

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

ОСНОВЫ КОМБИНАТОРИКИ И ТЕОРИИ ЧИСЕЛ  
II СЕМЕСТР

Лектор: *Андрей Михайлович Райгородский*



Автор: *Киселев Николай*  
*Репозиторий на Github*

весна 2025

# Содержание

<b>1</b>	<b>Квадратичные вычеты и невычеты</b>	<b>2</b>
<b>2</b>	<b>Матрицы Адамара</b>	<b>4</b>
2.1	Коды, исправляющие ошибки . . . . .	7
<b>3</b>	<b>Распределение простых чисел</b>	<b>9</b>
<b>4</b>	<b>Первообразный Корень</b>	<b>11</b>
4.1	Алгоритм шифрования . . . . .	12
4.2	Существование первообразного корня . . . . .	12
<b>5</b>	<b>Тесты на простоту чисел</b>	<b>14</b>
5.1	Тест Ферма на Простоту . . . . .	14
5.1.1	Свойства чисел Кармайкла . . . . .	15
5.2	Символ Якоби . . . . .	15
5.2.1	Свойства Символа Якоби . . . . .	15
5.3	Тест Соловея - Штрассена . . . . .	15
<b>6</b>	<b>Диофантовы приближения, теорема Дирихле</b>	<b>16</b>
6.1	Теорема Минковского. Еще одно доказательство теоремы Дирихле . . . . .	17
<b>7</b>	<b>Цепные дроби</b>	<b>18</b>
7.1	Конечная цепная дробь . . . . .	18
7.2	Бесконечная цепная дробь . . . . .	19
7.3	Трансцендентность и иррациональность числа $e$ . . . . .	21
7.4	7-ая проблема Гильберта . . . . .	22
<b>8</b>	<b>Геометрия чисел</b>	<b>23</b>
<b>9</b>	<b>Равномерное распределение последовательностей</b>	<b>25</b>
<b>10</b>	<b>Вероятностное детерминирования</b>	<b>27</b>
10.1	Тест Миллера-Рабина . . . . .	27
10.2	Числа Мерсенна . . . . .	28

# 1 Квадратичные вычеты и невычеты

**Определение 1.1.** Пусть  $a, m \in \mathbb{N}$ ,  $(a, m) = 1$ . Тогда

Если  $\exists x : x^2 \equiv_m a$ , то  $a$  называется квадратичным вычетом

Если  $\nexists x : x^2 \equiv_m a$ , то  $a$  называется квадратичным невычетом

Будем рассматривать случай, когда  $m$  — простое нечетное число

**Теорема 1.1** (Лагранжа). Пусть  $f(x) = a_n x^n + \dots + a_1 x + a_0$ . Тогда число решений  $f(x) \equiv_p 0$  не превосходит  $n$ .

*Доказательство.* От противного: пусть найдутся  $x_1, \dots, x_{n+1}$ , т.ч. они являются решениями. Заметим, что  $f$  можно представить следующим образом:

$$\begin{aligned} f(x) &= b_n(x - x_1) \dots (x - x_n) \\ &\quad + b_{n-1}(x - x_1) \dots (x - x_{n-1}) \\ &\quad \vdots \\ &\quad + b_1(x - x_1) \\ &\quad + b_0 \end{aligned}$$

Но тогда, подставляя  $x_1 \dots x_{n-1}$  получаем, что все  $b_i = 0 \forall i \leq n - 1$ . Но тогда  $f(x_{n+1}) \neq 0$ . Противоречие.  $\square$

**Замечание.** Если  $m$  — простое нечетное число, то решений

$$x^2 \equiv a^2$$

Ровно 2 ( $x = \pm a$ )

**Замечание.** Множество всех квадратичных вычетов:

$$\left\{ 1^2, 2^2, \dots, \frac{p-1}{2}^2 \right\}$$

Итого, квадратичных вычетов  $\frac{p-1}{2}$ , ровно как и невычетов.

**Определение 1.2.** Символ Лежандра  $\left(\frac{a}{p}\right)$  — читается " $a$  по  $p$ "

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & a = 0 \\ 1, & a \text{ — вычет} \\ -1, & a \text{ — невычет} \end{cases}$$

**Анекдот:** посчитать сумму

$$\frac{4}{p+1} \sum_{a=1}^p \left(\frac{a}{p}\right)$$

*Решение (1).* Если вы знаете, что  $\left(\frac{a}{p}\right)$  — символ Лежандра, то сумма будет равна 0

*Решение (2).* Иначе, вы посчитаете арифметическую прогрессию и получите свою оценку на экзамене

Рассмотрим уравнение

$$a^{p-1} \equiv_p 1$$

$$\left(a^{\frac{p-1}{2}} - 1\right) \left(a^{\frac{p-1}{2}} + 1\right) \equiv_p 0$$

Причем, первая скобка имеет не более  $\frac{p-1}{2}$  решений, поэтому, т.к. любой квадратичный вычет ее зануляет, ее решения — только квадратичные вычеты. Таким образом:

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

Поэтому можно сказать, что

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

**Замечание.**

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

**Утверждение 1.1.** *Зафиксируем некоторое число  $a$ . Пусть  $x$  пробегает числа  $1, 2, \dots, \frac{p-1}{2} = p_1$ . Рассмотрим числа  $ax = \varepsilon_x \cdot r_x$ , где  $\varepsilon_x \in \{-1, 1\}, r_x \in \{1, 2, \dots, p_1\}$ . Тогда  $x \neq y \Rightarrow r_x \neq r_y$ .*

*Доказательство.* Предположим противное. Тогда  $r_x = r_y, x \neq y$ . Но тогда  $\varepsilon_x \neq \varepsilon_y$ , т.к. в противном случае  $ax = ay$ , чего быть не может. Но тогда  $r_x \equiv_p -r_y \Rightarrow r_x + r_y \equiv_p 0$ , но такого тоже быть не может, т.к.  $r_x, r_y \leq \frac{p-1}{2}$ .  $\square$

**Утверждение 1.2.**  $\varepsilon_x = (-1)^{\left[\frac{2ax}{p}\right]}$

*Доказательство.* Если  $(ax \bmod p) \in \{1, 2, \dots, p_1\}$ , то  $(-1)^{\left[\frac{2ax}{p}\right]} = 1$ , иначе  $(-1)^{\left[\frac{2ax}{p}\right]} = -1$ .  $\square$

**Утверждение 1.3.**

$$a^{\frac{p-1}{2}} = \prod_{x=1}^{p_1} \varepsilon_x$$

*Доказательство.*

$$a^{\frac{p-1}{2}} \prod_{x=1}^{p_1} x = \prod_{x=1}^{p_1} \varepsilon_x r_x$$

Причем  $\prod x = \prod r_x$ , т.к. все  $x$  различны, все  $r_x$  различны и берутся из одного множества. Сократив множители, получим желаемое.  $\square$

**Утверждение 1.4.**

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^{\sum_{x=1}^{p_1} \left[\frac{2ax}{p}\right]}$$

*Доказательство.* Соединяем предыдущие два утверждения и получаем желаемое.  $\square$

**Утверждение 1.5 (Уточнение).** *Пусть  $a$  — нечетное. Тогда*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}$$

*Доказательство.* Рассмотрим

$$\begin{aligned} \left(\frac{2a}{p}\right) &= \left(\frac{2a+2p}{p}\right) = \left(\frac{4\left(\frac{a+p}{2}\right)}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{2\frac{1}{2}(a+p)x}{p}\right]} = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \sum_{x=1}^{p_1} x} = \\ &= (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p_1(p_1+1)}{2}} = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8}} \end{aligned}$$

Из этого можно показать, что  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$ . Тогда

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

Итого получили, что

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left[\frac{ax}{p}\right]}$$

□

**Теорема 1.2** (Квадратичный Закон Взаимности). Пусть  $p, q$  — различные нечетные простые. Тогда

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

*Доказательство.*

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\sum_{x=1}^{q_1} \left[\frac{px}{q}\right] + \sum_{y=1}^{p_1} \left[\frac{qy}{p}\right]}$$

Введем множество  $S = \{1, \dots, q_1\} \times \{1, \dots, p_1\}$ . Очевидно, что  $|S| = p_1 q_1$ . Введем  $S_1 = \{(x, y) \in S \mid qy < px\}$ ,  $S_2 = \{(x, y) \in S \mid qy > px\}$ . Тогда  $|S| = |S_1| + |S_2|$ , т.к.  $px = qy$  невозможно.

Причем,  $qy < px \Leftrightarrow y < \frac{px}{q}$ ,  $qy > px \Leftrightarrow \frac{qy}{p} > x$ . Заметим, что  $|S_1| = \sum_{x=1}^{q_1} \left[\frac{px}{q}\right]$ , т.к. количество  $y$  для фиксированного  $x$  равно  $\left[\frac{px}{q}\right]$ . Но тогда получаем, что  $|S| = |S_1| + |S_2|$ , что и требовалось. □

## 2 Матрицы Адамара

**Определение 2.1.** Матрицей Адамара называется матрица  $A$ , если и только если

$$[A]_{ij} \in \{1, -1\}$$

И ее строки попарно ортогональны (то есть скалярное произведение любых двух строк равно 0)

**Пример.** 1.  $n = 1$  — очев

2.  $n = 2$ :

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

3.  $n = 2$ :

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

**Замечание.**  $n \geq 2 \Rightarrow n = 2k$

*Доказательство.* Очевидно, т.к. если мы перемножим любые две строчки, то тогда в скалярном произведении придется сложить нечетное количество  $\pm 1$ , тогда эта сумма точно не будет равна 0.  $\square$

**Утверждение 2.1.** Если у матрицы попарно ортогональны сторчки, то и столбцы — тоже

**Определение 2.2.** Нормальная форма матрицы Адамара: когда  $A_1 = A^1 = (1, 1, \dots, 1)$

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

**Замечание.** Любую матрицу адамара можно привести к нормальному виду путем домножения строк и столбцов на  $-1$ .

**Теорема 2.1.**  $n > 2 \Rightarrow n = 4k$

*Доказательство.* Приведем матрицу Адамара к нормальному виду. Теперь переставим столбцы, чтобы вторая строчка была вида

$$\underbrace{(1, 1 \dots 1)}_{\frac{n}{2}}, \underbrace{(-1, -1, \dots -1)}_{\frac{n}{2}}$$

А третья строка была вида

$$\underbrace{(1, 1 \dots 1)}_x, \underbrace{(-1, -1, \dots -1)}_{\frac{n}{2}-x}, \underbrace{(1, 1 \dots 1)}_{\frac{n}{2}-x}, \underbrace{(-1, -1, \dots -1)}_x$$

Тогда скалярное произведение второй и третьей будет равно

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

Тогда  $x = \frac{n}{4}$

$\square$

**Теорема 2.2.** (Гипотеза Адамара) Если  $n = 4k$ , то матрица Адамара существует.

*Доказательство.* Не доказана

$\square$

**Определение 2.3.** Кронекеровское произведение матриц  $A * B = C \Rightarrow$

$$C = \begin{pmatrix} a_{11}B & \dots & a_{1n}B \\ \vdots & \ddots & \vdots \\ a_{n1}B & \dots & a_{nn}B \end{pmatrix} \in M_{mn \times mn}$$

