e^{-t}) = -f(t)e^{-t}|_0^x + \int_0^x f'(t)e^{-t}dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t}dt$$

Рекурсивно вычислим оставшийся интеграл. В итоге получится следующее выражение:

$$\int_0^x f(t)e^{-t}dt = \underbrace{f(0) - f(x)e^{-x} + f'(0) - f'(x)e^{-x} + \ldots + f^{(\nu)}(0) - f^{(\nu)}(x)e^{-x}}_{F(0)-F(x)e^{-x}} + \underbrace{\int_0^x f^{(\nu+1)}(t)e^{-t}dt}_{0}$$

□

Доказательство. (трансцендентности) Предположим, что e - не трансцендентное. Это значит существование многочлена $g(x)$, для которого e - это корень:

$$g(x) = a_m x^m + \ldots + a_1 x + a_0$$

Перепишем тождество Эрмита для $x = k \in \{0, m, \ldots,\}$ в следующем виде:

$$e^k F(0) - F(k) = e^k \int_0^k f(t)e^{-t}dt$$

Определим для числа $n \in \mathbb{N}$ многочлен $f(x)$:

$$f(x) = \frac{1}{(n-1)!} x^{n-1} \big((x-1) \cdot \ldots \cdot (x-m)\big)^n$$

Теперь, рассмотрим следующую сумму для нашего $f(x)$ (n выберем позже):

$$\sum_{k=0}^{m} a_k (e^k F(0) - F(k)) = F(0) \underbrace{\sum_{k=0}^{m} a_k e^k}_{0} - \sum_{k=0}^{m} a_k F(k) = \sum_{k=0}^{m} a_k e^k \int_0^k f(t) e^{-t} dt$$

Чтобы посчитать $F(k)$, нам нужно посчитать все $\nu := n - 1 + nm$ производные в целых точках:

▷ Производные в нуле

1. Для $\mu \in \{0, \ldots, n-2\}$ верно, что

$$f^{(\mu)}(0) = 0$$

так как за одно дифференцирование степень каждого слагаемого в производной уменьшается лишь на 1.

2. Производная в нуле при $\mu = n-1$ получается лишь из того слагаемого, где всегда брали производную лишь от x^{n-1}. То есть

$$f^{(n-1)}(0) = (-1)^{mn} (m!)^n$$

3. $\mu \geqslant n$. Тут уже конкретное значение производной сложно узнать. Тем не менее, можно заключить следующее:

$$f^{(\mu)}(0) = nB,\ B \in \mathbb{Z}$$

▷ Производные для $k \in \{1, \ldots, m\}$

1. Для $\mu \in \{0, \ldots, n-1\}$ очевидно

$$f^{(\mu)}(k) = 0$$

2. Для $\mu \geqslant n$ скажем то же, что и в последнем пункте про производные в нуле:

$$f^{(\mu)}(k) = nC,\ C \in \mathbb{Z}$$

Посчитав производные, мы можем вычислить сумму:

$$\sum_{k=0}^{m} a_k F(k) = a_0 F(0) + \sum_{k=1}^{m} a_k F(k) = a_0 (-1)^{mn} (m!)^n + a_0 nD + nE \equiv a_0 (-1)^{mn} (m!)^n \pmod{n}$$

Выберем такое n, что $n > |a_0|$ и $(n, m!) = 1$. Тогда гарантированно можем заявить следу-

ющее:

$$\left| -\sum_{k=0}^{m} a_k F(k) \right| \geqslant 1$$

Если мы докажем, что правая часть исходного равенства стремится к нулю при $n \to \infty$, то мы получим необходимое противоречие. Рассмотрим эту часть:

$$\left| \sum_{k=0}^{m} a_k e^k \int_0^k f(t) e^{-t} dt \right| \leqslant \sum_{k=0}^{m} |a_k| e^k \int_0^k |f(t)| e^{-t} dt$$

Оценим модуль $|f(t)|$. Заметим, что

$$\forall t \in [0; m] \ \forall i \in \{0, \ldots, m\} \ \ |t - i| \leqslant m$$

Отсюда следует

$$\sum_{k=0}^{m} |a_k| e^k \int_0^k |f(t)| e^{-t} dt \leqslant \sum_{k=0}^{m} |a_k| e^k \int_0^k \frac{1}{(n-1)!} m^{mn+n-1} e^{-t} dt =$$

$$\frac{1}{(n-1)!} m^{mn+n-1} \sum_{k=0}^{m} |a_k| e^k \left(\frac{1}{e^0} - \frac{1}{e^k} \right) \leqslant \frac{1}{(n-1)!} \underbrace{m^{mn+n-1} \sum_{k=0}^{m} |a_k| e^k}_{C^n \cdot C'} \xrightarrow[n \to \infty]{} 0$$

□

Теорема 1.25. *(без доказательства) Число Пи π - трансцендентное.*

Теорема 1.26. *(Гельфонда, 1929г., одна из проблем Гильберта. Без доказательства) Если $\alpha, \beta \in \mathbb{A}$, $\alpha \notin \{0, 1\}$, $\beta \notin \mathbb{Q}$, то $\alpha^\beta \notin \mathbb{A}$.*

Следствие. $e^\pi \notin \mathbb{A}$ - тоже трансцендентное число.

Доказательство. Предположим, что $e^\pi \in \mathbb{A}$. Но заметим, что $i \in \mathbb{A} \backslash \mathbb{Q}$:

$$(e^\pi)^i = e^{i\pi} = -1 \in \mathbb{A}$$

Получили противоречие с теоремой Гельфонда. □

Определение 1.22. Числа x, y называются *алгебраически независимыми*, если для любого многочлена P выполнено неравенство:

$$P(x, y) \neq 0$$

Теорема 1.27. *(Нестеренко. Без доказателсьтва) Числа $\pi, e^\pi, \Gamma(1/4)$ алгебраически независимы. $\Gamma(x)$ - обобщение факториала на всю действительную числовую прямую.*

1.6 Решётки в $\mathbb{R}^n$

Замечание. Зафиксируем линейно независимые вектора $\vec{a}_1, \ldots, \vec{a}_k \in \mathbb{R}^n$.

Определение 1.23. *Решёткой* Λ в пространстве $\mathbb{R}^n$ будем называть следующее множество векторов:

$$\Lambda = \{b_1\vec{a}_1 + \ldots + b_n\vec{a}_k \mid \forall i\ b_i \in \mathbb{Z}\}$$

Определение 1.24. Вектора $\vec{a}_1, \ldots, \vec{a}_k$ также можно назвать *базисом решётки* Λ.

Замечание. Базис в Λ, понятное дело, определён неоднозначно. Тем не менее, матрица перехода от базиса к базису должна быть целочисленной, а следовательно, её детерминант - это ± 1. Отсюда вытекает следующее определение:

Определение 1.25. *Определителем решётки* называется модуль детерминанта матрицы

$$\det\Lambda = \left|\det\begin{pmatrix}\alpha_1 & \cdots & \alpha_k\end{pmatrix}\right|, \quad \vec{a}_i \leftrightarrow_e \alpha_i$$

где e - ортонормированный базис

Замечание. В $\mathbb{R}^2$ $\det\Lambda$ символизирует объём параллелограмма, натянутого на базисные вектора решётки. В $\mathbb{R}^3$ - объём соответственно.

Определение 1.26. Множество $\Omega \subset \mathbb{R}^2$ называется *выпуклым*, если для любых двух точек из этого множества отрезок, соединяющих их, тоже лежит в этом множестве.

Определение 1.27. Зафиксируем ПДСК на плоскости. Будем называть множество $F \subset \mathbb{R}^2$ *простым*, если оно представляет собой совокупность прямоугольников, чьи стороны параллельны осям.

Определение 1.28. *Площадь простой фигуры* F - это просто сумма площадей прямоугольников, её составляющих.

Определение 1.29. Будем говорить, что множество $\Omega \subset \mathbb{R}^2$ обладает *площадью* S, если выполнено условие:

$$\mu_*(\Omega) = \mu^*(\Omega)$$

где $\mu_*(\Omega) = \sup\limits_{F\subset\Omega} S(F)$, $\mu^*(\Omega) = \inf\limits_{\Omega\subset F} S(F)$

Замечание. Величина S является частным случаем *меры Жордана*.

Теорема 1.28. *(Минковского) Пусть* $\Omega \subset \mathbb{R}^2$, $S(\Omega) > 4$, S *- выпукло и центрально симметрично относительно центра ПДСК. Тогда*

$$(\Omega \cap \mathbb{Z}^2)\backslash\{0\} \neq \varnothing$$

Доказательство. Здесь стоит вообразить картинку некоторого овала, покрытого сеточкой Рассмотрим решётку $(1/p)\mathbb{Z}^2$, $p \in \mathbb{N}$. Обозначим за N_p - количество точек в пересечении этой решётки с Ω:

$$N_p := \left|\frac{1}{p}\mathbb{Z}^2 \cap \Omega\right|$$

Без доказательства поверим, что если мы возьмём площади квадратиков, у которых левой верхней вершиной выступает точка из N_p, то эта площадь будет стремиться в $S(\Omega)$:

$$N_p \cdot \frac{1}{p^2} \xrightarrow[p\to\infty]{} S(\Omega) > 4$$

Следовательно

$$\exists P \in \mathbb{N} \mid \forall p \geqslant P \quad N_p \cdot \frac{1}{p^2} > 4$$

Это можно записать в несколько другом виде:

$$N_p > (2p)^2$$

Как задаётся любая точка в решётке $(1/p)\mathbb{Z}^2$? Её координаты будут иметь вид

$$\vec{v} \leftrightarrow_e (v_1/p,\, v_2/p)^T,\ v_1, v_2 \in \mathbb{Z}$$

Из неравенства на N_p по принципу Дирихле следует, что

$$\exists \vec{a}, \vec{b} \in \Omega \mid a_1 \equiv b_1 \pmod{2p}, \quad a_2 \equiv b_2 \pmod{2p}$$

Теперь мы можем рассмотреть точку $\vec{c} = (\vec{a} + \vec{b})/2 \neq \vec{0}$. В силу центральной симметрии, $-\vec{b} \in \Omega$, а из-за выпуклости $\vec{c} \in \Omega$. Более того, эта точка - целая, так как

$$a_i - b_i \equiv 0 \pmod{2p}$$

□

Теорема 1.29. *(без доказательства) Пусть $\Omega \subset \mathbb{R}^2$ - выпуклое, центрально симметричное, замкнутое множество. При этом $S(\Omega) \geqslant 4$. Тогда*

$$(\Omega \cap \mathbb{Z}^2) \backslash \{0\} \neq \varnothing$$

Следствие. Следствием уже этой теоремы является геометрическое доказательство теоремы Дирихле.

