Основы комбинаторики и теории чисел

Григорян Сергей

13 марта 2025 г.

Содержание

1 Лекция 1

1.1 Квадратичные вычеты и невычеты

1.1.1 Определение

Пусть $m \in \mathbb{N}$ — наш модуль. Пусть $a \in \mathbb{N}$: $(a, m) = 1$. Рассмотрим сравнение:

$$x^2 \equiv a \pmod m \tag{1}$$

Мы говорим, что a является **квадратичным вычетом по модулю** m, если у сравнения (1) **есть решение**.

Пусть a — квадратичный вычет. Будем всюду далее считать, что $m = p$ — нечётное простое число. Тогда сравнение (1) **имеет 2 решения по теореме Лагранжа**.

Теорема 1.1 (Лагранжа)**.** *Пусть:*

$$f(x) = a_n x^n + \ldots + a_1 x + a_0, a_i \in \mathbb{Z}_p$$

Тогда сравнение:

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

Имеет $\leq n$ *корней.*

Доказательство. От противного, пусть есть решения $x_1, \ldots, x_{n+1}$. Представим $f(x)$ в виде:

$$\begin{gathered} f(x) = b_n(x - x_1)(x - x_2)\ldots(x - x_n) + \\ + b_{n-1}(x - x_1)\ldots(x - x_{n-1}) + \\ \vdots \\ + b_1(x - x_1) + \\ + b_0 \end{gathered}$$

Рассм. $f(x_1) \equiv 0 \pmod p \Rightarrow f(x_1) \equiv b_0 \equiv 0 \pmod p$

$$f(x_2) \equiv 0 \equiv b_1(x_2 - x_1) \Rightarrow b_1 \equiv 0 \pmod p$$

Аналогичным образом, получаем, что $\forall i, b_i = 0$ $\square$

Таким образом, в нашем случае сравнение (1) имеет ровно 2 корня:

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

$$(-x_1)^2 \equiv a \pmod p$$

Выпишем все квадратичные вычеты по модулю p:

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

Покажем, что это действительно все корни:

$$1^2 \equiv (\pm 1)^2$$

$$2^2 \equiv (\pm 2)^2$$

$$\vdots$$

$$a^2 \equiv (\pm a)^2$$

Таким образом, все эти корни заполняют всю приведённую систему вычетов по модулю p. Поэтому мы имеем $\frac{p-1}{2}$ **квадратичных вычетов** и $\frac{p-1}{2}$ **квадратичных невычетов**.

Определение 1.1. Символом Лежандра числа a по модулю p (читается "a по p"), называется число:

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

1.1.2 Способы вычисления

Утверждение 1.1.

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

Доказательство. Рассм. МТФ:

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

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

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

Если a квадратичный вычет, то:

$$a \equiv x^2 \pmod p \Rightarrow a^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod p$$

У уравнения, $a^{\frac{p-1}{2}} - 1 \equiv 0 \pmod p$ — $\frac{p-1}{2}$ корней, т. е. это все наши квадратичные вычеты. Таким образом:

$$a^{\frac{p-1}{2}} \equiv 1 \iff a \text{ — квадратичный вычет}$$

$$a^{\frac{p-1}{2}} \equiv -1 \iff a \text{ — квадратичный невычет}$$

Таким образом:

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

□

Следствие.

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

Следствие.

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

Следствие.

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, p = 4k+1, k \in \mathbb{Z} \\ -1, p = 4k+3, k \in \mathbb{Z} \end{cases}$$

Следствие.

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

Утверждение 1.2.

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

Доказательство. Рассм. $x = 1, 2, 3, \ldots, \frac{p-1}{2}, p_1 := \frac{p-1}{2}$

$$ax = \varepsilon_x r_x \pmod p, \varepsilon_x \in \{+1, -1\}, r_x \in \{1, \ldots, p_1\}$$

Перемножим все ax и $\varepsilon_x r_x$, тогда т. к. x и r_x пробегают одни и те же числа, то:

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

Утверждение 1.3.