**Утверждение 2.2.** Кронекеровское произведение двух матриц Адамара есть матрица Адамара

*Доказательство.* Скалярное произведение двух строк равняется

$$\sum_{k=1}^n \left( \sum_{s=1}^m a_{ik} a_{jk} b_{i's} b_{j's} \right) = \sum_{k=1}^n a_{ik} a_{jk} \left( \sum_{s=1}^m b_{i's} b_{j's} \right) = (B_{i'}, B_{j'}) \left( \sum_{k=1}^n a_{ik} a_{jk} \right) = (B_{i'}, B_{j'})(A_i, A_j) = 0$$

□

**Теорема 2.3** (Пэли). Пусть  $p = 4k + 3$  — простое число. Тогда  $\exists$  матрица Адамара порядка  $p + 1$ .

*Доказательство.* Рассмотрим матрицу порядка  $p$ , такую, что  $A_{ab} = \left( \frac{a-b}{p} \right)$  (символ Лежандра). Тогда произведение любых двух строк  $i, j$  равно

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

$$c = i - b.$$

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

$$\text{Причем, } c = p \Rightarrow \left( \frac{c}{p} \right) = 0$$

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

При этом,  $i - j, c^{-1} \not\equiv_p 0 \Rightarrow$  выражение  $1 + c^{-1}(i - j)$  пробегает все остатки  $\mod p$ , кроме 1. Но тогда итоговая сумма равна  $0 - \left( \frac{1}{p} \right) = -1$ . Тогда рассмотрим такую матрицу:

$$C = \left( \begin{array}{c|ccc} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & A & \\ 1 & & & \end{array} \right)$$

Где все нули в  $A$  заменены на  $-1$  (получится матрица  $A'$ , причем замены произойдут только на главной диагонали). Докажем, что она подходит. Заметим, что в матрице  $A'$  поровну 1 и  $-1$ . Тогда скалярное произведение с первой строчкой точно будет 0. Возьмем строчки  $i, j$  в матрице  $A'$ . В их скалярном произведении добавилась  $(-1) \left( \frac{i-j}{p} \right) + (-1) \left( \frac{j-i}{p} \right) = 0$ . Теперь посчитаем скалярное произведение любых двух строк, к нему просот добавится 1 за счет первого столбца. Тогда это будет матрицей Адамара. □

**Теорема 2.4** (Пэли). Пусть  $p = 4k + 1$  — простое число. Тогда  $\exists$  матрица Адамара порядка  $2(p + 1)$ .

**Теорема 2.5** (б/д).  $\forall \varepsilon > 0 \exists n_0 : \forall n > n_0$  на отрезке  $[n, (1 + (1 + \varepsilon)n)]$  есть порядок матрицы Адамара

**Теорема 2.6** (переформулировка, тоже б/д).  $\exists f : f(n) = o(n)$ , такая, что на отрезке  $[n, n + f(n)]$  есть порядок матрицы Адамара

## 2.1 Коды, исправляющие ошибки

Представим ситуацию: разговариваем с бабушкой. Еще мы с ней общаемся азбукой морзе (отправляем ей 0 или 1) и передаем ей сообщения длины  $n$ . Известно, что бабушка неправильно услышит не более чем  $k$  циферок. Как тогда с ней общаться?

**Определение 2.4.** Расстояние Хэмминга между словами — количество несовпадающих координат

Тогда нам, по сути, надо расположить непересекающиеся "шары" радиуса  $k$ , состоящие из слов. В таком случае мы сможем определить, какое слово мы передали, т.к. оно будет лежать не более, чем в одном шаре.

**Определение 2.5.**  $(n, M, d)$ -код — такой словарь, в котором  $M$  слов, каждое из которых имеет длину  $n$  и минимальное расстояние между любыми двумя словами равно  $d$ .

**Теорема 2.7** (Граница Плоткина). Пусть дан  $(n, M, d)$ -код, где  $2d > n$ . Тогда  $M \leq \frac{2d}{2d-n}$ .

*Доказательство неулучшаемости оценки.* Рассмотрим матрицу Адамара:

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

И зачеркнем в ней первый столбец. Будем рассматривать строки как слова. Тогда расстояние Хэмминга между ними равно  $\frac{n}{2}$  (т.к. скалярное произведение любых двух равно 0). Тогда получили  $(n-1, n, \frac{n}{2})$ -код. Но тогда плоткин дает результат  $\frac{2\frac{n}{2}}{2\frac{n}{2}-(n-1)} = n$ , т.е. мы нашли пример, который точно подходит под оценку.  $\square$

*Доказательство.* Рассмотрим  $(n, M, d)$ -код,  $a_{ij} \in \{0, 1\}$

$$\sum_{k=1}^n \sum_{i < j} |a_{ik} - a_{jk}| = \sum_{i < j} \underbrace{\sum_{k=1}^n |a_{ik} - a_{jk}|}_{\text{Хеммингово расстояние между } i\text{-ой и } j\text{-ой строками}} \geq \sum_{i < j} d = \frac{M(M-1)}{2} d$$

Однако заметим, что если в слове  $x$  единиц, то в нем  $M-x$  нулей, и тогда пар  $\{0, 1\}$  в нем будет ровно  $x(M-x) \leq \frac{M^2}{4}$ . Тогда общая сумма будет  $\leq \frac{nM^2}{4}$ , т.к.  $\frac{nM^2}{4}$  — верхняя оценка на количество пар. Но тогда:

$$\begin{aligned} \frac{M(M-1)}{2} d &\leq \frac{nM^2}{4} \\ (M-1)d &\leq \frac{nM}{2} \\ 2(M-1)d &\leq nM \end{aligned}$$



$$M(2d - n) \leq 2d$$

$$M \leq \frac{2d}{2d - n}$$

□

**Теорема 2.8.** Пусть  $\mathcal{R}_n = \{1, 2, \dots, n\}$ . Пусть  $\{M_1, M_2, \dots, M_n\} \subseteq \mathcal{R}$ . Тогда  $\exists$  раскраска множества  $\mathcal{R}_n$  в красный и синий цвета, при которой  $\forall i$  в  $M_i$  разность между количеством чисел элементов по модулю  $\leq 6\sqrt{n}$

*Доказательство.* Доказательство нас будет ожидать в 4 семестре и будет использовать энтропию. Не бойтесь никакой физики там не будет. □

**Теорема 2.9.** Пусть  $\chi$  — раскраска  $\mathcal{R}_n$  в красный и синий цвета. Введем  $\chi : 2^{\mathcal{R}_n} \rightarrow \mathbb{Z} : \chi(A) = \#(\text{красных элементов } A) - \#(\text{синих элементов } A)$ . Пусть существует матрица Адамара порядка  $n$ . Тогда  $\exists M_1, M_2, \dots, M_n : \forall \chi : \exists i |\chi(M_i)| \geq \frac{\sqrt{n}}{2}$

*Доказательство.* Рассмотрим матрицу Адамара нормального вида

$$H = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \pm 1 & \dots & \pm 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \pm 1 & \dots & \pm 1 \end{pmatrix}$$

Возьмем каждую строку  $H$ . Это элементы  $\{+1, -1\}^n$ . Пусть  $J : [J]_{ik} = 1$ . Докажем, что  $\forall v \in \{+1, -1\}^n$  у вектора  $\left(\frac{H+J}{2}\right)v$  существует координата, модуль которой  $\geq \frac{\sqrt{n}}{2}$ . Заметим, что

$$(Hv, Hv) = (vh_1 + vh_2 + vh_3 + \dots, vh_1 + vh_2 + vh_3 + \dots)$$

$$\begin{aligned} (v_1h_1 + v_2h_2 + v_3h_3 + \dots, v_1h_1 + v_2h_2 + v_3h_3 + \dots) &= v_1^2(h_1, h_1) + v_2^2(h_2, h_2) + \dots + v_n^2(h_n, h_n) = \\ &= \underbrace{(h_1, h_1)}_n + \underbrace{(h_2, h_2)}_n + \dots + \underbrace{(h_n, h_n)}_n = n^2 \end{aligned}$$

Пусть  $Hv = (L_1, L_2, \dots, L_n)$ . Тогда  $(Hv, Hv) = L_1^2 + L_2^2 + \dots + L_n^2 = n^2 \Rightarrow \exists i : |L_i| \geq \sqrt{n}$ . Пусть теперь  $(H + J)v = (L_1 + \lambda, L_2 + \lambda, \dots, L_n + \lambda)$ .

$$((H + J)v, (H + J)v) = \underbrace{L_1^2 + L_2^2 + \dots + L_n^2}_{n^2} + 2\lambda(L_1 + L_2 + \dots + L_n) + \lambda^2 n$$

Причем,  $\sum_{i=1}^n L_i = \sum_{j=1}^n v_j \left( \underbrace{\sum_{i=1}^n h_{ij}}_{=0 \text{ при } i \neq 1} \right) = v_1 n$ . Но тогда:

$$((H + J)v, (H + J)v) = n^2 + 2\lambda n + \lambda^2 n$$

Эта парабола принимает минимум в  $\lambda \pm 1$ ,  $\lambda$  — четное  $\Rightarrow$  реальный минимум в  $\lambda = 0, 2$  или  $0, -2$ . Значит в 0 точно принимается минимум  $\Rightarrow \min \geq n^2$ . Поэтому у этого вектора есть координата  $\geq \sqrt{n}$ . Но тогда у  $\left(\frac{H+J}{2}\right)v \geq \frac{\sqrt{n}}{2}$ . Но заметим, что  $\left(\frac{H+J}{2}\right)v$  элементы  $\in \{0, 1\}$ . Но тогда координаты  $\left(\frac{H+J}{2}\right)v$  — значения  $\chi(H_i)$ , где  $H_i$  — это множество, состоящее из

элементов, которые удовлетворяют маске  $i$ -ой строки  $H$ . Но тогда мы получили желаемое  $\square$

**Следствие.** При  $n \rightarrow +\infty \exists M_1, M_2, \dots M_n \forall \chi \exists i |\chi(M_i)| \geq \frac{\sqrt{n}}{2}(1 - o(1))$

*Доказательство неумлучшаемости оценки.*  $\square$

### 3 Распределение простых чисел

**Определение 3.1.**  $\pi(x) = |\{p \leq x | p - \text{простое}\}|$

**Определение 3.2.**  $\theta(x) = \sum_{p \leq x} \ln p$

**Определение 3.3.**  $\psi(x) = \sum_{(p, \alpha), p^\alpha \leq x} \ln p = \sum_{p \leq x} \ln p [\log_p x] = \sum_{p \leq x} \left\lfloor \frac{\ln x}{\ln p} \right\rfloor \leq \sum_{p \leq x} \ln p$

Также введем:

$$\lambda_1 = \overline{\lim}_{x \rightarrow \infty} \frac{\theta(x)}{x}, \lambda_2 = \overline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x}, \lambda_3 = \overline{\lim}_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x}$$

$$\mu_1 = \underline{\lim}_{x \rightarrow \infty} \frac{\theta(x)}{x}, \mu_2 = \underline{\lim}_{x \rightarrow \infty} \frac{\psi(x)}{x}, \mu_3 = \underline{\lim}_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x}$$