Пусть $\alpha \in \mathbb{R}\backslash\mathbb{Q}$. Тогда, рассмотрим множество точек $\{(x, y) \colon\ |y - \alpha x| \leqslant 1/Q,\ |x| \leqslant Q\}$, где $Q \in \mathbb{N}$.

Здесь должен быть рисунок, который можно найти в 26й лекции ОКТЧ за 2022й год на моменте 1:03:20

Это множество точек задаёт параллелограмм около прямой $y = \alpha x$, и его площадь $S = (2/Q) \cdot 2Q = 4$. Согласно теореме, внутри него найдётся целая нетривиальная точка (q, p). Повторим операцию, «растянув» параллелограмм до такого состояния, что эта точка уже в него не входит. Очевидно $q \leqslant Q$, а поэтому

$$|p - \alpha q| \leqslant \frac{1}{Q} \leqslant \frac{1}{q}$$

откуда уже возникает знакомое неравенство теоремы Дирихле.

Теорема 1.30. *(Многомерная теорема Минковского) Пусть $\Omega \subset \mathbb{R}^n$ - выпуклое, центрально симметричное множество, $V(\Omega) > 2^n$. Тогда*

$$(\Omega \cap \mathbb{Z}^2) \backslash \{0\} \neq \varnothing$$

Доказательство. Абсолютно аналогично случаю на плоскости, просто мера маленького n-мерного гиперкуба теперь $(1/p^n)$. □

Теорема 1.31. *Пусть $\Omega \subset \mathbb{R}^n$ - выпуклое, центрально симметриченое множество. $\Lambda \subset \mathbb{R}^n$ - произвольная решётка, причём $V(\Omega) > 2^n \cdot \det \Lambda$. Тогда*

$$(\Omega \cap \Lambda) \backslash \{0\} \neq \varnothing$$

Доказательство. Тут можно произвести геометрическое доказательство, исходя из элементарной центрально симметричной фигуры, образованной решёткой, чей объём будет в аккурат $2^n \cdot \det \Lambda$. □

Определение 1.30. *Критическим определителем* $\Omega \subset \mathbb{R}^n$ называется следующая величина

$$\Delta(\Omega) := \inf\{\det \Lambda \mid (\Lambda \cap \Omega) \backslash \{0\} = \varnothing\}$$

Теорема 1.32. *(Минковского через критический определитель, без доказательства) Если $\Omega \subset \mathbb{R}^n$ - выпуклое и центрально симметричное множество, то*

$$\frac{V(\Omega)}{\Delta(\Omega)} \leqslant 2^n$$

Теорема 1.33. *(Минковского-Главки, 1945 г., без доказательства) Для любого $\Omega \subset \mathbb{R}^n$ верна оценка*

$$\frac{V(\Omega)}{\Delta(\Omega)} \geqslant 1 - \varepsilon(n)$$

где $\varepsilon(n) \xrightarrow[n\to\infty]{} 0$

Утверждение 1.27. *Эквивалентным определением решётки будет следующее утверждение:*

$\Lambda \subset \mathbb{R}^n$ *- решётка, если она:*

1. *Образует дискретное множество в $\mathbb{R}^n$ (то есть любая точка Λ изолирована). То есть $\exists r \mid \forall \vec{x} \in \mathbb{R}^n$ в шаре с центром $\vec{x}$ и радиуса r не больше одной точки этого множества.*
2. *$\exists R \mid \forall \vec{x} \in \mathbb{R}^n$ в шаре с центром $\vec{x}$ и радиуса R есть хотя бы одна точка этого множества.*
3. *Λ - подгруппа $\mathbb{R}^n$ по сложению.*

Доказательство.

▷ $\Rightarrow$ Из определения решётки 3 свойства очевидны.

▷ $\Leftarrow$ А вот это красиво написать пока не удалось.

□

Определение 1.31. Рассмотрим следующий вектор в $\mathbb{Z}^n$:

$$\vec{a} \leftrightarrow_e \left(\frac{a_1}{q}, \ldots, \frac{a_n}{q}\right)^T, \quad (a_1, \ldots, a_n, q) = 1$$

Тогда, обозначим за $\Lambda_{\vec{a}}$ решётку следующего вида:

$$\Lambda_{\vec{a}} = \{\vec{a}l + \vec{b},\, l \in \mathbb{Z}, \vec{b} \in \mathbb{Z}^n\}$$

$\Lambda_{\vec{a}}$ называется *циклической центрировкой* $\mathbb{Z}^n$. Это связано со следующим фактом:

$$\Lambda_{\vec{a}}/\mathbb{Z}^n = \langle \vec{a} \rangle$$

Замечание. То есть фактически мы взяли все целые точки $\mathbb{Z}^n$ и объединили это множество с другими $\mathbb{Z}^n$, где каждая точка сдвинулась на $\vec{a}l$.

Утверждение 1.28. *Для вектора $\vec{a}$ из определения следует, что*

$$\Lambda_{\vec{a}} \subset \frac{1}{q}\mathbb{Z}^n$$

Теорема 1.34. *(без доказательства) Утверждается, что*

$$\det \Lambda_{\vec{a}} = \frac{1}{q}$$

Напоминание. n-мерный октаэдр обозначается как O^n, в $\mathbb{R}^n$ задаётся уравнением

$$|x_1| + \ldots + |x_n| \leqslant 1$$

и имеет меру, равную

$$V(O^n) = \frac{2^n}{n!}$$

Следствие. Если в O^n нет нетривиальных точек (то есть нуля и его вершин) $\Lambda_{\vec{a}}$, то в каноническом разложении q число простых множителей $\leqslant n$.

Доказательство. По теореме Минковского

$$V(O^n) \leqslant 2^n \cdot \det \Lambda_{\vec{a}}$$

Подставим известные величины и получим следующее неравенство:

$$\frac{2^n}{n!} \leqslant 2^n \cdot \frac{1}{q} \Leftrightarrow q \leqslant n!$$

Разложим q в произведение простых и сделаем самую базовую оценку:

$$1 \cdot \ldots \cdot s \leqslant p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \leqslant n! \Rightarrow s < n$$

□

Теорема 1.35. *В случае n-мерного октаэдра существуте более сильный аналог теоремы Минковского-Главки:*

$$\forall \varepsilon > 0\ \exists n_0 \in \mathbb{N} \mid \forall n \geqslant n_0\ \exists \vec{a} \leftrightarrow_e ((a_1/q), \ldots, (a_n/q))^T$$

такой, что в O^n нет нетривиальных точек $\Lambda_{\vec{a}}$ и при этом

$$\frac{V(O^n)}{\det \Lambda_{\vec{a}}} \geqslant 1 - \varepsilon$$

Доказательство. Для краткости, обозначим множество тривиальных точек буквой T:

$$T = \{0, \pm\vec{e}_1, \ldots, \pm\vec{e}_n\}$$

Для $\varepsilon > 0$ будем искать $\vec{a}$ такой, что $q = p$, где p - простое число. Для начала, найдём способ подсчёта числа нетривиальных точек $\Lambda_{\vec{a}}$ в октаэдре O^n:

Определим характеристическую функцию для $\forall \vec{x} \in \mathbb{Q}^n$:

$$\delta(\vec{x}) := \begin{cases} 1, & \text{если } \vec{x} \in \mathbb{Z}^n \\ 0, & \text{иначе} \end{cases}$$

Теперь распишем величину $|(\Lambda_{\vec{a}} \cap O^n) \backslash T|$:

$$\left|(\Lambda_{\vec{a}} \cap O^n) \backslash T\right| = \sum_{l=1}^{p-1} \left(\sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \backslash T} \delta(\vec{a}l - \vec{x}) \right)$$

Здесь возникает несколько вопросов, на которые необходимо дать ответ:

1. Почему это посчитает ровно те $\vec{x}$, что лежат внутри решётки и октаэдра?

$$\delta(\vec{a}l - \vec{x}) = 1 \Leftrightarrow \vec{a}l - \vec{x} = \vec{b} \in \mathbb{Z}^n \Leftrightarrow \vec{x} = \vec{a}l - \vec{b} \in \Lambda_{\vec{a}}$$

2. Почему достаточно посмотреть $l \in \{1, \ldots, p-1\}$? Вспомним, что решётка - это наложение сдвинутых $\mathbb{Z}^n$. При сдвиге на p они совпадают, а $l = 0$ нам не нужен, так как при таком l единственные точки, которые мы встретим, будут из T.

Описанная выше конструкция даёт мощность для конкретного $\vec{a}$. А теперь мы её расширим, сделав перебор по всем возможным $\vec{a}$:

$$\sum_{a_1=1}^{p} \cdots \sum_{a_n=1}^{p} \sum_{l=1}^{p-1} \left(\sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \backslash T} \delta(\vec{a}l - \vec{x}) \right)$$

В этой сумме будет p^n слагаемых-мощностей $\left|(\Lambda_{\vec{a}} \cap O^n) \backslash T\right|$. Если мы каким-то образом докажем неравенство

$$\frac{1}{p^n} \cdot \sum_{a_1=1}^{p} \cdots \sum_{a_n=1}^{p} \sum_{l=1}^{p-1} \left(\sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \backslash T} \delta(\vec{a}l - \vec{x}) \right) < 1$$

то отсюда будет следовать (так как величина слева - ничто иное чем среднее арифмети-

ческое мощностей по всем $\vec{a}$), что

$$\exists \vec{a} \mid \sum_{l=1}^{p-1} \left(\sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T} \delta(\vec{a}l - \vec{x}) \right) < 1 (\Rightarrow = 0)$$

Такой $\vec{a}$ будет соответствовать лишь одному условию, но у нас есть ещё и второе:

$$\frac{2^n}{n!} \cdot p \geqslant 1 - \varepsilon$$

Итак, зафиксируем $\varepsilon > 0$. Из того факта, что, начиная с некоторого n_0, всегда есть простое число $p \in [n; n + O(n^{0.525})]$, мы можем заявить следующее:

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \mid \forall n \geqslant n_0 \ \exists p\colon \quad \frac{(1-\varepsilon)n!}{2^n} \leqslant p \leqslant \frac{(1-\varepsilon)n!}{2^n} + C \cdot \left(\frac{(1-\varepsilon)n!}{2^n} \right)^{0.525} \leqslant \frac{(1-\varepsilon)n!}{2^n} + \frac{\varepsilon}{2} \cdot \frac{n!}{2^n}$$

То есть

$$1 - \varepsilon \leqslant \frac{2^n}{n!} \cdot p \leqslant 1 - \frac{\varepsilon}{2}$$

Оценка сверху нам нужна, чтобы доказать неравенство выше. Так как знаки суммирования можно переставлять, то

$$\frac{1}{p^n} \cdot \sum_{a_1=1}^{p} \cdots \sum_{a_n=1}^{p} \sum_{l=1}^{p-1} \left(\sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T} \delta(\vec{a}l - \vec{x}) \right) = \frac{1}{p^n} \cdot \sum_{l=1}^{p-1} \sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T} \left(\sum_{a_1=1}^{p} \cdots \sum_{a_n=1}^{p} \delta(\vec{a}l - \vec{x}) \right)$$

Теперь мысленно зафиксируем $l \in \{1, \ldots, p-1\}$ и $\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T$. Распишем $\vec{a}l - \vec{x}$:

$$\vec{a}l - \vec{x} \leftrightarrow_e \left(\frac{a_1 l - x_1}{p}, \ldots, \frac{a_n l - x_n}{p} \right)$$

Заметим, что $(l, p) = 1$. Отсюда по расширенному алгоритму Евклида следует, что

$$\exists! a \in \mathbb{Z}_p \ \exists b \in \mathbb{Z} \mid al + bp = x_i$$

Так как a_i пробегает всю приведённую систему вычетов, то

$$\exists! a_i \mid \exists b_i \in \mathbb{Z} \quad a_i l + b_i p = x_i; \quad a_i l - x_i = -b_i p$$

Значит, будет ровно один набор $\{a_i\}$, на которых дельта станет единицей (вектор $\vec{a}$, которые ему соответствует - искомый). В итоге имеем

$$\frac{1}{p^n} \cdot \sum_{l=1}^{p-1} \sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T} \left(\sum_{a_1=1}^{p} \cdots \sum_{a_n=1}^{p} \delta(\vec{a}l - \vec{x}) \right) = \frac{1}{p^n} \sum_{l=1}^{p-1} \sum_{\vec{x} \in (O^n \cap (1/p)\mathbb{Z}^n) \setminus T} 1$$

Оценим сумму внутри (то есть число векторов $\vec{x}$). Для этого нам потребуются старые рассуждения про меру, применённые в доказательстве теоремы Минковского:

$$\sum_{\vec{x}\in(O^n\cap(1/p)\mathbb{Z}^n)\setminus T} 1 \leqslant |O^n \cap (1/p)\mathbb{Z}^n| = N_p \leqslant \frac{\frac{2^n}{n!}\cdot(1+\frac{2}{p})^n}{1/p^n}$$

Числитель последней дроби - это мера октаэдра, который увеличили в $(1+2/p)$ раз, а знаменатель - это мера, соответствующая одной точке. Соберём всё полученное вместе:

$$\frac{1}{p^n}\sum_{l=1}^{p-1}\sum_{\vec{x}\in(O^n\cap(1/p)\mathbb{Z}^n)\setminus T} 1 \leqslant \frac{p-1}{p^n}\cdot\frac{2^n}{n!}\cdot p^n\cdot\left(1+\frac{2}{p}\right)^n \leqslant$$
$$p\cdot\frac{2^n}{n!}\cdot\left(1+\frac{2}{p}\right)^n \leqslant \frac{n!}{2^n}\left(1-\frac{\varepsilon}{2}\right)\cdot\frac{2^n}{n!}\cdot\left(1+\frac{2^{n+1}}{n!(1-\varepsilon)}\right)^n < \left(1-\frac{\varepsilon}{2}\right)\cdot\left(1+\frac{\varepsilon}{2}\right) < 1$$

Предпоследняя оценка верна для достаточно большого n, это важно отметить. □

1.7 Равномерное распределение последовательностей

Замечание. До конца данной темы, мы будем обозначать последовательность чисел как $(x_n)_{n=0}^{\infty}$. При этом $x_n \in \mathbb{R}$, если не оговорено иного.

Сделано это для того, чтобы за $\{x_n\}$ обозначать здесь дробную часть числа x_n.

Определение 1.32. Последовательность $(x_n)_{n=0}^{\infty}$ называется *равномерно распределённой по модулю* 1, если выполнено следующее:

$$\forall a,b\in[0;1],\ a<b \quad \frac{|\{n\in\{0,\dots,N-1\}\colon \{x_n\}\in[a;b)\}|}{N} \xrightarrow[N\to\infty]{} b-a$$

Замечание. Интуитивное понятие такое: берём первые N чисел, смотрим на дробную часть каждого. Если она попала в полуинтервал $[a;b)$, то учитываем это число, иначе нет.

Утверждение 1.29. *Эквивалентным определением равномерной распределённости будет утверждение*

$$\forall\gamma\in[0;1) \quad \frac{|\{n\in\{0,\dots,N-1\}\colon \{x_n\}<\gamma\}|}{N} \xrightarrow[N\to\infty]{} \gamma$$

Доказательство.

- ▷ Из изначального в новое определение очевидно: просто положим $a=0, b=\gamma$
- ▷ Из нового определения тоже понятно, как получить изначальное: выберем $\gamma_1 = a, \gamma_2 = b$ и вычтем одно множество-индикатор из другого. Если расписать предел доли, то получим ровно $b-a$ в пределе.

□

Пример. Рассмотрим $x_n = \sqrt{n}$. Докажем, что она равномерно распределена, пользуясь эквивалентным определением:

$$x_0,\dots,x_N = \sqrt{0},\dots,\sqrt{N}$$

Сколько среди чисел выше полных квадратов (то есть заведомо попадающих в множество-индикатор, потому что не имеют дробной части)? Их ровно $\left\lfloor \sqrt{N} \right\rfloor + 1$. Какие ещё числа подойдут, если мы зафиксировали γ? Ну, например, те, которые отступили от целого корня вправо не более чем на γ. Значит, если целый корень имел значение k, то нам подойдут также x_n с номерами в полуинтервале $[k^2; (k+\gamma)^2)$. Количество номеров внутри этого полуинтервала не превышает $2k\gamma + \gamma^2$. Более того, их не меньше $2k\gamma + \gamma^2 - 1$ и из-за этого можно сказать, что их $2k\gamma + O(1)$ (Интуитивно это можно понять, если начертить прямую с отметками k^2 и $(k+\gamma)^2$). Теперь, распишем нашу долю:

$$\frac{|n \in \{0, \dots, N-1\} \colon \{x_n\} < \gamma|}{N} = \frac{\sum\limits_{k=0}^{\lfloor \sqrt{N-1} \rfloor} (2k\gamma + O(1))}{N} =$$

$$\frac{2\gamma}{N} \cdot \frac{\lfloor \sqrt{N-1} \rfloor \left(\lfloor \sqrt{N-1} \rfloor + 1 \right)}{2} + \frac{\lfloor \sqrt{N-1} \rfloor \cdot O(1)}{N} =$$

$$\frac{\gamma \lfloor \sqrt{N-1} \rfloor \left(\lfloor \sqrt{N-1} \rfloor + 1 \right)}{N} + O\left(\frac{\left\lfloor \sqrt{N} \right\rfloor}{N} \right) \xrightarrow[N \to \infty]{} \gamma + 0 = \gamma$$

Пример. Рассмотрим $x_n = \lambda^n$, $\lambda < 1$. В таком случае последовательность очевидно не равномерно распределена, так как

$$\lim_{n \to \infty} x_n = 0$$

Пример. Рассмотрим последовательность из предыдущего примера, но с $\lambda > 1$.