**Лемма 3.1.**  $\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$

*Доказательство.*

$$\frac{\theta(x)}{x} = \frac{\sum_{p \leq x} \ln p}{x} \leq \frac{\psi(x)}{x} \leq \frac{\sum_{p \leq x} \ln x}{x} = \frac{\ln x}{x} \sum_{p \leq x} 1 = \frac{\ln x}{x} \pi(x) = \frac{\pi(x)}{x / \ln x}$$

$$\lambda_1 \leq \lambda_2 \leq \lambda_3$$

При  $\beta \in [0, 1)$ :

$$\theta(x) = \sum_{p \leq x} \ln p \geq \sum_{x^\beta < p \leq x} \ln p \geq \sum_{x^\beta < p \leq x} \ln x^\beta = \beta \ln x \sum_{x^\beta < p \leq x} 1 = \beta \ln x (\pi(x) - \pi(x^\beta))$$

Заметим, что  $x > \pi(x)$ :

$$\beta \ln x (\pi(x) - \pi(x^\beta)) \geq \beta \ln x (\pi(x) - x^\beta)$$

$$\frac{\theta(x)}{x} \geq \frac{\beta \pi(x)}{x / \ln x} - \frac{\beta x^\beta \ln x}{x}$$

$$\overline{\lim}_{x \rightarrow \infty} \frac{\theta(x)}{x} \geq \overline{\lim}_{x \rightarrow \infty} \left( \frac{\beta \pi(x)}{x / \ln x} - \frac{\beta x^\beta \ln x}{x} \right) = \overline{\lim}_{x \rightarrow \infty} \frac{\beta \pi(x)}{x / \ln x} \quad \forall \beta \in [0, 1)$$

Теперь, если взять супремум по  $\beta$ , получится

$$\overline{\lim}_{x \rightarrow \infty} \frac{\theta(x)}{x} \geq \overline{\lim}_{x \rightarrow \infty} \frac{\pi(x)}{x / \ln x} \Rightarrow \lambda_1 \geq \lambda_3$$

Итого,  $\lambda_1 \leq \lambda_2 \leq \lambda_3 \leq \lambda_1 \Rightarrow$  они все равны  $\square$

**Теорема 3.1.**

$$\pi(x) \sim \frac{x}{\ln x}$$

**Теорема 3.2** (Чебышев).  $\forall \varepsilon > 0 \exists x_0 \forall x > x_0 :$

$$(1 - \varepsilon) \frac{x}{\ln x} \cdot \ln 2 \leq \pi(x) \leq (1 + \varepsilon) \frac{x}{\ln x} \cdot 4 \ln 2$$

*Доказательство.* Рассмотрим  $C_{2n}^n$ . Заметим, что  $C_{2n}^n < 2^{2n}$ .  $\ln C_{2n}^n < 2n \ln 2$

$$C_{2n}^n = \frac{(2n)!}{n!n!} \geq \prod_{n < p \leq 2n} p \Rightarrow \ln C_{2n}^n \geq \sum_{n < p \leq 2n} \ln p = \theta(2n) - \theta(n)$$

Рассмотрим  $n = 1, 2, \dots, 2^k$ .

$$2n \ln 2 > \ln C_{2n}^n \geq \theta(2n) - \theta(n)$$

$$2n \ln 2 > \theta(2n) - \theta(n)$$

$$2(1 + 2 + \dots + 2^k) \ln 2 > \theta(2^{k+1})$$

$$2^{k+1} \ln 2 > \theta(2^{k+1})$$

Рассмотрим  $2^k \leq x \leq 2^{k+1}$

$$\theta(x) \leq \theta(2^{k+1}) < 2^{k+2} \ln 2 < 4x \ln 2 \Rightarrow \frac{\theta(x)}{x} < 4 \ln 2$$

Получили правое неравенство. Теперь получим левое:

$$C_{2n}^0 + C_{2n}^1 + \dots + C_{2n}^{2n} = 2^{2n} \Rightarrow C_{2n}^n > \frac{2^{2n}}{2n+1}$$

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

$$C_{2n}^n = \frac{(2n)!}{n!n!} = \frac{\prod_{p \leq 2n} p^{\left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \dots}}{\left(\prod_{p \leq 2n} p^{\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \dots}\right)^2} =$$

$$= \prod_{p \leq 2n} p^{\left(\left[\frac{2n}{p}\right] - \left[\frac{n}{p}\right]\right) + \left(\left[\frac{2n}{p^2}\right] - \left[\frac{n}{p^2}\right]\right) + \dots} \leq \prod_{p \leq 2n} p^{\lfloor \log_p(2n) \rfloor} = e^{\psi(2n)} \Rightarrow \ln C_{2n}^n \leq \psi(2n)$$

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

Если  $x \in [2n, 2n+2)$ , то  $\psi(x) \geq \psi(2n) \geq (x-2) \ln 2 - \ln(x+1)$ . Итого:

$$\frac{\psi(x)}{x} \geq \frac{x-2}{x} \ln 2 - \frac{\ln(x+1)}{x} \Rightarrow \mu_2 \geq \ln 2, \mu_3 \geq \ln 2$$

И тогда:

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x/\ln x} \geq \ln 2$$

Но тогда, с какого-то момента:

$$(1 - \varepsilon x) \frac{x}{\ln x} \ln 2 \leq \pi(x)$$

□

**Анекдот:** Райгор учился на кафедре мехмата в девяностые годы и интересовался теорией чисел. Один раз он сидел со своим руководителем на кафедре, и вдруг туда заходит калоритный иностранец с сильным акцентом. Зашел и говорит: "А не расскажите ли вы мне, сколько нулей на конце числа 100!". Они с научруком ему объяснили, что надо посчитать степень вхождения 5 и 2, в общем он понял и ушел. Приходит через неделю и говорит: "Я понял, как посчитать количество нулей на конце числа 100!, а теперь скажите мне, как посчитать количество нулей на конце числа 1000!"

**Утверждение 3.1** (Постулат Бертрана).  $\forall x \geq 2 \exists p \in [x, 2x] = [x, x + x]$

Но это сложно, мы займемся другим вопросом: При каких  $f(x)$  можно рассчитывать на существование  $p \in [x, x + f(x)]$  хотя бы при  $x \geq x_0$ .

**Утверждение 3.2** (Асимптотический Закон Распределения Простых Чисел).  $f(x) = o(x)$

**Утверждение 3.3** (Гипотеза).  $f(x) = O(\ln^2 x)$

## 4 Первообразный Корень

**Определение 4.1.** Пусть  $(a, m) = 1$ . Показатель числа  $a \bmod m$  — это минимальное  $\delta$ , такое, что  $a^\delta \equiv_m 1$ .

**Утверждение 4.1.**  $\delta | \varphi(m)$

**Определение 4.2.** Пусть  $(a, m) = 1$ . Если показатель  $a \bmod m = \varphi(m)$ , то  $a$  называется первообразным корнем и обозначается  $g$ .

**Замечание.** Если по  $\bmod m \exists$  первообразный корень, то  $1, g, g^2 \dots g^{\varphi(m)-1}$  — все взаимно простые с  $m$  остатки.

**Определение 4.3.**  $\text{ind}_g a$  — такое число, что  $g^{\text{ind}_g a} = a$

**Теорема 4.1.** Первообразный корень существует по модулю  $m \Leftrightarrow m \in \{2, 4, p^\alpha, 2p^\alpha\}$ , где  $p$  — нечетное простое

При этом, на данный момент человечество не умеет быстро решать задачу дискретного логарифмирования: по заданному  $a$  найти  $b$ , такое, что  $g^b \equiv a$  (то есть быстрее, чем экспоненциально).

## 4.1 Алгоритм шифрования

У нас есть Алиса, Боб и Ева. Алиса и боб хотят установить некоторый секрет, про который будут знать только они, а все остальные — нет, используя канал связи, который прослушивает Ева. Для этого алиса и боб выбирают  $p, g$  — простое число и его первообразный корень и эта информация открыта для всех. После этого, каждый из них придумывает числа  $a, b$  посылают друг другу  $g^a, g^b$  соответственно. Каждый из них, получив  $g^b, g^a$  возводит его в свою степень, оба получают  $g^{ab}, g^{ab}$ .

Алиса	Открытый канал	Боб
$a$	$p, g$	$b$
↓	↓	↓
$a, g^a$	$g^a, p, g, g^b$	$b, g^b$
↓	↓	↓
$a, g^a, (g^b)^a$	$g^a, p, g, g^b$	$b, g^b, (g^a)^b$
↓		↓
$g^{ab}$		$g^{ab}$

[Подробнее про этот протокол](#)

## 4.2 Существование первообразного корня

**Утверждение 4.2.** *Не существует первообразного корня  $\mod 2^\alpha, \alpha \geq 3$*

*Доказательство.* Предположим противное. Тогда  $(a, 2^\alpha) = 1 \Leftrightarrow a \equiv_2 1, \varphi(2^\alpha) = 2^{\alpha-1}, a = 2t + 1$ . Тогда

$$\begin{aligned}
 a^2 &= 4t^2 + 4t + 1 = 4t(t+1) + 1 = 8t_1 + 1 \\
 a^4 &= 64t^2 + 16t + 1 = 16t_2 + 1 \\
 &\vdots \\
 a^{2^k} &= 2^{k+2}t_k + 1, a^{2^{\alpha-2}} = 2^\alpha t_{\alpha-2} + 1 \equiv_{2^\alpha} 1
 \end{aligned}$$

□

**Утверждение 4.3.** *Существует первообразный корень  $\mod p$*

*Доказательство.* Пусть  $\delta_i$  — показатель числа  $i \mod p, \tau = \text{НОК}(\delta_1, \delta_2, \dots, \delta_{p-1})$ . Заметим, что сравнению  $x^\tau \equiv_p 1$  удовлетворяют все  $x \in \{1, 2, 3, \dots, p-1\}$ . Тогда  $\tau \geq p-1$ . Пусть  $\tau = q_1^{\alpha_1} q_2^{\alpha_2} \dots q_k^{\alpha_k}$ . Тогда  $\forall i \in \{1, \dots, k\} \exists \delta \in \{\delta_1, \dots, \delta_k\} : \delta = a_i \cdot q_i^{\alpha_i}$  (т.к. иначе НОК бы делился на меньшую степень  $q_i$ ). Возьмем за  $x_i$ , показателем которого является  $\delta$  для данного  $i$ . Тогда  $x_i^{\alpha_i}$  имеет показатель  $q_i^{\alpha_i}$ . Теперь рассмотрим  $g = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_k^{\alpha_k}$ . □

**Упражнение.** *Довести доказательство*

**Лемма 4.1.** *Пусть  $g$  — первообразный корень  $\mod p \Rightarrow \exists t : (g + pt)^{p-1} = 1 + pu$ , где  $(u, p) = 1$*

*Доказательство.*

$$\begin{aligned}
 (g + pt)^{p-1} &= g^{p-1} + (p-1)g^{p-2}pt + p^2(\dots) = 1 + pv + p((p-1)g^{p-2}t + p(\dots)) = \\
 &= 1 + p(v + (p-1)g^{p-2}t + p(\dots))
 \end{aligned}$$

Итого, такое  $t$  можно подобрать, т.к.  $v, p-1, g^{p-2}$  — константы □

*Доказательство.* Существует первообразный корень  $\text{mod } p^\alpha$  □

*Доказательство.*  $m = p^\alpha, \alpha \geq 2, \varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$ . Пусть  $\delta$  — порядок  $(g+pt)$ , тогда  $(g+pt)^\delta \equiv_{p^\alpha} 1 \Rightarrow (g+pt)^\delta \equiv_p 1$ . При этом,  $g+pt$  — первообразный корень  $\text{mod } p \Rightarrow (p-1) | \delta$ . С другой стороны,  $\delta | \varphi(p-1) \Rightarrow \delta = p^k(p-1)$ . Рассмотрим числа вида  $(g+pt)^{p^k(p-1)}$ .

$$(g+pt)^{p(p-1)} = (1+pk)^p = 1 + p^2u + p^3v = 1 + p^2(u+pv) = 1 + p^2u_1, (u_1, p) = 1$$

$$(g+pt)^{p^2(p-1)} = (1+p^2u_1)^p = 1 + p^3u_2, (u_2, p) = 1$$

$$\vdots$$

$$(g+pt)^{p^{\alpha-2}(p-1)} = 1 + p^{\alpha-1}u_{\alpha-2}, (u_{\alpha-2}, p) = 1$$

Таким образом, получили, что  $g+pt$  — первообразный корень  $\text{mod } p$  □

**Утверждение 4.4.** *Существует первообразный корень  $\text{mod } 2p^\alpha$*

*Доказательство.* Заметим, что  $\varphi(2p^\alpha) = \varphi(p^\alpha)$ . Но тогда одно из чисел  $g, g+p^\alpha$  является первообразным корнем, в зависимости от чётности числа  $g$  □

**Теорема 4.2** (Шевалле). *Пусть  $F(x_1, \dots, x_n)$  — многочлен, такой, что  $\deg F < n$ . Тогда количество решений  $F(x_1, \dots, x_n) \equiv_p 0$  делится на  $p$ .*

*Доказательство.*

$$N = \sum_{x_1=1}^p \sum_{x_2=1}^p \dots \sum_{x_n=1}^p (1 - F^{p-1}(x_1, x_2, \dots, x_n))$$

$$N \equiv_p 0 \Leftrightarrow \sum_{x_1=1}^p \sum_{x_2=1}^p \dots \sum_{x_n=1}^p F^{p-1}(x_1, x_2, \dots, x_n) \equiv_p 0$$

Докажем, что  $\sum_{x_1=1}^p \sum_{x_2=1}^p \dots \sum_{x_n=1}^p x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \equiv_p 0, 0 \leq \alpha_i, \sum \alpha_i \leq (n-1)(p-1)$

$$\sum_{x_1=1}^p \sum_{x_2=1}^p \dots \sum_{x_n=1}^p x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n} \equiv_p \left( \sum_{x_1=1}^p x_1^{\alpha_1} \right) \left( \sum_{x_2=1}^p x_2^{\alpha_2} \right) \dots \left( \sum_{x_n=1}^p x_n^{\alpha_n} \right)$$

1.  $\exists i : \alpha_i = 0 \Rightarrow \sum_{x_i=1}^p x_i^{\alpha_i} \equiv_p 0$
2.  $p = 2$ . Тогда  $\alpha_1 + \alpha_2 + \dots + \alpha_n \leq 1 \Rightarrow$  аналогично случаю 1.
3. Пусть  $p \geq 3, \forall i \alpha_i \geq 1 \Rightarrow \exists i : 1 \leq \alpha_i \leq p-2$

$$S = \sum_{x_i=1}^p x_i^{\alpha_i}, g^{\alpha_i} S \equiv_p \sum_{x_i=1}^p (gx_i)^{\alpha_i} \equiv_p S \Rightarrow S \equiv 0$$

□

## 5 Тесты на простоту чисел

Хотелось бы чтобы тест на простоту работал за  $O(poly(\log n))$ . Они делятся на вероятностные и детерминированные. Вероятностные тесты определяют простоту с некоторой вероятностью, при этом, если они ломаются, то искомое число "почти простое". Детерминированные тесты, в основном, придуманы для простых чисел особого вида, например, для чисел Мерсенна:  $2^p - 1, p$  — простое. Существует один алгоритм [Агравала — Каяла — Саксены](#), но константа там настолько большая, что данный тест непригоден для использования.

### 5.1 Тест Ферма на Простоту

Пусть требуется проверить, является ли число  $N$  простым.

1. Проверяем, что  $N$  не делится на первые простые числа
2. Выбираем произвольное  $a$ . Если  $(a, N) \neq 1 \Rightarrow N$  точно не простое.
3. Считаем  $a^{N-1}$ . Если  $\equiv_N 1$ , то переходим к пункту 2, иначе  $N$  — не простое

**Определение 5.1.** Пусть  $B_F = \{a \in \mathbb{Z}_N^* | a^{N-1} \equiv_N 1\}$ . Тогда  $B_F \neq \mathbb{Z}_N^* \Rightarrow |B_F| \leq \frac{1}{2} |\mathbb{Z}_N^*|$

*Первое доказательство.*  $B_F$  — подгруппа в  $\mathbb{Z}_N^*$ . Тогда по теореме Лагранжа,  $|\mathbb{Z}_N^*| : |B_F| \Rightarrow |B_F| \leq \frac{1}{2} |\mathbb{Z}_N^*|$  □

*Второе доказательство.* Домножим  $B_F$  на остаток  $a$ , не лежащий в  $B_F$ . Получится число не из  $B_F$ . Но Тогда  $|B_F| \leq \frac{1}{2} |\mathbb{Z}_N^*|$  □

**Определение 5.2.**  $N$  называется числом Кармайкла, если  $B_F = \mathbb{Z}_N^*$

**Утверждение 5.1.** Если  $N$  — не простое и не Число Кармайкла, то после  $k$  независимых проверок теста Ферма,  $P(N \text{ — псевдопростое}) = \frac{1}{2^k}$

*Доказательство.* □

**Теорема 5.1.**  $N$  — число Кармайкла тогда и только тогда, когда

1.  $N$  свободно от квадратов
2.  $N = p_1 p_2 \dots p_s \Rightarrow p_i - 1 \mid N - 1$

*Доказательство.*

$\Leftarrow$  Хотим проверить, что  $a^{N-1} \equiv_N 1$ , если  $(a, N) = 1$ . Заметим, что  $a^{p_i-1} \equiv_{p_i} 1 \Rightarrow a^{N-1} \equiv_{p_i} 1$ . Но тогда по КТО,  $a^{N-1} \equiv_N 1$ .

$\Rightarrow$  Докажем от противного. Пусть  $n = p^k s, k \geq 2$ . Тогда  $a^{N-1} \equiv_N 1 \Rightarrow a^{N-1} \equiv_{p^k} 1 \Rightarrow a^{N-1} \equiv_{p^2} 1$ . Пусть  $g$  — первообразный корень  $\mod p^2 \Rightarrow \text{ord}(g) = p(p-1)$ . Найдем  $a : \begin{cases} a \equiv_{p^k} g \\ a \equiv_s 1 \end{cases}$ . Такое существует по КТО. Тогда  $a^{N-1} \equiv_{p^2} g^{N-1} \equiv_{p^2} 1 \Rightarrow N : p$ , но противоречие с тем, что  $N - 1 : p$ , а  $(N, N-1) = 1$ .

Пусть  $N = p_1 p_2 \dots p_s, g_i$  — первообразный корень  $\mod p_i$ . Найдем  $a$ , такой, что  $\begin{cases} a \equiv_{p_i} g_i \\ a \equiv_{p_j} 1 \end{cases}$ .  $a^{N-1} \equiv_N 1 \Rightarrow g_i^{N-1} \equiv_{p_i} 1 \Rightarrow N - 1 : p_i - 1$ .

□

### 5.1.1 Свойства чисел Кармайкла

1. Числа Кармайкла нечетны
2. Числа Кармайкла представимы в виде  $p_1 \dots p_s, s \geq 3, p_i$  — простое
3. Если для некоторого  $k$ , верно, что  $6k + 1, 12k + 1, 18k + 1$  — простые, то  $(6k + 1)(12k + 1)(18k + 1)$  — число Кармайкла, например  $7 \cdot 13 \cdot 19$  — число Кармайкла

## 5.2 Символ Якоби

Как улучшить Тест Ферма? Большие простые числа нечетные, поэтому можно проверять  $a^{\frac{N-1}{2}} \equiv_N \pm 1$ . Заметим, что для  $p$  — простого верно  $a^{\frac{p-1}{2}} \equiv_p 1 \Leftrightarrow a$  — вычет  $\bmod p$

**Определение 5.3.** Пусть  $N$  — нечетное число. Символ Якоби:

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_s}\right)$$

Где  $\left(\frac{a}{p_i}\right)$  — символы Лежандра

### 5.2.1 Свойства Символа Якоби

1.  $\left(\frac{a}{N}\right) \equiv_N a^{\frac{N-1}{2}}$
2.  $\left(\frac{-1}{N}\right) = (-1)^{\frac{N-1}{2}}$
3.  $\left(\frac{2}{N}\right) = (-1)^{\frac{N^2-1}{8}}$
4.  $\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right) \left(\frac{b}{N}\right)$
5.  $\left(\frac{M}{N}\right) \left(\frac{N}{M}\right) = (-1)^{\frac{N-1}{2} \frac{M-1}{2}}$ , если  $(M, N) = 1$

## 5.3 Тест Соловея - Штрассена

Алгоритм такой же, как и в тесте Ферма, только здесь мы проверяем равенство  $\left(\frac{a}{N}\right) \equiv_N a^{\frac{N-1}{2}}$  для каждого  $a$ .

**Теорема 5.2.** Обозначим за  $B_{SS} = \{a \in \mathbb{Z}_N^* | a^{\frac{N-1}{2}} \equiv_N \left(\frac{a}{N}\right)\}$ . Тогда

1.  $B_{SS} = \mathbb{Z}_N^* \Leftrightarrow N$  — простое
2.  $N$  — составное  $\Leftrightarrow |B_{SS}| \leq \frac{1}{2} |\mathbb{Z}_N^*|$
3.  $B_{SS} \subset B_F$

*Доказательство.*

1.  $\Leftarrow$  по свойству символа Лежандра



$\Rightarrow B_{SS} = \mathbb{Z}_N^* \Rightarrow B_F = \mathbb{Z}_N^*$ . Пусть  $N$  — не простое, тогда  $N$  — число Кармайкла,  $N = p_1 p_2 \dots p_s$ . Пусть  $b$  — квадратичный невычет  $\mod p_1$ . Возьмем  $\begin{cases} a \equiv_{p_1} b \\ a \equiv_{p_i} 1 \end{cases}$

$$a^{\frac{N-1}{2}} \equiv_N \left( \frac{a}{N} \right) \equiv_N -1$$

Противоречие, т.к.  $1 \equiv_{p_2} -1$

2.  $B_{SS}$  — подгруппа в  $\mathbb{Z}_N^* \Rightarrow |\mathbb{Z}_N^*| : |B_{SS}|$  по теореме Лагранжа

□

## 6 Диофантовы приближения, теорема Дирихле

Рассмотрим число  $\pi = 3.1415926\dots$

$$\left| \pi - \frac{314}{100} \right| = 0.0015926\dots \quad \left| \pi - \frac{22}{7} \right| = 0.0012\dots$$

**Теорема 6.1.** (Дирихле) Пусть  $\alpha \notin \mathbb{Q}$ . Тогда  $\exists$  бесконечно много дробей  $\frac{p}{q}$ , что

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{q^2}$$

*Доказательство.*  $Q \in \mathbb{N}$ . Рассмотрим деление отрезка  $[0, 1]$  на отрезки длины  $\frac{1}{Q}$ .