1. Пусть нам так повезло, что λ - один из корней квадратного уравнения $x^2 + px + q = 0$ с целыми коэффициентами, причём второй корень $\theta \in (0; 1)$. Рассмотрим последовательность $y_n = \lambda^n + \theta^n$. Она удовлетворяет линейному рекуррентному соотношению вида

   $$y_{n+2} + p y_{n+1} + q y_n = 0$$

   При этом

   $$\begin{cases} y_0 = \lambda^0 + \theta^0 = 2 \in \mathbb{Z} \\ y_1 = \lambda^1 + \theta^1 = -p \in \mathbb{Z} \end{cases}$$

   То есть $y_n \in \mathbb{Z}$ для любого n. Стало быть

   $$\{\lambda^n + \theta^n\} = 0 \Leftrightarrow \{\lambda^n\} = 1 - \theta^n$$

   Значит, при таких условиях x_n не будет равномерно распределённой последовательностью

2. Открытой проблемой на сегодняшний день является случай при $\lambda = (3/2)$. Неизвестно ничего: ни плотность множества дробных частей, ни распределение.

Теорема 1.36. *Последовательность $(x_n)_{n=0}^{\infty}$ равномерно распределена по модулю 1 тогда и только тогда, когда для любой непрерывной на $[0; 1]$ функции f верно следующее:*

$$\frac{1}{N} \sum_{n=0}^{N-1} f(\{x_n\}) \xrightarrow[N \to \infty]{} \int_0^1 f(x) dx$$

Определение 1.33. Функция $g(x)\colon [0;1] \to \mathbb{R}$ называется *ступенчатой*, если её можно описать как

$$g(x) = c_1\mathbb{I}_{[0;a_1)} + c_2\mathbb{I}_{[a_1;a_2)} + \ldots + c_{n+1}\mathbb{I}_{[a_n;1]}$$

где $P\colon 0 = a_0 < a_1 < \ldots < a_n < a_{n+1} = 1$ - разбиение отрезка $[0;1]$, а $\mathbb{I}_{[a;b]}$ — функция-индикатор

Доказательство. 1. Для начала докажем утверждение не для непрерывных функций, а ступенчатых. Если мы как-то докажем, что

$$\frac{1}{N}\sum_{n=0}^{N-1}\mathbb{I}_{[a;b)}(\{x_n\}) \xrightarrow[N\to\infty]{} \int_0^1 \mathbb{I}_{[a;b)}dx = b - a$$

то и общее утверждение про ступенчатую функцию станет очевидным (в силу аддитивности интеграла).

Что из себя представляет выражение слева? На самом деле, это то же самое выражение, что было в равномерном распределении:

$$\frac{1}{N}\sum_{n=0}^{N-1}\mathbb{I}_{[a;b)}(\{x_n\}) = \frac{|\{n \in \{0,\ldots,N-1\}\colon \{x_n\} \in [a;b)\}|}{N}$$

Отсюда уже очевидно следует равносильность утверждений.

2. Для доказательства исходной теоремы, воспользуемся одним утверждением из математического анализа:

Утверждение 1.30. *$\forall\varepsilon > 0$ существуют 2 ступенчатые функции f_1, f_2 такие, что*

$$\forall x\ f_1(x) \leqslant f(x) \leqslant f_2(x);\quad \int_0^1 (f_2(x) - f_1(x))dx \leqslant \varepsilon$$

Аналогично мы можем зажать ступенчатую функцию непрерывными. Теперь мы можем заняться непосредственно доказательством теоремы

▷ $\Rightarrow$ Зафиксируем $\varepsilon > 0$. Тогда, мы можем написать следующую цепочку неравенств:

$$\int_0^1 f(x)dx - \varepsilon \leqslant \int_0^1 f_2(x)dx - \varepsilon \leqslant \left(\varepsilon + \int_0^1 f_1(x)dx\right) - \varepsilon = \lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1} f_1(\{x_n\}) \leqslant$$

$$\underline{\lim_{N\to\infty}}\sum_{n=0}^{N-1} f(\{x_n\}) \leqslant \overline{\lim_{N\to\infty}}\sum_{n=0}^{N-1} f(\{x_n\}) \leqslant$$

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N-1} f_2(\{x_n\}) = \int_0^1 f_2(x)dx \leqslant \int_0^1 f_1(x)dx + \varepsilon \leqslant \int_0^1 f(x)dx + \varepsilon$$

▷ $\Leftarrow$ Нам нужно показать, что

$$\frac{1}{N}\sum_{n=0}^{N-1}\mathbb{I}_{[a;b)}(\{x_n\}) \xrightarrow[N\to\infty]{} b - a$$

Положим $f = \mathbb{I}_{[a;b)}$. Для неё существуют непрерывные g_1, g_2 из утверждения выше. Зафиксируем $a, b \in [0;1]$, $a < b$, $\varepsilon > 0$. Тогда

$$b - a - \varepsilon = \int_0^1 \mathbb{I}_{[a;b)}(x)dx - \varepsilon \leqslant \int_0^1 g_2(x)dx - \varepsilon \leqslant \int_0^1 g_1(x)dx =$$
$$\lim_{N\to\infty} \sum_{n=0}^{N-1} \frac{1}{N} g_1(\{x_n\}) \leqslant \underline{\lim}_{N\to\infty} \sum_{n=0}^{N-1} \mathbb{I}_{[a;b)}(\{x_n\}) \leqslant \frac{1}{N} \sum_{n=0}^{N-1} \mathbb{I}_{[a;b)}(\{x_n\}) \leqslant$$
$$\overline{\lim}_{N\to\infty} \sum_{n=0}^{N-1} \mathbb{I}_{[a;b)}(\{x_n\}) \leqslant \lim_{N\to\infty} \sum_{n=0}^{N-1} g_2(\{x_n\}) = \int_0^1 g_2(x)dx \leqslant \int_0^1 g_1(x)dx + \varepsilon \leqslant b - a + \varepsilon$$

□

Следствие. Последовательность $(x_n)_{n=0}^{\infty}$ равномерно распределена по модулю 1 тогда и только тогда, когда для любой интегрируемой по Риману на $[0;1)$ функции f верно следующее:

$$\frac{1}{N} \sum_{n=0}^{N-1} f(\{x_n\}) \xrightarrow[N\to\infty]{} \int_0^1 f(x)dx$$

Следствие. Последовательность $(x_n)_{n=0}^{\infty}$ равномерно распределена тогда и только тогда, когда для любой комплекснозначной функции f, которая периодична с периодом 1 верно, что

$$\frac{1}{N} \sum_{n=0}^{N-1} f(x_n) \xrightarrow[N\to\infty]{} \int_0^1 f(x)dx$$

где интеграл - это надо взять отдельно интеграл от реальной и мнимой части, интеграл мнимой части домножить на i и сложить с реальной.

Следствие. (из последнего следствия) Если $(x_n)_{n=0}^{\infty}$ равномерно распределена, то

$$\forall m \in \mathbb{Z}\backslash\{0\} \quad \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i m x_n} \xrightarrow[N\to\infty]{} 0$$

Доказательство. Понятно, что $f(x) = e^{2\pi i m x_n}$ - периодическая комплекснозначная функция с периодом 1. Тогда, нам просто надо посчитать интеграл:

$$\int_0^1 e^{2\pi i m x} dx = \frac{1}{2\pi i m} e^{2\pi i m x}\Big|_0^1 = \frac{1}{2\pi i m}(e^{2\pi i m} - 1) = 0$$

□

Теорема 1.37. *(Критерий Вейля) Последовательность $(x_n)_{n=0}^{\infty}$ равномерно распределена тогда и только тогда, когда верно следующее:*

$$\forall m \in \mathbb{Z}\backslash\{0\} \quad \frac{1}{N} \sum_{n=0}^{N-1} e^{2\pi i m x_n} \xrightarrow[N\to\infty]{} 0$$

Пример. Рассмотрим последовательность $x_n = \{\alpha n\}$. Если пытаться определить её распределение без критерия Вейля, то это будет крайне тяжело. Однако, применим теорему:

▷ $\alpha \in \mathbb{Q}$. В таком случае, $(x_n)_{n=0}^{\infty}$ будет ходить по кругу конечного числа значений. Понятно, что это не может быть равномерно распределённой последовательностью.

▷ $\alpha \in \mathbb{R}\backslash\mathbb{Q}$, то она равномерно распределена. Действительно, по критерию Вейля

$$\frac{1}{N}\sum_{n=0}^{N-1} e^{2\pi imn\alpha} = \frac{1}{N}\frac{e^{2\pi im\alpha N}-1}{e^{2\pi im\alpha}-1}$$

Посмотрим на модуль этой суммы:

$$\left|\frac{1}{N}\sum_{n=0}^{N-1} e^{2\pi imn\alpha}\right| = \left|\frac{1}{N}\frac{e^{2\pi im\alpha N}-1}{e^{2\pi im\alpha}-1}\right| \leqslant \frac{1}{N}\frac{2}{C},\ C \neq 0$$

Очевидно, что при стремлении N к бесконечности, модуль стремится к нулю.

Доказательство. Для доказательства критерия Вейля нам потребуется *теорема Вейерштрасса* из математического анализа:

Теорема 1.38. *Если f - непрерывная комплекснозначная функция с периодом 1, то $\forall \varepsilon > 0$ существует функция $\psi(x)$ такая, что*

$$\psi(x) = \sum_{m\neq 0} c_m e^{2\pi imx}$$

причём

$$\sup_{x\in\mathbb{R}} |f(x) - \psi(x)| < \varepsilon$$

Замечание. Сумма по $m \neq 0$ подразумевает, что мы смотрим на конечный набор целых $m \neq 0$. Если даже так не понятно написанное, то выражение просто-напросто означает, что $\psi(x)$ - конечная линейная комбинация экспонент с какими-то коэффициентами.

Из всего сказанного выше, нам достаточно доказать теорему лишь в одну сторону: от предела к равномерной распределённости.