Рассмотрим  $\{\alpha x\}$ , где  $x = 0, 1, \dots, Q$ .  $\exists x_1, x_2 : x_1 > x_2$  и  $|\{\alpha x_1 - \alpha x_2\}| \leq \frac{1}{Q}$

$$|\alpha x_1 - [\alpha x_1] - \alpha x_2 + [\alpha x_2]| \leq \frac{1}{Q}$$

$$\left| \alpha \underbrace{(x_1 - x_2)}_q - \underbrace{([\alpha x_1] - [\alpha x_2])}_p \right| \leq \frac{1}{Q}$$

Если  $q \leq Q$

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}$$

□

**Замечание.** Покажем, как получать новые дроби:

Пусть  $\alpha = \left| \alpha - \frac{p}{q} \right|, \alpha \leq \frac{1}{q^2}, a > 0$

Возьмем  $Q_1 \in \mathbb{N} : \frac{1}{Q_1} \leq a$ . По  $Q_1$  найдем соответствующие ей  $\frac{p_1}{q_1}$ .

**Почему полученные  $p_1, q_1$  не совпадают с  $p, q$ ?**

Как мы доказали, верно следующее:

$$\left| \alpha - \frac{p_1}{q_1} \right| \leq \underbrace{\frac{1}{q_1 Q_1}}_{< \alpha} \leq \frac{1}{q_1^2}.$$

$$\left| \alpha - \frac{p_1}{q_1} \right| \leq \frac{1}{q_1 Q_1} \leq \frac{\alpha}{q_1} \leq \left| \alpha - \frac{p}{q} \right| \implies \frac{p_1}{q_1} \neq \frac{p}{q}$$

## 6.1 Теорема Минковского. Еще одно доказательство теоремы Дирихле

**Теорема 6.2.** (Минковского) Пусть  $\Omega \subset \mathbb{R}^2 : \Omega$  выпукло, симметрично относительно 0,  $S(\Omega) > 4$ . Тогда  $(\Omega \cap \mathbb{Z}^2) \setminus 0 \neq \emptyset$

*Доказательство.* Рассмотрим  $N_p$  - все координаты в  $\mathbb{Z}^2 \cap \Omega$ , имеющие вид  $(\frac{a}{p}, \frac{b}{p})$ ,  $a, b, p \in \mathbb{N}$ .

$$\frac{N_p}{p^2} \rightarrow S(\Omega) > 4, \text{ при } p \rightarrow \infty$$

Этот факт оставляется без доказательства. Обещали не спрашивать его на экзамене.

$$\exists P : \forall p \geq P \quad \frac{N_p}{p^2} > 4$$

$$N_p > (2p)^2 \implies \exists a = \left( \frac{a_1}{p}, \frac{a_2}{p} \right), b = \left( \frac{b_1}{p}, \frac{b_2}{p} \right) : a \neq b, a_1 \equiv b_1(2p), a_2 \equiv b_2(2p)$$

$$\text{Рассмотрим } \frac{a-b}{2} = \left( \frac{a_1-b_1}{2p}, \frac{a_2-b_2}{2p} \right) \in \mathbb{Z}^2$$

1.  $-b \in \Omega$ , так как  $\Omega$  - центрально симметричная.

2.  $\frac{a-b}{2} \in \Omega$ , так как  $\Omega$  выпукло.

□

**Замечание.** Есть еще усиление теоремы Минковского - в случае замкнутого множества оценка становится нестрогой ( $\geq 4$ ).

Приведем еще одно доказательство теоремы Дирихле

*Доказательство.*  $\Omega = \{(x, y) : |y - \alpha x| \leq \frac{1}{Q}, |x| \leq Q\}$ . Если нарисовать на плоскости фигуру, то получится параллелограмм. По формуле площади:

$$S(\Omega) = 4 \implies \text{по теореме } \exists (q, p) \in \Omega, q > 0$$

$$|p - \alpha q| \leq \frac{1}{Q} \implies \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}$$

□

## 7 Цепные дроби

### 7.1 Конечная цепная дробь

$$a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{1}{a_3 + \dots}}}$$

$$a_0 \in \mathbb{Z}, a_i \in \mathbb{N} \forall i \geq 1.$$

Раскрыв скобки, получим  $\alpha := [a_0; a_1, a_2, a_3, \dots, a_n] \in \mathbb{Q}$

**Определим теперь цепную дробь индуктивно:**

1.  $[a_0] = \frac{a_0}{1}$
2.  $[a_0; a_1, \dots, a_n] = a_0 + \frac{1}{[a_1; a_2, \dots, a_n]} = a_0 + \frac{1}{\frac{p}{q}} = a_0 + \frac{q}{p} = \frac{a_0 p + q}{p}$

**Определение 7.1.** Подходящая дробь к  $\alpha$  - дробь  $\frac{p_k}{q_k} = [a_0; a_1, a_2, \dots, a_k]$ .

**Теорема 7.1.**

$$p_{k+2} = a_{k+2}p_{k+1} + p_k$$

$$q_{k+2} = a_{k+2}q_{k+1} + q_k$$

*Доказательство.* Успеем проверить только переход : (

$$\frac{p_0}{q_0} = [a_0] = \frac{a_0}{1}$$

$$\frac{p_1}{q_1} = [a_0; a_1] = a_0 + \frac{1}{a_1} = \frac{a_0 a_1 + 1}{a_1}$$

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

Теперь проверяем утверждение:

$$p_2 \stackrel{?}{=} a_2 p_1 + p_0 = a_2 a_0 a_1 + a_2 + a_0$$

$$q_2 = a_2 q_1 + q_0 = a_2 a_1 + 1$$

*Пытаемся успеть сделать переход:*  $[a_0; a_1, \dots, a_m] = a_0 + \frac{1}{[a_1; a_2, \dots, a_m]}$

Не успели...

□

*Проделаем переход индукции с прошлой лекции, напомним, что хотим доказать:*

**Теорема 7.2.**

$$p_{k+2} = a_{k+2}p_{k+1} + p_k$$

$$q_{k+2} = a_{k+2}q_{k+1} + q_k$$

*Доказательство.* Пусть  $[a_0; a_1, \dots, a_n] = \frac{p_n}{q_n}, [a_1; a_2, \dots, a_k] = \frac{p'_k}{q'_k}$

$$a_0 + \frac{1}{[a_1; a_2, \dots, a_n]} = a_0 + \frac{1}{\frac{p'_n}{q'_n}} = a_0 + \frac{q'_n}{p'_n} = \frac{a_0 p'_n + q'_n}{p'_n}$$

$$p_n = a_0 p'_n + q'_n = a_0(a_n p'_{n-1} + p'_{n-2}) + a_n q'_{n-1} + q'_{n-2} = a_n \underbrace{(a_0 p'_{n-1} + q'_{n-1})}_{p_{n-1}} + \underbrace{a_0 p'_{n-2} + q'_{n-2}}_{p_{n-2}}$$

□

**Замечание.**  $p_{n+2} \cdot q_{n+1} - p_{n+1} q_{n+2} = p_n q_{n+1} - q_n p_{n+1}$

Так как  $p_0 q_1 - q_0 p_1 = a_0 a_1 - (a_1 a_0 + 1) = -1$ ,  $p_n q_{n+1} - q_n p_{n+1} = (-1)^{n+1}$  и  $\frac{p_n}{q_n}$  нельзя сократить.

**Замечание.**  $p_{n+2} q_n - q_{n+2} p_n = a_{n+2} (-1)^n$

Из прошлого замечания получаем еще одно тождество:

$$p_{n+2} q_n - q_{n+2} p_n = a_{n+2} \underbrace{(p_{n+1} q_n - q_{n+1} p_n)}_{(-1)^n}$$

**Утверждение 7.1.** Из первого замечания можно понять очень важный факт:

1. Дроби с нечетным  $n$  убывают
2. Дроби с четным  $n$  возрастают
3. Но все они отличаются друг от друга на небольшое число -  $\frac{(-1)^n}{q_n q_{n+1}}$

## 7.2 Бесконечная цепная дробь

Формально почти все операции над цепными дробями остаются без изменений, но значение дроби определяется как предел подходящего ряда:

$$[a_0; a_1, \dots, a_n, \dots] = \lim_{n \rightarrow \infty} \frac{p_n}{q_n}$$

**Теорема 7.3.** (Докажут на семинаре)

Предел всегда существует.

**Пример.**  $[1; 1, 1, \dots, 1] = ?$

Пусть  $[1; 1, 1, \dots, 1] = \alpha$ .  $1 + \frac{1}{\alpha} = \alpha \implies \alpha = \frac{1+\sqrt{5}}{2}$

**Теорема 7.4.** Если цепная дробь периодична, то ее значение будет являться квадратичной иррациональностью (решением квадратного уравнения с иррациональными коэффициентами)

*Доказательство.*  $\alpha = [a_0; a_1, \dots, a_k, \overline{b_1, b_2, \dots, b_m}]$ .

Аналогично с примером обозначаем дробь  $[b_1; b_2, \dots, b_m]$  за  $\beta$ . Тогда:

$$b_m + \frac{1}{\beta} = \frac{\beta b_m + 1}{\beta}$$

$$\frac{\beta}{\beta b_m + 1} + b_{m-1} = \frac{\beta + \beta b_{m-1} b_m + b_{m-1}}{\beta b_m + 1}$$

Понятно, что если выражать дальше  $\beta$ , то в числителе и знаменателе будет получаться линейная функция от  $\beta$ .  $\beta = \frac{c_1 \beta + c_2}{c_3 \beta + c_4} \implies \beta$  - квадратичная иррациональность. □

**Теорема 7.5.** (б/д) Верно и обратное.

**Теорема 7.6.**  $\forall \psi : \psi(q) \rightarrow +\infty \exists \alpha > 0 : \text{неравенство } \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{\psi(q)}$  имеет бесконечно много решений в дробях  $\frac{p}{q}$ .

*Доказательство.* Пусть построили дробь  $\alpha = [a_0; a_1, \dots]$ . Найдем теперь  $a_{n+1}$  из соображений:

$$\alpha - \frac{p}{q} \leq \frac{1}{q_n q_{n+1}} < \frac{1}{\frac{1}{\psi(q_n) q_n}} < \frac{1}{\psi(q_n)}, \text{если выбрать } a_{n+1} \text{ } q_{n+1} = a_{n+1} q_n + q_{n-1} > \psi(q_n) \cdot \frac{1}{q_n} \quad \square$$

**Определение 7.2.**  $\alpha \in A \iff \alpha$  является корнем какого-то многочлена с целыми коэффициентами.

Говорят,  $A$  - множество трансцендентных чисел

**Замечание.** Так как  $\mathbb{R}$  - континуум, а  $A$  - не больше множества всех многочленов, которых счетно, то есть числа не в  $A$ .

**Теорема 7.7.** (Лувилля) Пусть  $\alpha \in A, \deg \alpha = d$ , тогда  $\exists c(\alpha) : \forall \frac{p}{q} \left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^d}$

**Определение 7.3.**  $\alpha \in A$  называется алгебраическим числом степени  $d$ , если min степень многочлена, корнем которого является  $\alpha$ , равна  $d$ .

$$\alpha \in A, \deg \alpha = d. f(x) = a_d x^d + \dots + a_1 x + a_0$$

$$1. \left| \alpha - \frac{p}{q} \right| \geq 1 \implies \left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q^d} \implies c_1(\alpha) = 1$$

$$2. \left| \alpha - \frac{p}{q} \right|$$

$$\frac{p}{q} \neq 0, f\left(\frac{p}{q}\right) = \frac{a_d p^d + \dots + a_0 q^d}{q^d}. \left| f\left(\frac{p}{q}\right) \right| \geq \frac{1}{q^d}$$

Положим  $c(\alpha) = \min\{c_1(\alpha), c_2(\alpha)\}$

$$\left| f\left(\frac{p}{q}\right) \right| = \left| \alpha - \frac{p}{q} \right| \cdot \left| \alpha_1 - \frac{p}{q} \right| \cdot \dots \cdot \left| \alpha_{d-1} - \frac{p}{q} \right| \cdot a_d$$

$$\left| \alpha_i - \frac{p}{q} \right| = \left| \alpha_i - \alpha + \alpha - \frac{p}{q} \right| \leq |\alpha_i - \alpha| + \left| \alpha - \frac{p}{q} \right| \leq \underbrace{|\alpha_i - \alpha|}_{\bar{c}_i(\alpha)}$$

$$\left| \alpha - \frac{p}{q} \right| \geq \frac{1}{q^d} \cdot \frac{1}{a_d \prod_{i=1}^{d-1} \bar{c}_i(\alpha)}$$

**Теорема 7.8** (Roth). Пусть  $\alpha \notin \mathbb{Q}, \alpha \in \mathbb{A}$ . Тогда  $\forall \varepsilon > 0 \exists c(\alpha) :$

$$\forall p, q \quad \left| \alpha - \frac{p}{q} \right| \geq \frac{c(\alpha)}{q^{2+\varepsilon}}$$

**Теорема 7.9.** Пусть  $\alpha \notin \mathbb{Q} \Rightarrow \exists$  бесконечно много различных  $\frac{p}{q}$ , таких, что  $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{\sqrt{5}q^2}$

**Теорема 7.10.**  $\forall \varepsilon > 0 \exists$  лишь конечное число различных  $\frac{p}{q} : \left| \frac{1+\sqrt{5}}{2} - \frac{p}{q} \right| < \frac{1}{(\sqrt{5}+\varepsilon)q^2}$

**Теорема 7.11.** Если выкинуть числа, которые ведут себя так же, как и  $\frac{1+\sqrt{5}}{2}$ , то любое из оставшихся чисел удовлетворяют  $\left| \alpha - \frac{p}{q} \right| \leq \frac{1}{\sqrt{8}q^2}$  для бесконечно многих

**Утверждение 7.2** (Гипотеза Заремба, Коробова, Бахвалова).  $\forall p$  — простое  $\exists a \in \{1, 2, \dots, p-1\}$ , такое, что все ненулевые частные в разложении  $\frac{a}{p}$  в цепную дробь не превосходят 5.

### 7.3 Трансцендентность и иррациональность числа $e$

**Теорема 7.12.**  $e \notin \mathbb{Q}$ .

*Доказательство.* Предположим противное, тогда  $e = \frac{m}{n} \Rightarrow e \cdot n! \in \mathbb{Z}$

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

$$en! = \sum_{k=0}^{\infty} \frac{n!}{k!} = A + \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \dots = A + \frac{1}{n+1} \underbrace{\left( 1 + \frac{1}{n+2} + \dots \right)}_B$$

$$B < 1 + \frac{1}{n+2} + \frac{1}{(n+2)^2} + \dots \leq \frac{1}{1 - \frac{1}{n+2}} = \frac{n+2}{n+1}$$

$$0 < B \frac{1}{n+1} < \frac{n+2}{n+1} < 1, n \geq 1$$

Получили противоречие □

**Утверждение 7.3** (Тождество Эрмита). Пусть  $f(x)$  — многочлен степени  $d$ . Рассмотрим

$$\int_0^x f(t)e^{-t} dt = F(0) - e^{-x}F(x), F(x) = f(x) + f'(x) + \dots + f^{(d)}(x)$$

*Доказательство.*

$$\begin{aligned} \int_0^x f(t)e^{-t} dt &= -f(t)e^{-t} \Big|_0^x + \int_0^x f'(t)e^{-t} dt = f(0) - f(x)e^{-x} + \int_0^x f'(t)e^{-t} dt = \dots = \\ &= f(0) + f'(0) + \dots + f^{(d)}(0) - e^{-x}(f(x) + f'(x) + \dots + f^{(d)}(x)) \end{aligned}$$

□

**Утверждение 7.4.** Пусть  $g(x)$  — многочлен с целыми коэффициентами. Тогда все коэффициенты  $k$ -ой производной этого многочлена делятся на  $k!$

*Доказательство.* Рассмотрим произвольный моном  $a_n x^n$ . Если  $n \leq k-1$ , то после дифференцирования,  $a_n \rightarrow 0$ . Иначе,  $a_n \rightarrow a_n n(n-1) \dots (n-k+1)x^{n-k} \Rightarrow$  т.к. произведение  $k$  последовательных чисел делится на  $k!$ , то  $a_n n(n-1) \dots (n-k+1) \cdot k!$  □

**Теорема 7.13.**  $e \notin \mathbb{A}$

*Доказательство.* Предположим противное, тогда  $e$  является корнем  $a_mx^m + a_{m-1}x^{m-1} + \dots + a_0$ , причем  $a_0 \neq 0$ . Рассмотрим

$$\begin{aligned} \sum_{x=0}^m a_x(F(0)e^x - F(x)) &= \sum_{x=0}^m \left( a_x e^x \int_0^x f(t)e^{-t} dt \right) \\ \sum_{x=0}^m a_x F(0)e^x &= F(0) \sum_{x=0}^m a_x e^x = 0 \\ \Rightarrow - \sum_{x=0}^m a_x F(x) &= \sum_{x=0}^m \left( a_x e^x \int_0^x f(t)e^{-t} dt \right) \end{aligned}$$

Рассмотрим многочлен  $f(x) = \frac{1}{(n-1)!} x^{n-1} ((x-1)(x-2)\dots(x-m))^n$ .  $\deg f = nm + n - 1$ . Посмотрим на  $a_0 F(0) = a_0 (f(0) + f'(0) + \dots + f^{(d)}(0)) = a_0 (f^{n-1}(0) + \dots + f^{(d)}(0))$ , т.к.  $f^{(i)}(0) = 0$  при  $i \leq n-2$ . При этом,  $f^{(n-1)}(0) = ((-1)(-2)\dots(-m))^n = a_0((-1)^{mn}(m!)^n)$  (остальные слагаемые будут содержать  $x$  в ненулевой степени). Но тогда  $a_0 F(0) = a_0((-1)^{mn}(m!)^n) + nA$ ,  $A \in \mathbb{Z}$ , т.к. коэффициенты оставшихся производных делятся на  $n$ . Теперь рассмотрим  $-(a_1 F(1) + a_2 F(2) + \dots + a_m F(m)) = Bn$  по аналогичным рассуждениям.  $\Rightarrow -\sum_{x=0}^m a_x F(x) = a_0((-1)^{mn}(m!)^n) + Cn$ . Существует бесконечно много  $n$ , таких, что  $a_0((-1)^{mn}(m!)^n)$  не делится на  $n$ . Выберем такое  $n$  и получим, что  $-\sum_{x=0}^m a_x F(x) \in \mathbb{Z} \setminus \{0\}$ .

$$\begin{aligned} \left| \sum_{x=0}^m a_x e^x \int_0^x f(t)e^{-t} dt \right| &\leq \sum_{x=0}^m |a_x| e^x \int_0^x |f(t)| e^{-t} dt = (*) \\ t \in \{0, \dots, m\} &\Rightarrow |f(t)| \leq \frac{1}{(n-1)!} m^{mn+n-1} \\ (*) &\leq \frac{1}{(n-1)!} m^{nm+n-1} \sum_{x=0}^m |a_x| e^x \int_0^x e^{-t} dt \leq \frac{1}{(n-1)!} m^{nm+n-1} \sum_{x=0}^m |a_x| e^x = \\ &= \frac{1}{(n-1)!} \frac{(m^{m+1})^n \cdot c(e)}{m} \rightarrow 0, n \rightarrow \infty \end{aligned}$$

□

## 7.4 7-ая проблема Гильберта

**Задача** (7-ая проблема Гильберта). Верно ли, что  $\alpha, \beta \in \mathbb{A} \Rightarrow \alpha^\beta \in \mathbb{A}$ ?

**Теорема 7.14.** Если  $\alpha \notin \{0, 1\}, \alpha \in \mathbb{A}, \beta \in \mathbb{A} \setminus \mathbb{Q} \Rightarrow \alpha^\beta \notin \mathbb{A}$

Доказана А.О. Гельфандом.

**Утверждение 7.5.**  $e^\pi \notin \mathbb{A}$

*Доказательство.* Предположим противное. Известно, что  $(e^\pi)^i = e^{i\pi} = -1 \Rightarrow -1$  должно быть Трансцендентным □

## 8 Геометрия чисел

**Теорема 8.1** (Минковского). Пусть  $\Omega \subset \mathbb{R}^n$ ,  $\Omega$  — выпукло, симметрично относительно  $O$ , и  $V(\Omega) > 2^n$  (или  $\geq 2^n$  для случая замкнутого  $\Omega$ ). Тогда  $\Omega \cap \mathbb{Z}^n \setminus \{0\} \neq \emptyset$

*Доказательство.* Рассмотрим  $N_p = \left| \frac{1}{p} \mathbb{Z}^n \cap \Omega \right|$ . Интуитивно понятно (дается без доказательства), что

$$\frac{N_p}{p^n} \rightarrow V(\Omega)$$

Т.к.  $\frac{N_p}{p^n}$  — количество "кубиков" размера  $\frac{1}{p}$  внутри  $\Omega$

$$\Rightarrow \exists p_0 \forall p > p_0 \frac{N_p}{p^n} > 2^n \Rightarrow N_p > (2p)^n$$

Тогда рассмотрим  $a = \left( \frac{a_1}{p}, \frac{a_2}{p}, \dots, \frac{a_n}{p} \right), b = \left( \frac{b_1}{p}, \frac{b_2}{p}, \dots, \frac{b_n}{p} \right) \in \Omega$ , такие, что  $\forall i \ a_i \equiv_{2p} b_i \Rightarrow \frac{a-b}{2} \in \mathbb{Z}^n \setminus \{0\}$   $\square$

Рассмотрим  $\mathbb{R}^n$  и базис в нем  $a_1, a_2, \dots, a_n$ .