Зафиксируем какую-то непрерывную периодическую комплекснозначную функцию f с периодом 1 и $\varepsilon > 0$. Теперь, воспользуемся теоремой выше и выберем $\psi(x)$:

$$\psi(x) = \sum_{m\in M} c_m e^{2\pi imx}, \quad \sup_{x\in\mathbb{R}} |f(x) - \psi(x)| < \frac{\varepsilon}{3}$$

Достаточно доказать, что

$$\frac{1}{N}\sum_{n=0}^{N-1} f(x_n) \xrightarrow[N\to\infty]{} \int_0^1 f(x)dx$$

Давайте добьёмся следующей оценки на модуль суммы $\psi(x_n)$:

$$\left|\frac{1}{N}\sum_{n=0}^{N-1} \psi(x_n)\right| < \frac{\varepsilon}{3}$$

Это сделать достаточно просто: выполним перегруппировку слагаемых, и тогда можно

получить нужную оценку через условие

$$\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)=\frac{1}{N}\sum_{n=0}^{N-1}\sum_{m\in M}c_m e^{2\pi i m x_n}=\sum_{m\in M}c_m\left(\frac{1}{N}\sum_{n=0}^{N-1}e^{2\pi i m x_n}\right)$$

То есть воспользуемся условием и выберем такое N, что выполнено неравенство (этого будет достаточно на желаемую оценку выше):

$$\exists N \mid \forall m\in M \quad \left|\frac{1}{N}\sum_{n=0}^{N-1}e^{2\pi i m x_n}\right|<\frac{\varepsilon}{3|M|\cdot\max\limits_{m\in M}|c_m|}$$

Осталось написать небольшую цепочку преобразований над разностью между суммой и интегралом:

$$\left|\frac{1}{N}\sum_{n=0}^{N-1}f(x_n)-\int_0^1 f(x)dx\right|=$$
$$\left|\frac{1}{N}\sum_{n=0}^{N-1}f(x_n)-\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)+\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)-\int_0^1\psi(x)dx+\int_0^1\psi(x)dx-\int_0^1 f(x)dx\right|\leqslant$$
$$\left|\frac{1}{N}\sum_{n=0}^{N-1}f(x_n)-\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)\right|+\left|\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)-\int_0^1\psi(x)dx\right|+\left|\int_0^1\psi(x)dx-\int_0^1 f(x)\right|=$$
$$\left|\frac{1}{N}\sum_{n=0}^{N-1}(f(x_n)-\psi(x_n))\right|+\left|\frac{1}{N}\sum_{n=0}^{N-1}\psi(x_n)\right|+\int_0^1|\psi(x)-f(x)|dx<3\cdot\frac{\varepsilon}{3}=\varepsilon$$

□

Определение 1.34. *Суммой Гаусса* мы будем называть следующую сумму:

$$S(q)=\sum_{x=1}^{q}e^{2\pi i\frac{ax^2}{q}},\ (a,q)=1$$

Теорема 1.39.

$$|S(q)|=\begin{cases}\sqrt{q},\ \textit{если } q \textit{ нечётно}\\ 0,\ \textit{если } q \textit{ чётно, но не делится на } 4\\ \sqrt{2q},\ \textit{иначе}\end{cases}$$

Доказательство. Вначале немного распишем сам модуль:

$$|S(q)|^2=S(q)\cdot\overline{S(q)}=\left(\sum_{x=1}^{q}e^{2\pi i\frac{ax^2}{q}}\right)\cdot\left(\sum_{y=1}^{q}e^{-2\pi i\frac{ay^2}{q}}\right)$$

Утверждение 1.31. *Имеет место следующее равенство:*

$$\forall t\in\mathbb{Z}\quad\sum_{y=1}^{q}e^{-2\pi i\frac{ay^2}{q}}=\sum_{y=1}^{q}e^{-2\pi i\frac{a(y-t)^2}{q}}$$

Доказательство. Сделаем несколько шагов к данному утверждению:

1. $\forall \alpha \in \mathbb{R} \quad e^{-2\pi i \alpha} = e^{-2\pi i(\lfloor \alpha \rfloor + \{\alpha\})} = e^{-2\pi i \{\alpha\}}$

2. Покажем, что для $\forall y \in \{1, \dots, q\}$ мы можем однозначно сопоставить $y' \in \{1, \dots, q\}$ такой, что
$$ay^2 \equiv a(y' - t)^2 \pmod{q}$$
Понятно, что выполнение этого условия даст нам биекцию между суммами в утверждении, а значит докажет их равенство. В силу свойств арифметических операций в поле $\mathbb{Z}_q$, нам нужно просто взять y' таким, что
$$y' \equiv y + t \pmod{q}$$
Так как t фиксировано, а y пробегает полную систему вычетов, то сопоставление y' будет однозначным (просто какая-то другая полная система вычетов, сдвинутая относительно данной).

□

Отсюда имеем

$$|S(q)|^2 = \left(\sum_{x=1}^{q} e^{2\pi i \frac{ax^2}{q}}\right) \cdot \left(\sum_{y=1}^{q} e^{-2\pi i \frac{a}{q}(y-x)^2}\right) = \sum_{y=1}^{q} e^{-2\pi i \frac{a}{q} y^2} \cdot \sum_{x=1}^{q} e^{2\pi i \frac{2axy}{q}}$$

Разберём случаи:

1. q - нечётное. Тогда, так как $(a, q) = 1$, то и $(2a, q) = 1$. Распишем правую сумму в произведении:

   ▷ $y \in \{1, \dots, q-1\}$:
   $$\sum_{x=1}^{q} e^{2\pi i \frac{2axy}{q}} = e^{2\pi i (2ay/q)} \frac{e^{2\pi i (2ay/q) \cdot q} - 1}{e^{2\pi i (2ay/q)} - 1} = 0$$

   ▷ $y = q$:
   $$\sum_{x=1}^{q} e^{2\pi i \frac{2axy}{q}} = \sum_{x=1}^{q} e^{2\pi (2ax) i} = q$$

   Таким образом, исходная сумма превратилась в следующую:
   $$\sum_{y=1}^{q} e^{-2\pi \frac{a}{q} y^2} \cdot \sum_{x=1}^{q} e^{2\pi i \frac{2axy}{q}} = e^{-2\pi i \cdot aq} \cdot q$$

2. q - чётное. Тогда из условия следует, что a - нечётное. Отсюда у нас есть только 2 внутренние суммы, которые не схлопнутся в ноль: им соответствует $y \in \{q/2, q\}$. То есть
   $$\sum_{y=1}^{q} e^{-2\pi \frac{a}{q} y^2} \cdot \sum_{x=1}^{q} e^{2\pi i \frac{2axy}{q}} = e^{-2\pi \frac{aq}{4}} \cdot q + 1 \cdot q$$

   Получается ещё 2 случая:

(a) $q \equiv 0 \pmod 4$

$$|S(q)|^2 = 1 \cdot q + 1 \cdot q = 2q$$

(b) $q \not\equiv 0 \pmod 4 \Leftrightarrow q = 2t, (t, 2) = 1$

$$(e^{-2\pi \frac{aq}{4}} + 1) \cdot q = (e^{-\pi a \frac{2 \cdot 2t}{4}} + 1) \cdot q = 0$$

□

2 Начала теории графов

Определение 2.1. *Графом* называется пара *множества вершин* и *множества рёбер.*

Определение 2.2. Граф $G = (V, E)$ называется *обыкновенным (простым)*, если выполнены следующие условия:

1. Нет «петель», то есть
$$\forall x \in V \quad \nexists (x, x) \in E$$
2. Нет ориентации, то есть
$$\forall x, y \in V \quad (x, y) = (y, x)$$
3. Нет кратных рёбер, то есть
$$E \subseteq C_V^2$$

Замечание. C_V^2 обозначает множество пар вершин из V без повторений наборов в них.

Замечание автора. Во втором пункте я бы лучше сформулировал так:

$$\forall x, y \in V \quad (x, y) \in E \Leftrightarrow (y, x) \in E$$

Замечание. В дальнейшем, если мы говорим о графе без каких-либо оговорок, то подразумевается именно простой граф.

Сюда бы картиночку с каким-то графом

Определение 2.3. Если мы отказываемся в определении обыкновенного графа от **первого** свойства, то он называется *псевдографом.*

Определение 2.4. Если мы отказываемся в определении обыкновенного графа от **второго** свойства, то он называется *орграфом (ориентированным графом).*

Определение 2.5. Если мы отказываемся в определении обыкновенного графа от **третьего** свойства, то он называется *мультиграфом* (не путать с гиперграфом!!!).

Замечание. Естественно, определения можно комбинировать.

Определение 2.6. Граф $K_n = (V, E)$, $|V| = n$ называется *полным*, если у него есть все возможные рёбра. То есть $|E| = C_n^2$

Пример. Сколько существует графов на $V = \{1, \ldots, n\}$ вершинах?

У нас C_n^2 рёбер и каждое мы можем либо включить, либо не брать в наш граф. Отсюда их $2^{C_n^2}$ штук.

Определение 2.7. Графы $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными*, если существует биекция, удовлетворяющая следующему условию:

$$\varphi\colon V_1 \to V_2 \;\big|\; \forall e = (x, y) \quad e \in E_1 \Leftrightarrow (\varphi(x), \varphi(y)) \in E_2$$

Определение 2.8. *Степенью вершины* $v \in V$ называется количество рёбер, инцидентных ей. Обозначается как $\deg v$

Определение 2.9. *Входящей степенью* $\operatorname{indeg} v$ называется число рёбер, инцидентных данной вершине, в которых v стоит на **втором** месте:

$$\operatorname{indeg} v = |\{y \;\big|\; (y, v) \in E\}|$$

Определение 2.10. *Исходящей степенью* $\operatorname{outdeg} v$ называется число рёбер, инцидентных данной вершине, в которых v стоит на **первом** месте:

$$\operatorname{outdeg} v = |\{y \;\big|\; (v, y) \in E\}|$$

Замечание. Для простого графа $\forall v \in V \;\; \operatorname{indeg} v = \operatorname{outdeg} v$. Определения, данные выше, получают смысл для орграфов.