**Определение 8.1.** Решетка — это множество точек  $\Lambda = \{b_1 a_1 + \dots + b_n a_n | b_i \in \mathbb{Z}\}$

**Пример.** В  $\mathbb{R}^2$  и базиса  $(0, 1), (1, 0)$  решеткой является  $\mathbb{Z}^2$

**Теорема 8.2.**  $\Lambda \subset \mathbb{R}^n$  является решеткой  $\Leftrightarrow \Lambda$  образует группу по сложению,  $\Lambda$  дискретно и "заполняет все пространство". То есть, если

1. **Дискретность:** Каждая точка  $\Lambda$  изолированная
2. **"Заполнение всего  $\mathbb{R}^n$ ":**  $\exists r > 0 \forall x \in \Lambda \ \overset{\circ}{B}(x) \cap \Lambda \neq \emptyset$

**Определение 8.2.** Определителем  $\Lambda$  (детерминантом  $\Lambda$ ) называется величина  $\det \Lambda$ , равная модулю определителя матрицы, составленной из векторов произвольного базиса  $\Lambda$ .

**Теорема 8.3** (Минковского). Пусть  $\Omega \subset \mathbb{R}^n$  — выпуклое и симметричное относительно  $O$  множество. Пусть  $\Lambda$  — решетка, и  $V(\Omega) > 2^n \det \Lambda$ . Тогда  $(\Omega \cap \Lambda) \setminus \{0\} \neq \emptyset$

*Доказательство.* Доказательство аналогично доказательству обычной теоремы Минковского.  $\square$

**Определение 8.3.** Критический определитель  $\Omega$  —  $\Delta(\Omega) = \inf \{x | \exists \Lambda \subset \mathbb{R}^n : \det \Lambda = x, (\Omega \cap \Lambda) \setminus \{0\} \neq \emptyset\}$

**Утверждение 8.1.** Из теоремы минковского следует, что  $\forall \Omega$  — выпуклого и симметрично относительно  $O$

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

*Доказательство.* Предположим, что  $\frac{V(\Omega)}{\Delta(\Omega)} > 2^n$ . Тогда  $V(\Omega) > 2^n \Delta(\Omega) \Rightarrow \exists \Lambda : V(\Omega) > 2^n \det \Lambda, (\Omega \cap \Lambda) \setminus \{0\} \neq \emptyset$   $\square$

Возникает логичный вопрос:  $\frac{V(\Omega)}{\Delta(\Omega)} \geq ?$



**Теорема 8.4** (1945г. Минковского-Главка).  $\frac{V(\Omega)}{\Delta(\Omega)} \geq 1$

**Теорема 8.5** (1950е годы. Роджерс, Шмидт).  $\frac{V(\Omega)}{\Delta(\Omega)} \geq cn$

**Определение 8.4.** Октаэдр — это множество точек  $O^n = \{(x_1, x_2, \dots, x_n) \mid |x_1| + |x_2| + \dots + |x_n| \leq 1\}$ .

**Утверждение 8.2.**  $V(O^n) = \frac{2^n}{n!}$

**Теорема 8.6** (Минковский-Главка).  $\forall \varepsilon > 0 \exists n \geq N \exists \Lambda : (\Omega \cap \Lambda) \setminus \{0\} = \emptyset, \frac{V(\Omega)}{\det \Lambda} \geq 1 - \varepsilon$

*Доказательство для Октаэдра.* Помним, что у нас была теорема о том, что  $\exists f : f = O(x^{0,525\dots}) \forall x \exists p \in [x, x + f(x)]$ . Из этого следует, что  $\forall \varepsilon > 0 \exists x_0 : \forall x \geq x_0 \exists p \in [x, (1 + \varepsilon)x]$ . Зафиксируем  $\varepsilon > 0$  и выберем  $N, p > N$  (такое  $N$  существует по утверждению выше) так, что  $(1 - \varepsilon) \frac{n!}{2^n} \leq p \leq (1 - \frac{\varepsilon}{2}) \frac{n!}{2^n}$ . Рассмотрим

$$\frac{V(O^n)}{\det \Lambda_{\vec{a}}} = \frac{\frac{2^n}{n!}}{\frac{1}{p}} = \frac{2^n}{n!} p \geq (1 - \varepsilon) \frac{2^n}{n!} \frac{n!}{2^n} \geq 1 - \varepsilon$$

□

**Определение 8.5.** Положим  $\vec{a} = \left(\frac{a_1}{p}, \frac{a_2}{p} \dots \frac{a_n}{p}\right), 1 \leq a_i \leq p$ . Тогда решетка  $\langle \mathbb{Z}^n, \vec{a} \rangle_{\mathbb{Z}} = \{\vec{a}l + \vec{b} : l \in \mathbb{Z}, \vec{b} \in \mathbb{Z}^n\}$  называется рациональной центровкой.

**Замечание.** Заметим, что  $\Lambda_{\vec{a}} \subset \frac{1}{p}\mathbb{Z}^n, \det \frac{1}{p}\mathbb{Z}^n = \frac{1}{p^n}$

**Утверждение 8.3.**  $\det \Lambda_{\vec{a}} = \frac{1}{p}$

**Лемма 8.1.**

$$\left| \Lambda_{\vec{a}} \cap O^n \setminus \underbrace{\{0, \pm \vec{e}_1, \dots, \pm \vec{e}_n\}}_{\varepsilon} \right| = \sum_{l=1}^{p-1} \sum_{\vec{x} \in (\frac{1}{p}\mathbb{Z}^n \cap O^n \setminus \varepsilon)} \delta(\vec{a}l - \vec{x})$$

$$\Gamma \text{де } \delta(\vec{y}) = \begin{cases} 1, y \in \mathbb{Z}^n \\ 0, \text{ иначе} \end{cases}$$

Докажем аналогичное утверждение для Октаэдра

**Теорема 8.7.**  $\forall \varepsilon > 0 \exists N \forall n > N \exists \vec{a} (\Omega \cap \Lambda_{\vec{a}}) \setminus \{0, \pm \vec{e}_1, \pm \vec{e}_2 \dots, \pm \vec{e}_n\} = \emptyset$

*Доказательство.* Рассмотрим

$$\begin{aligned} \frac{1}{p^n} \sum_{a_1=1}^p \sum_{a_2=1}^p \dots \sum_{a_n=1}^p |\Lambda_{\vec{a}} \cap O^n \setminus \varepsilon| &= \frac{1}{p^n} \sum_{a_1=1}^p \sum_{a_2=1}^p \dots \sum_{a_n=1}^p \sum_{\vec{x}} \delta(\vec{a}l - \vec{x}) = \\ &= \frac{1}{p^n} \sum_{l=1}^{p-1} \sum_{\vec{x}} \left( \sum_{a_1=1}^p \sum_{a_2=1}^p \dots \sum_{a_n=1}^p \delta(\vec{a}l - \vec{x}) \right) = (*) \end{aligned}$$

Зафиксируем  $l \in \{1, \dots, p-1\}, \vec{x} \in \frac{1}{p}\mathbb{Z}^n \cap O^n \setminus \varepsilon, \vec{x} = \left(\frac{x_1}{p}, \dots, \frac{x_n}{p}\right) \Rightarrow \vec{a}l - \vec{x} = \left(\frac{a_1 l - x_1}{p}, \dots, \frac{a_n l - x_n}{p}\right)$ . Обозначим за  $N_p$  количество точек, попавших внутрь Октаэдра. Покроем наш октаэдр другим октаэдром побольше, так, чтобы каждый прямоугольничек, пересекающийся с

нашим октаэдром, покрылся. Тогда наш октаэдр надо растянуть в  $\leq 1 + \frac{n}{p}$  раз. Рассмотрим  $\frac{N_p}{p^n} \leq \frac{2^n}{n!} \left(1 + \frac{n}{p}\right)^n$ .

$$N_p \leq \frac{2^n}{n!} p^n \left(1 + \frac{n}{p}\right)^n$$

Заметим, что

$$(*) = \frac{1}{p^n} \sum_{l=1}^{p-1} \sum_{\vec{x}} 1 \leq \frac{1}{p^n} \sum_{l=1}^{p-1} \frac{2^n}{n!} p^n \left(1 + \frac{n}{p}\right)^n < p \frac{2^n}{n!} \left(1 + \frac{n}{p}\right)^n \leq \left(1 - \frac{\varepsilon}{2}\right) \frac{n!}{2^n} \frac{2^n}{n!} \left(1 + \frac{n}{(1-\varepsilon)\frac{n!}{2}}\right)^n$$

При некотором  $n \geq N_2$ :

$$\leq \left(1 - \frac{\varepsilon}{2}\right) \left(1 + \frac{\varepsilon}{2}\right) = 1 - \frac{\varepsilon^2}{4} \leq 1$$

□

## 9 Равномерное распределение последовательностей

В дальнейшем будем считать, что  $\{x_n\}_{n=1}^{\infty}$  — последовательность дробных долей чисел  $x_n$ .

**Определение 9.1.** Будем говорить, что последовательность  $\{x_n\}_{n=1}^{\infty}$  равномерно распределенной на  $[0, 1)$ , если

$$\forall \gamma \in (0, 1) \lim_{N \rightarrow \infty} \frac{|\{n \leq N | x_n \in [0, \gamma]\}|}{N} = \gamma$$

**Пример** (Равномерно распределенная последовательность). Рассмотрим  $\{\sqrt{n}\}_{n=1}^{\infty}$ . Заметим, что если  $\{\sqrt{n}\} \in [0, \gamma] \Rightarrow k^2 \leq n \leq (n + \gamma)^2$ . При фиксированном  $k$ , таких  $n$  не больше, чем  $2k\gamma + 2$  и не меньше, чем  $2k\gamma - 1$ . При фиксированном  $N$ ,  $k$  можно варьировать от 1 до  $[\sqrt{N}]$

$$|\{n \leq N : \sqrt{n} \in [0, \gamma]\}| = \sum_{k=1}^{[\sqrt{N}]} (2k\gamma \pm 2) = 2\gamma \frac{[\sqrt{N}]([\sqrt{N}] + 1)}{2} \pm 2[\sqrt{N}]$$

Но тогда  $\lim_{N \rightarrow \infty} \frac{|\{n \leq N : \sqrt{n} \in [0, \gamma]\}|}{N} = \gamma$ .

**Замечание.** Аналогично можно доказать, что  $\{n^\alpha\}_{n=1}^{\infty}$  равномерно распределенна.

**Пример** (Неравномерно распределенная последовательность).  $\{\alpha n\}_{n=1}^{\infty}$ ,  $\alpha \in \mathbb{Q}$  очевидно неравномерно распределена

Какие экспоненциальные последовательности равномерно распределены?

1.  $a \in (0, 1) \Rightarrow \{a^n\}_{n=1}^{\infty}$  неравномерно распределена
2.  $a > 1 \Rightarrow$  есть примеры когда нет, но кроме этого ничего не известно. Например, решения нет в следующем случае: рассмотрим  $x^2 + px + q$ , который имеет один корень на  $\lambda_1 \in (0, 1)$ , а другой на  $\lambda_2 \in (1, +\infty)$ . Тогда последовательность  $\{\lambda_1^n + \lambda_2^n\}$

**Теорема 9.1.** Последовательность  $\{x_n\}_{n=1}^{\infty}$  равномерно распределена  $\Leftrightarrow \forall$  непрерывной функции  $f : [0, 1] \rightarrow [0, 1]$  верно:

$$\frac{1}{N} \sum_{n=1}^N f(x_n) \rightarrow \int_0^1 f(x) dx$$

*Доказательство.*

$\Rightarrow$  От противного. Пусть существует функция  $f$ , которая не удовлетворяет условию выше. Мы знаем, что если взять функцию  $g(x) = I_{x \in [a, b]}$  ( $0 < a, b < 1$ ), то  $\frac{1}{N} \sum_{n=1}^N g(x_n) \rightarrow \int_0^1 g(x) dx$ . Зафиксируем  $\varepsilon > 0$ . Подберем 2 комбинации индикаторов  $g_1(x), g_2(x)$  так, что  $g_1(x) \leq f(x) \leq g_2(x), \int_0^1 (g_2(x) - g_1(x)) dx < \varepsilon$ . По критерию интегрируемости Римана,  $\frac{1}{N} \sum_{n=1}^N f(x_n) \rightarrow \int_0^1 f(x) dx$

□

**Теорема 9.2** (О приближении непрерывной функции тригонометрическими многочленами). Пусть  $f : \mathbb{C} \rightarrow \mathbb{C}$  непрерывна и периодична. Тогда  $\forall \varepsilon > 0 \exists$  тригонометрический многочлен  $\psi$ , такой, что  $\sup_{x \in [0, 1]} |f(x) - \psi(x)| < \varepsilon$ .

**Теорема 9.3** (Критерий Вейля). Последовательность  $\{x_n\}_{n=1}^{\infty}$  равномерно распределена  $\Leftrightarrow \forall m \neq 0 \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N e^{2\pi i m x_n} = 0$

*Доказательство.*  $\Rightarrow \int_0^1 e^{2\pi i m x} dx = 0 /$

$\Leftarrow$  Возьмем произвольную  $f : \mathbb{C} \rightarrow \mathbb{C}$  — непрерывную и периодичную. Зафиксируем  $\varepsilon > 0$  и подберем  $\psi : \sup_{x \in [0, 1]} |f(x) - \psi(x)| \leq \frac{\varepsilon}{3}$

$$\begin{aligned} & \left| \frac{1}{N} \sum_{n=1}^N f(x_n) - \int_0^1 f(x) dx \right| = \\ & = \left| \frac{1}{N} \sum_{n=1}^N f(x_n) - \frac{1}{N} \sum_{n=1}^N \psi(x_n) + \frac{1}{N} \sum_{n=1}^N \psi(x_n) - \int_0^1 \psi(x) dx + \int_0^1 \psi(x) dx - \int_0^1 f(x) dx \right| = \\ & = \left| \left( \frac{1}{N} \sum_{n=1}^N (f(x_n) - \psi(x_n)) \right) + \left( \frac{1}{N} \sum_{n=1}^N \psi(x_n) - \int_0^1 \psi(x) dx \right) + \left( \int_0^1 (\psi(x) - f(x)) dx \right) \right| \leq \\ & \leq \underbrace{\left| \frac{1}{N} \sum_{n=1}^N (f(x_n) - \psi(x_n)) \right|}_{\leq \frac{\varepsilon}{3}} + \underbrace{\left| \frac{1}{N} \sum_{n=1}^N \psi(x_n) - \int_0^1 \psi(x) dx \right|}_{\leq \frac{\varepsilon}{3}} + \underbrace{\left| \int_0^1 (\psi(x) - f(x)) dx \right|}_{\leq \frac{\varepsilon}{3}} \leq \varepsilon \end{aligned}$$

Это верно для достаточно больших  $N$

□

**Утверждение 9.1.**  $\{\alpha n\}_{n=1}^{\infty}, \alpha \notin \mathbb{Q}$  — равномерно распределена

*Доказательство.*

$$\forall m \neq 0 \frac{1}{N} \sum_{n=1}^N e^{2\pi i m \alpha n} = \frac{1}{N} \sum_{n=1}^N (e^{2\pi i \alpha m})^n = \frac{e^{2\pi i \alpha m N} - 1}{N(e^{2\pi i \alpha m} - 1)} e^{2\pi i \alpha m}$$

При этом

$$\left| \frac{1}{N} \sum_{n=1}^N e^{2\pi i \alpha n} \right| \leq \left| \frac{e^{2\pi i \alpha m N} - 1}{N(e^{2\pi i \alpha m} - 1)} e^{2\pi i \alpha m} \right| \leq \frac{2e^{2\pi i \alpha m}}{N|e^{2\pi i \alpha m} - 1|} \rightarrow 0$$

$\alpha \notin \mathbb{Q} \Rightarrow e^{2\pi i \alpha m} \neq 1.$  □

**Теорема 9.4.** Последовательность  $\{x_n\}_{n=1}^\infty$  равномерно распределена  $\Leftrightarrow \forall f : \mathbb{C} \rightarrow \mathbb{C}$ , таких, что  $f$  периодична с периодом 1,

$$\int_0^1$$

*Доказательство.* Доказательство предоставляется читателю в качестве нетрудного упражнения □

## 10 Вероятностное детерминирования

С прошлой лекции мы знаем про тесты Ферма и Соловея - Штрассена, сейчас рассмотрим что-то новое

### 10.1 Тест Миллера-Рабина

$$m - 1 = 2^s \cdot l$$

Пусть  $B_{MR} = \{a \in \mathbb{Z}_m^*\}$ , если для  $a$  выполнено одно из следующих условий:

1.  $a^l \equiv_m \pm 1$
2.  $a^{2^l} \equiv_m -1$
3.  $a^{4^l} \equiv_m -1$
4.  $a^{\frac{m-1}{2}} = a^{2^{s-1}l} \equiv_m -1 \pmod m$

*Доказательство.* Пусть  $m$  - простое. Несложно заметить факт, что для простых чисел существует некоторое дерево ветвлений:  $a^{p-1} = 1$ , для половины простых  $a^{\frac{p-1}{2}} = 1$ , для другой половины  $a^{\frac{p-1}{2}} = -1$ . Первая половина делится на еще 2 группы простых (для которых  $a^{\frac{p-1}{4}} = 1$  и  $a^{\frac{p-1}{4}} = -1$ ).

В обратную сторону воспользуемся утверждением ниже (б/д). □

**Утверждение 10.1.**  $(b/d) B_{MR}(m) \subset B_S S(m)$

**Утверждение 10.2.**  $|B_{MR}(m)| \leq |\mathbb{Z}_m^*(m)|$

*Доказательство.* 1.  $m: p, q, r$  - различные простые.

2.  $m = p^\alpha q^\beta \Rightarrow m -$  не число Кармайкла  $\Rightarrow |B_F(m)| \leq \frac{1}{2} |\mathbb{Z}_m^*|$

3.  $m = p^\alpha$

**Первый случай:**

Пусть  $M_i$  - множество остатков  $a$  из первого доказательства, то есть  $M'_0 = \{a \in \mathbb{Z}_m^* | a^l \equiv_m 1\}$ ,  $M_j = \{a \in \mathbb{Z}_m^* | a^{2^{j \cdot l}} \equiv_m -1\}$ . Выбирая минимальные  $j$ , добьемся того, что  $B_{MR}(m) = M'_0 \sqcup M_0 \sqcup M_1 \sqcup \dots \sqcup M_{s-1}$ .

**Утверждение 10.3.**  $d \in \mathbb{Z}, d > 1$ , если  $|\{a \in \mathbb{Z}_d^* | a^k = -1\}| \neq 0 \implies |\{a \in \mathbb{Z}_d^* | a^k = 1\}|$

*Доказательство простое, достаточно просто взять  $a^2$*

Определим  $M_j = \left| \{a \in \mathbb{Z}_m^* | a^{2^{j \cdot l}} \equiv_m -1\} \right|$ , что по КТО равносильно системе:

$$1. a^{2^{j \cdot l}} \equiv_{p^\alpha} -1$$

$$2. a^{2^{j \cdot l}} \equiv_{p^\beta} -1$$

$$3. a^{2^{j \cdot l}} \equiv_{p^\gamma} -1$$

**Утверждение 10.4.**  $|N_j| = 6|M_j|$

**Утверждение 10.5.**  $N_j \cup M_{j+k} = \emptyset \implies N_j \cup N_{j+k} = \emptyset$

*Доказательство.*  $a \in N_j \implies a^{2^{j \cdot l}} \equiv_m 1$  □

Из описанного следует, что  $|M'_0| \sqcup M_0 \sqcup M_1 \sqcup \dots \sqcup M_{s-1}| \leq \frac{1}{3}|N_0 \sqcup N_1 \sqcup \dots \sqcup N_{s-1}|$  □

## 10.2 Числа Мерсенна

**Определение 10.1.** Простые числа  $2^p - 1$  называются числами Мерсенна

**Определение 10.2.** Простые числа  $2^{2^n} - 1$  называются числами Ферма

**Замечание.**  $\forall n > 5$  числа Ферма составные

**Замечание.**  $2^n - 1$  — простое число  $\Rightarrow n$  — простое

*Доказательство.* Пусть нет, тогда  $n = mk \Rightarrow 2^{mk} - 1 = (2^m)^k - 1 \equiv_{2^m} 0$  □

**Определение 10.3.**  $s_0 = 4, s_{k+1} = s_k^2 - 2$ .

**Лемма 10.1.**  $s_k = (2 + \sqrt{3})^{2^k} + (2 - \sqrt{3})^{2^k}$

*Доказательство.* По индукции □

**Определение 10.4.**  $\mathbb{Z}_m[\sqrt{k}] = \mathbb{Z}_m[x]/(x^2 - k)$ , т.е. это все остатки при делении на многочлен  $x^2 - k$

**Теорема 10.1** (Люка-Лемера). Тогда  $M_p$  — простое  $\Leftrightarrow M_p | s_{p-2}$

*Доказательство.*

$\Leftarrow$  Пусть  $q$  — наименьший делитель  $M_p$

$$(2 + \sqrt{3})^{2^{p-2}} + (2 - \sqrt{3})^{2^{p-2}} \equiv_q 0$$

$$(2 + \sqrt{3})^{2^{p-2}} \equiv_q -(2 - \sqrt{3})^{2^{p-2}}$$

$$(2 + \sqrt{3})^{2^{p-1}} \equiv_q -1$$

$$(2 + \sqrt{3})^{2^p} \equiv_q 1$$

$$\text{ord}(2 + \sqrt{3}) | 2^p \Rightarrow \text{ord}(2 + \sqrt{3}) = 2^k, k > p - 1 \Rightarrow \text{ord}(2 + \sqrt{3}) = 2^p$$

$$M_p = 2^p - 1 < \text{ord}(2 + \sqrt{3}) = 2^p < || = q^2 \leq M_p$$

КОРОЧЕ СОРЯН Я НЕ УСПЕЛ

[ВОТ ВАМ ВИКИПЕДИЯ](#)

□