Определение 2.11. Говорят, что в графе вершина $v \in V$ *инцидентна* ребру $e \in E$ (или ребро e инцидентно вершине v), если e содержит в себе эту вершину.

Лемма 2.1. *(О рукопожатиях) В графе любого типа $G = (V, E)$ верно утверждение:*

$$\sum_{v \in V} \deg v = 2|E|$$

Доказательство. Давайте мысленно зафиксируемся на каком-то из рёбер, и начнём суммировать степени вершин. Наше ребро может быть учтено лишь тогда, когда мы будем считать вершины ему инцидентные, коих всего 2. Отсюда и получается равенство. □

Определение 2.12. Граф называется *регулярным*, если степени всех вершин одинаковы.

Определение 2.13. *Маршрутом в графе $G = (V, E)$* будем называть чередующуюся последовательность вершин и рёбер, которая начинается и заканчивается на вершинах.

$$v_1 e_1 v_2 e_2 \dots e_n v_{n+1}, \quad \forall e_i \;\; e_i = (v_i, v_{i+1})$$

Замечание. Определение маршрута, естественно, допускает возможность появления одинаковых рёбер и вершин в последовательности.

Определение 2.14. Маршрут называется *замкнутым*, если $v_1 = v_{n+1}$

Определение 2.15. Если в замкнутом маршруте все рёбра разные, то он называется *циклом*

Лемма 2.2. *В замкнутом маршруте можно найти цикл. То есть из замкнутого маршрута получить корректный маршрут цикла.*

Доказательство. Пусть есть замкнутый маршрут. Возможно 2 ситуации:

1. Все рёбра замкнутого маршрута оказались разными. Тогда он будет циклом по определению.

2. Нашлось хотя бы 2 одинаковых ребра. В силу конечности маршрута, мы можем рассмотреть такие 2 одинаковых ребра $e = (v, u)$, что между ними в маршруте стоят только разные рёбра. Возможно снова 2 ситуации:

   (a) В маршруте по ребру e мы прошли с разных сторон.
   Если мы прошли $v \to u$, а потом $u \to v$, то мы нашли цикл, у которого начало и конец будут на вершине u. Как маршрут это бы означало следующее:

   $$veu \dots uev \mapsto u \dots u$$

   (b) В маршруте по ребру e мы прошли с одной и той же стороны.
   То есть вначале могло быть $u \to v$, но и потом вышло так же $u \to v$. Снова нашли цикл, который начинается и заканчивается в вершине u.

   $$uev \dots uev \mapsto uev \dots u$$

□

Определение 2.16. Цикл называется *простым*, если помимо разных рёбер, у него все промежуточные вершины тоже разные (то есть кроме v_1 и v_{n+1}).

Определение 2.17. Если маршрут не замкнут и все его рёбра разные, то он называется *путём (или же цепью)*.

Определение 2.18. Путь называется *простым*, если все его вершины разные.

Определение 2.19. Граф $G = (V, E)$ *связен*, если для любой пары вершин $x, y \in V$ существует маршрут, начинающийся в x и заканчивающийся в y.

Замечание. Есть между двумя вершинами в графе есть маршрут, то есть и простой путь. Действительно, давайте как-нибудь «выкинем» из маршрута части между двумя одинаковыми промежуточными вершинами так, чтобы больше одинаковых промежуточных вершин не осталось.

Замечание. Отношение существования пути между вершинами является отношением эквивалентности на множестве V.

Определение 2.20. Граф называется *ациклическим*, если в нём не содержится циклов.

Определение 2.21. Граф $G = (V, E)$ называется *деревом*, если он является связным ациклическим графом.

Теорема 2.1. *Для графа $G = (V, E)$ следующие 4 утверждения эквивалентны:*

1. *G - дерево*
2. *В G любые 2 вершины соединены единственной простой цепью*
3. *G связен и если $|V| = n$, то $|E| = n - 1$*

4. G ацикличен и если $|V| = n$, то $|E| = n - 1$

Доказательство. Построим цикл утверждений:

▷ $1 \Rightarrow 2$ В силу определения дерева G, между двумя вершинами будет существовать простой путь. Если их как минимум 2, то на них можно найти цикл, что противоречит ацикличности дерева.

▷ $2 \Rightarrow 3$ Связность очевидна. Для доказательства второго факта, воспользуемся индукцией по n:

- База $n = 1$ тривиальна.
- Переход $n > 1$.

  У всех вершин не может быть степень, равная 1, ибо тогда отсутствует связность (граф имеет вид пар вершин, инцидентных своему ребру). При этом не может быть и степень, больше либо равная 2: выберем произвольную вершину и будем просто идти по рёбрам, пока можем. В силу конечности графа мы обязательно придём в вершину, из которой либо нету ребра (то есть её степень равна 1, а такого быть не может), либо мы в ней оказались второй раз и нашли цикл (то есть какие-то 2 вершины соединены не единственным путём), противоречие.

  Теперь, доказав наличие вершины степени 1 в нашем графе, выберем её и рассмотрим граф G' без неё и инцидентного ей ребра. Тогда, к G' применимо предположение индукции и $|V'| = n - 1, |E'| = n - 2$. Для графа G это означает, что $|V| = |V'| + 1 = n, |E| = |E'| + 1 = n - 1$.

▷ $3 \Rightarrow 4$ Нужно проверить только ацикличность. Снова воспользуемся индукцией

- База $n = 1$ тривиальна
- Переход $n > 1$. Предположим, что это не так и есть цикл. Тогда у всех вершин цикла степень $\geqslant 2$. По лемме о рукопожатиях

$$\sum_{v \in V} \deg v = 2|E| = 2n - 2$$

  Отсюда в частности следует, что $\exists v_0 \in V\colon \deg v_0 = 1$, так как если у всех вершин степень $\geqslant 2$, то сумма степеней $\geqslant 2n$, а если меньше или равна единице, то сумма $\leqslant n$. Более того, из сказанного выше эта вершина не лежит на цикле. Значит, мы можем её и инцидентное ребро убрать из графа, применить предположение индукции и получить противоречие.

▷ $4 \Rightarrow 1$ Снова индукция по n (проблема только со связностью).

□

Пример. Пусть t_n - число деревьев на n вершинах. Попробуем заметить некоторую за-

кономерность

$$\begin{aligned} t_1 &= 1 \\ t_2 &= 1 = 2^{2-2} \\ t_3 &= 3 = 3^{3-2} \\ t_4 &= 16 = 4^{4-2} \\ t_5 &= 125 = 5^{5-2} \\ &\vdots \end{aligned}$$

Теорема 2.2. *(Формула Кэли, 1857г.)*

$$t_n = n^{n-2}$$

Доказательство. Приведём идею с *кодами Прюфера*: из формулы логично предположить, что мы можем каждому дереву на n вершинах сопоставить размещение $n-2$ чисел из множества $\{1, \dots, n\}$ с повторениями. Покажем явно алгоритмы, один из которых будет по графу находить код, а другой по нему восстанавливать его.

▷ Алгоритм, который по графу возвращает код.

1. Выберем вершину степени 1 с наименьшим номером. Допишем справа в уже имеющийся код номер вершины, которая связана с нашей при помощи ребра.
2. Удалим из графа выбранную вершину и инцидентное ей ребро.
3. Повторим итерацию, пока не останется дерево на 2х вершинах.

▷ Алгоритм, который по коду возвращает граф. Выпишем последовательность $\{1, \dots, n\}$, а под ней код, полученный из графа.

1. Выберем самое малое число из верхнего ряда, которого нет в нижнем.
2. Сделаем пару-ребро (u, v), где u - выбранная на предыдущем этапе вершина, v - первая вершина в нижнем ряде.
3. Удалим найденные вершины из рядов.
4. Повторим итерацию, пока не закончится нижний ряд. Сверху останется всего 2 вершины, и они тоже будут образовывать ребро.

Остаётся обосновать, что полученная функция сопоставления графу его кода - биекция.

▷ Инъективность

▷ Сюръективность

□

Определение 2.22. *Унициклическим графом (одноцикловым)* называется связный граф с ровно одним циклом.

Замечание. Из того, что в унициклическом графе всего 1 цикл следует, что этот цикл простой. Более того, унициклический граф на n вершинах - это такой, в котором $|V| = |E| = n$.

Пример. Сколько существует унициклических графов на n вершинах?

Решение. Для начала разберёмся с тем, какие циклы у нас могут быть и сколько разных и может быть. Пусть k - длина цикла по числу вершин. Тогда $k \in \{3, \dots, n\}$, так как при $k = 2$ требуются кратные ребра, чем простой граф не обладает.

Количество способов выбрать k вершин для цикла - C_n^k, но сколькими их можно зациклить? Ответом будет $C_n^k \cdot k!/(2k)$, так как всего перестановок у нас $k!$, но нужно исключить циклические и зеркальные.

Отсюда искомое количество U_n можно записать так:

$$U_n = \sum_{k=3}^{n} C_n^k \frac{(k-1)!}{2} \cdot F(n,k)$$

где $F(n,k)$ - количество способов достроить цикл на k вершинах до унициклического графа на n вершинах. Иначе говоря, это число лесов на n вершинах с k деревьями, где выделенные k вершин служат представителями отдельных деревьев.

Теорема 2.3. $F(n,k) = k \cdot n^{n-1-k}$

Доказательство. Остаётся читателю в качестве домашнего задания. Будет на экзамене! Нужно расширить идею с кодами Прюфера □

Итого, вся формула имеет следующий вид:

$$U_n = \sum_{k=3}^{n} C_n^k \frac{k!}{2} \cdot n^{n-1-k}$$

Следствие. В курсе дискретного анализа будет доказано, что

$$U_n \sim \sqrt{\frac{\pi}{8}} \cdot n^{n-\frac{1}{2}}$$

Замечание. Если положить за $C(n, n+k)$ - количество связных графов на n вершинах и с $n+k$ рёбрами, то верно следующее:

- $$t_n = C(n, n-1) = n^{n-2}$$
- $$U_n = C(n,n) \sim \sqrt{\frac{\pi}{8}} n^{n-\frac{1}{2}}$$
- $$C(n, n+1) \sim \frac{5}{24} n^{n+1}$$
- $$C(n, n+k) \sim \gamma(k) \cdot n^{n+\frac{3k-1}{2}}$$

2.1 Эйлеровость графов

Замечание. Далее, говоря о графах в этой теме, мы подразумеваем просто неориентированные графы.

История про Кёнигсбергские мосты

Кёнигсберг (нем. Königsberg) - это нынешний Калининград. В 17м веке в этом городе было 7 мостов, расположенных следующим образом:

Когда-нибудь тут будет картинка, ну а так смотрите либо на Википедии, либо в лекции Андрея Михайловича

У людей был интересный вопрос: можно ли начать из какой-то точки города, пройти ровно 1 раз по каждому мосту и вернуться в исходную точку. Задача была решена математиком Леонардом Эйлером в его статье от 1736г., где была доказана невозможность такого обхода и было создано понятие *эйлерового графа*.

Определение 2.23. Граф $G = (V, E)$ называется *эйлеровым* (или же *циклом*), если в нём существует цикл на всех рёбрах.

Теорема 2.4. *Для связного псевдографа следующие 3 свойства эквивалентны:*

1. *Граф является циклом (эйлеровым графом).*
2. *Степень каждой вершины чётна.*
3. *Множество рёбер этого графа можно разбить на простые циклы (маршруты то есть), у которых могут быть общие вершины, но все рёбра разные.*

Доказательство.

▷ $1 \Rightarrow 2$ Очевидно, так как сколько раз мы вошли в какую-то вершину, столько же раз мы и вышли из неё, при этом ребро входа/выхода всегда было новым.

▷ $2 \Rightarrow 1$ Проведём индукцию по m - числу рёбер:

- База $m \leqslant 1$: тривиально (граф с одним ребром является просто петлей)
- Переход $m > 1$: Выберем произвольную вершину x и просто пойдём от неё куда-то по рёбрам, по которым мы ещё не ходили. Рассмотрим возможные ситуации с вершиной, в которую мы придём:
  1. Из вершины есть путь. Тогда возможно ещё 2 варианта:
     (a) Мы не были в этой вершине. Просто идём дальше.
     (b) Мы были в этой вершине, а значит получился простой цикл, у которого начало и конец на этой вершине.
  2. Из конечной вершины нет пути. Так как степень всех вершин чётна, то такое может быть только в случае, если мы попали обратно в вершину x. Следовательно, получили простой цикл с началом и концом в x.

  Обозначим найденный простой цикл за C, его начало за y, а множество рёбер цикла как E_C. Рассмотрим граф $G' = (V, E \backslash E_C)$, полученный из исходного графа $G = (V, E)$. Понятно, что степень любой вершины из G' тоже чётная, но граф G' мог оказаться не связным, а состоять из нескольких компонент связности. Воспользуемся для каждой из них предположением индукции. Тогда пусть v_i - это i-я вершина в обходе цикла C, а μ_i - это соответствующий ей эйлеров цикл в своей компоненте. Чтобы получить эйлеров цикл для G, достаточно обойти C и, например, пройти по μ_i лишь тогда, когда v_i - это последняя вершина, связанная с данной компонентой в обходе C.

▷ $1 \Rightarrow 3$ Посмотрим на эйлеров цикл μ исходного графа $G = (V, E)$. Возможно 2 ситуации:

1. В μ нету одинаковых промежуточных вершин. В таком случае эйлеров цикл - простой, и утверждение тривиально выполнено.
2. В маршруте μ нашлась хотя бы пара одинаковых промежуточных вершин. Среди всех таких пар выберем самую левую и такую, что между парой нету третьей такой же вершины. Тогда цикл выглядит так:

$$xAvBvCx$$

где A, B, C - сокращения для частей маршрута. При этом vBv - простой цикл, а $xAvCx$ - обычный.

Применим аналогичные рассуждения к $xAvCx$. Так как либо длина рассматриваемого маршрута уменьшается, либо он просто нам подходит, то мы обязательно разобьём его на простые циклы.

▷ $3 \Rightarrow 2$ Заметим, что рёбра, инцидентные одной вершине, разбиваются на пары по принадлежности к какому-то из циклов. Отсюда сразу следует необходимое.

□

2.2 Гамильтоновость графов

Определение 2.24. Граф $G = (V, E)$ называется *гамильтоновым*, если существует простой путь, содержащий все его вершины. Такой путь называется тоже *гамильтоновым.*

Определение 2.25. Если найдётся гамильтонов путь, который является ещё и циклом, то он называется *гамильтоновым циклом.*

Теорема 2.5. *(Дирака) Если у графа $G = (V, E), |V| = n$ степень каждой вершины $\geqslant \frac{n}{2}$, то он гамильтонов.*

Доказательство. Предположим, это не так. Тогда пусть $n > 2$ и $k > 0$ - минимальное количество вершин, которые нужно добавить в граф G, чтобы он стал гамильтоновым. Пусть G' - это граф G, дополненный этими вершинами. Рассмотрим гамильтонов цикл:

$$v \mapsto p \mapsto w \mapsto \ldots \mapsto v$$

Из-за необходимости дополнительных вершин, мы можем потребовать, что p - одна из таких (ибо цикл покрывает все вершины, причём промежуточные по одному разу). При этом w не может быть тогда новой вершиной в силу минимальности k. Заметим 2 факта:

1. Вершина w не смежная к v, ибо иначе нам не нужна вершина p.
2. Пусть w', v' - вершины, смежные с w, v соответственно. Тогда v' не может следовать за w' в нашем цикле, иначе исходный цикл

$$v \mapsto p \mapsto w \mapsto \ldots \mapsto v' \mapsto w' \mapsto \ldots \mapsto v$$

можно заменить на следующий:

$$v \mapsto v' \mapsto \ldots \mapsto w \mapsto w' \mapsto \ldots \mapsto v$$

То есть избавились от p, чего быть не должно.

Из вышесказанного следует, что множество смежных с w вершин не пересекается с множеством смежных с v вершин. Так как $\deg v,\ \deg w \geqslant n/2 + k$, то отсюда число вершин в G' должно быть как минимум $n + 2k$, а на деле оно $n + k$. Противоречие. □

Определение 2.26. Пусть дан граф $G = (V, E)$. Множество $W \subseteq V$ называется *независимым*, если

$$\forall x, y \in W\ (x, y) \notin E$$

Определение 2.27. Для графа $G = (V, E)$ величина $\alpha(G)$ называется *числом независимости графа* и означает максимальную мощность независимого подмножества в V.

$$\alpha(G) = \max\{k \in \mathbb{N} \mid |W| = k\}$$

Пример. Для графа-простого цикла на n вершинах верно, что

$$\alpha(G) = \left\lfloor \frac{n}{2} \right\rfloor$$

Определение 2.28. *Подграфом* $G' = (W, E')$ графа $G = (V, E)$ называется граф, у которого $W \subseteq V$, а $E' \subseteq \{(x, y) \mid x, y \in W, (x, y) \in E\}$.

Определение 2.29. Подграф $G' = (W, E')$ называется *индуцированным*, если $E' = \{(x, y) \mid x, y \in W, (x, y) \in E\}$.

Обозначение $G_{V\setminus A}$ подразумевает индуцированный подграф, у которого $V' = V\setminus A$.

Определение 2.30. Для графа $G = (V, E)$ величина $\varkappa(G)$ называется *числом вершинной связности* и описывается так:

$$\varkappa(G) = \min\{k \in \mathbb{N} \mid \exists W \subseteq V, |W| = k \text{ и } G|_{V\setminus W} \text{ не связен }\}$$

Замечание. $\varkappa(G)$ означает минимальное число вершин, которое нужно удалить из графа G, чтобы он перестал быть связен. Для полного графа понятие обычно не применяют (или же как-то доопределяют).

Теорема 2.6. *(Э́рдёш, Хва́тал) Если $\alpha(G) \leqslant \varkappa(G), |V| \geqslant 3$, то G - гамильтонов граф.*

Доказательство. Сразу отметим, что G связен. Если бы это было не так, то $\varkappa(G) = 0$, но при этом $\alpha(G) > 0$ (пустой граф мы не рассматриваем). Проведём доказательство в несколько стадий:

1. Предположим, что в G нет циклов. Тогда G - дерево, причём в нём есть как минимум 2 листа, не соединённых друг с другом. Тогда очевидно, что $\alpha(G) \geqslant 2, \varkappa(G) = 1$. Противоречие.

2. Теперь в графе G есть хотя бы один цикл. Рассмотрим самый длинный простой цикл $C = \{x_1, \ldots, x_k\}$. Предположим, что $k < n$, где $|V| = n$. Тогда, посмотрим на индуцированный подграф $G' := G_{V\setminus C}$ и у него выберем W - множество вершин любой

связной компоненты G'. Обозначим за $N_W(G)$ - множество «соседей» вершин из W в графе G:

$$N_W(G) = \{y \in V \backslash W \mid \exists x \in W, (x, y) \in E(G)\}$$

Заметим несколько утверждений про этот объект:

(a) $N_W(G) \subseteq C$, так как рёбер из W в G' нет (мы выбрали W как компоненту связности в графе G').

(b) Если $x_i \in N_W(G)$, то $x_{i+1} \notin N_W(G)$. Это понятно, так как иначе мы можем продлить цикл за счёт вершин из W. Значит, $N_W(G) \subset C$

(c) $\varkappa(G) \leqslant |N_W(G)|$. Действительно, при удалении $N_W(G)$ у нас возникает отдельная компонента W, но при этом от цикла что-то да останется, ибо по уже доказанному $N_W(G) \subset C$.

(d) Если положить за $M = \{x_{i+1} \mid x_i \in N_W(G)\}$, то $M \cap N_W(G) = \varnothing$ и $|M| = |N_W(G)|$. При этом M оказывается независимым множеством. Доказательство последнего факта можно провести от противного: предположим, что $x_i, x_j \in N_W(G), i < j$, но при этом между x_{i+1} и x_{j+1} есть ребро. В таком случае, путь x_i соединяется с $a \in W$, а x_j с $b \in W$. Рассмотрим следующий цикл:

$$x_1 \mapsto x_i \mapsto a \mapsto b \mapsto x_j \mapsto x_{i+1} \mapsto x_{j+1} \mapsto x_1$$

Он простой, но при этом на 1 ребро длиннее C. Противоречие.

(e) $\forall x \in W$ $M \cup \{x\}$ тоже независимое множество. В самом деле, $M \cap N_W(G) = \varnothing$, поэтому мы можем взять любую вершину из W к себе.

Отсюда имеем, что

$$\alpha(G) \geqslant |M| + 1$$

Но при этом

$$\varkappa(G) \leqslant |N_W(G)| = |M|$$

Противоречие с условием.

□

Замечание. Доказательство также даёт нам алгоритм для поиска гамильтонова пути - найдём какой-то простой цикл и будем его увеличивать при помощи рассуждений из теоремы, пока он не станет гамильтоновым циклом.

Определение 2.31. Граф $G_n = (V_n, E_n)$, $|V_n| = n$ называется *разреженным*, если

$$\lim_{n\to\infty} \frac{|V_n|}{|E_n|} = 0$$

Пример. В некоторых случаях можно аккуратно посчитать число независимости графа при помощи математики. Рассмотрим один из них (и попробуем применить к нему теорему Дирака или Эрдёша-Хватала):

Пусть дан граф $G = (V, E)$, где $V = \{A \subset \{1, \ldots, n\} \mid |A| = 3\}$, а $E = \{(A, B) \mid |A \cap B| = 1\}$. Из определения понятно, что $|V| = C_n^3$. Более того, заметим, что наш граф - регулярный. Степень вершины A можно посчитать так:

Выберем одно из чисел A. Тогда, остаётся $n-3$ числа, откуда нужно выбрать 2, и тогда мы получим вершину B, соединённую с A. То есть $\deg A = 3 \cdot C_{n-3}^2$, а по лемме о рукопожатиях

$$|E| = \frac{1}{2}\sum_{A \in V} \deg A = \frac{3 \cdot C_{n-3}^2 \cdot C_n^3}{2} \sim \frac{3}{24} n^5$$

Число вершин асимптотически ведёт себя как $n^3/6$, поэтому граф G - разреженный. Значит, применить теорему Дирака не получится.

Что из себя представляет любое независимое множество $W = \{A_1, \ldots, A_t\}$ этого графа?

$$\forall i, j \in [1; t] \ |A_i \cap A_j| \in \{0, 2\}$$

Утверждение 2.1.

$$\alpha(G) = \begin{cases} n, \ n \equiv 0 \pmod 4 \\ n-1, \ n \equiv 1 \pmod 4 \\ n-2, \ \textit{иначе} \end{cases}$$

Доказательство. Докажем оценку снизу. Разобьём множество $\{1, \ldots, n\}$ на множества по 4 элемента (за исключением, быть может, последнего): $\{1,2,3,4\}, \{5,6,7,8\}, \ldots$ В каждой такой четвёрке у нас есть $C_4^3 = 4$ вершины с соответствующим набором чисел. При этом пересекаться любые из этих 4 будут пересекаться по двум элементам, тогда как любые вершины из разных множеств не будут пересекаться вовсе. Отсюда и следует оценка. Другая часть остаётся читателю в качестве домашнего задания (там просто по индукции надо). □

Дополнительно покажем красивый способ доказать, что $\alpha(G) \leqslant n$. Сопоставим $A_i \mapsto \vec{x}_i \in \{0,1\}^n = \mathbb{Z}_2^n$ (координаты являются маской множества $\{1, \ldots, n\}$). Заметим следующий факт:

$$|A_i \cap A_j| = (\vec{x}_i, \vec{x}_j)$$

Если мы теперь докажем, что векторы, соответствующие независимому множеству M, образуют линейно независимую систему, то нужное неравенство автоматически доказано, ибо $\dim \mathbb{Z}_2^n = n$. Запишем линейную комбинацию векторов из M, которая оказалась равна нулю:

$$c_1\vec{x}_1 + \ldots + c_t\vec{x}_t = \vec{0}$$

Что будет, если мы возьмём скалярное произведение с $\vec{x}_1$ от обеих частей равенства?

$$c_1(\vec{x}_1, \vec{x}_1) + \ldots + c_t(\vec{x}_t, \vec{x}_1) = (\vec{0}, \vec{x}_1) = 0$$

Но при этом скалярное произведение для разных векторов либо 0, либо 2, что тоже равно 0 в $\mathbb{Z}_2$. Также $(\vec{x}_1, \vec{x}_1) = 3 \equiv 1$. Значит, $c_1 = 0$. Отсюда $\forall c_i = 0$, что и требовалось доказать.

Теперь нужно как-то показать, что $\varkappa(G) \geqslant n$, и тогда сможем применить теорему Эрдеша-Хватала. Рассмотрим следующий факт:

Утверждение 2.2. *Пусть есть произвольный граф $G = (V, E)$. Введём величину $f(x, y)$:*

$$f(x,y) := |\{u \in V \mid (x,u), (y,u) \in E\}|$$

В таком случае, оценка на $\varkappa(G)$ снизу будет как минимум такой:

$$\varkappa(G) \geqslant \min_{x,y} f(x,y)$$

Замечание. То есть $f(x,y)$ - это число общих соседов у x и y.

Доказательство. Действительно, попробуем удалить меньше вершин, чем минимум $f(x,y)$. Тогда для любых двух вершин у нас останется сосед, который их соединяет. □

Теперь мы явно посчитаем $\min\limits_{x,y\in V} f(x,y)$ для нашего графа. Рассмотрим возможные случаи:

- $|x \cap y| = 0$, то есть тройки не пересекаются. Тогда мы должны выбрать по одному элементу из каждой тройки и взять ещё 1 среди тех, которые не встречаются в $x \cup y$. Отсюда
$$f(x,y) = 3^2 \cdot (n-6) = 9(n-6)$$
- $|x \cap y| = 1$. Аналогичным образом получаем
$$f(x,y) = C_{n-5}^2 + 2^2 \cdot (n-5)$$
- $|x \cap y| = 2$. Снова так же имеем
$$f(x,y) = 2C_{n-4}^2 + 1^2 \cdot (n-4)$$

Из анализа величин выше несложно выяснить, что для достаточно большого n первый случай будет минимальным. Очевидно, что $9(n-6) \geqslant n$ для вполне большого n. Значит, граф будет гамильтоновым.

2.3 Последовательности де Брёйна

Определение 2.32. Пусть дано $n \in \mathbb{N}$ и алфавит $\Sigma = \{0,1\}$. Составим словарь из двоичных слов длины n. Тогда, суммарное число символов в словаре будет $2^n \cdot n$. *Последовательностью де Брёйна* называется такая последовательность из нулей и единиц длины N, что любое подслово длины n будет уникальным и соответствующим какому-то слову из словаря выше.

Замечание. То есть, если мы возьмём «рамку» на n элементов и пройдёмся по последовательности де Брёйна от начала и до конца, то в рамке будет получаться любое слово из словаря, причём один раз

Утверждение 2.3. *Длина последовательности де Брёйна всегда* $2^n + n - 1$.

Доказательство. Рассмотрим более подробно идею с окном. У нас должны встретиться все 2^n слов и только они, а чтобы была возможность показать первое - нужно ещё $n-1$ символ. Отсюда получаем длину. □

Построение последовательностей де Брёйна

Теорема 2.7. *Последовательности де Брёйна существуют для любого* $n \in \mathbb{N}$.

Доказательство. Как доказательство этой теоремы, приведём 2 способа построения таких последовательностей:

1. Правило *«0 лучше 1»*: начнём последовательность с n единиц. Затем будем руководствоваться следующим соображением: ставим следующим символом 0, если такое слово-суффикс ещё не встречалось в последовательности. Иначе 1.

   Пример. $n = 3 \Rightarrow N = 10 \Rightarrow 1110001011$

2. Введём понятия *графа де Брёйля* $G = (V, E)$. Это ориентированный граф, у которого вершины $V = \{0, 1\}^{n-1}$, а ребро $(v, u) \in E$ тогда и только тогда, когда суффикс слова v длины $n - 2$ является префиксом u.

   Для орграфов есть аналогичное условие эйлеровости:

   $$\forall v \in V \;\; \operatorname{indeg} v = \operatorname{outdeg} v > 0$$

   Понятно, что у любой вершины построенного нами графа входящая и исходящая степень равны 2. Значит, он эйлёров и есть эйлеров обход. Если мы возьмём за начало последовательности первую вершину обхода, а по мере прохождения будем брать только последние элементы следующих вершин, то получим в точности последовательность де Брёйна.

□