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

Доказательство. Рассм. случаи принадлежности ax к:

1. $\{1, \ldots, p_1\}$
2. $\{p_1 + 1, p - 1\}$

□

Тогда:

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

□

Утверждение 1.4. *Если a — **нечётное**, то:*

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

Доказательство. Рассм. a — нечёт. Рассм.

$$\left(\frac{2a}{p}\right) = \left(\frac{4\left((a+2)/2\right)}{p}\right) =$$

$$= \left(\frac{4}{p}\right)\left(\frac{\frac{1}{2}(a+p)}{p}\right) = (-1)^{\sum_{x=1}^{p_1} \left\lfloor \frac{(a+p)x}{p} \right\rfloor} = (-1)^{\sum_{x=1}^{p_1} \left\lfloor \frac{ax}{p} \right\rfloor + \sum_{x=1}^{p_1} x} =$$

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

Подставим $a = 1$:

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

При этом в общем виде:

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

Что равно тому, что получено выше. Сокращая одинаковые члены, получаем:

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

$\square$

<u>**Следствие.**</u>

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

1.1.3 Квадратичный закон взаимности

Пусть p и q — разные нечётные простые числа. Тогда:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p_1\cdot q_1} \tag{2}$$

Доказательство.

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

Положим:

$$S = \{\,(x,y)\colon x = 1,\dots q_1; y = 1,\dots,p_1\,\}\,, |S| = p_1\cdot q_1$$

$$S_1 = \{\,(x,y)\in S\colon qy < px\,\}$$

$$S_2 = \{\,(x,y)\in S\colon qy > px\,\}$$

Тогда:

$$|S| = |S_1| + |S_2|$$

$$qy < px \iff y < \frac{px}{q} \Rightarrow |S_1| = \sum_{x=1}^{q_1}\left\lfloor \frac{px}{q}\right\rfloor$$

$$qy > px \iff x < \frac{qy}{p} \Rightarrow |S_2| = \sum_{y=1}^{p_1}\left\lfloor \frac{qy}{p}\right\rfloor$$

$$\Rightarrow p_1 q_1 = |S| = |S_1| + |S_2| = \sum_{x=1}^{q_1} \left\lfloor \frac{px}{q} \right\rfloor + \sum_{y=1}^{p_1} \left\lfloor \frac{qy}{p} \right\rfloor$$

$\square$

2 Лекция 2

2.1 Матрица Адамара

2.1.1 Определение

Определение 2.1. Матрица Адамара — это квадратная матрица:

$$A_{n\times n} = \left(a_{ij}\right), a_{ij} \in \{\,+1, -1\,\}$$

Такая, что любые две строки ортогональны (скалярное произведение в ОНБ $= 0$).

Рассмотрим несколько случаев:

$n = 1:$

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

$n = 2:$

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

$n = 3:$ Невозможно

Замечание. *Матриц Адамара нечётного размера не существует (кроме $n = 1$)*

$$\Rightarrow n \geq 2 \Rightarrow n = 2k$$

2.1.2 Необходимое условие существования

Теорема 2.1. $n \geq 2 \Rightarrow n = 4k, k \in \mathbb{N}$

Доказательство.

Задача 2.1. Если у матрицы из ± 1 попарно ортогональны строки, то у неё также попарно ортогональны и столбцы.

Б. О. О.:

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

Т. к. каждая строка ортогональна 1-ой, то в каждой строке, кроме первой, поровну 1 и -1

Б. О. О.:

Вторая строка: $1, 1, 1, \dots, 1, 1, 1, -1, -1, -1, \dots, -1, -1, -1$

Третья строка: $1, \dots, 1, -1, \dots, -1, 1, \dots, 1, -1, \dots, -1$

Получаем 4 блока с одним скал. произведением: $x, \frac{n}{2} - x, \frac{n}{2} - x, x$:

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

$$\Rightarrow 4x - n = 0$$

$$\Rightarrow n = 4x$$

□

Гипотеза Адамара: $n = 4k$ — достаточное условие, для существования матрицы Адамара.

2.1.3 Конструирование матриц Адамара

Алгоритм построения H_{2^n} из $H_{2^{n-1}}$:

$$H_{2^n} = \begin{pmatrix} H_{2^{n-1}} & H_{2^{n-1}} \\ H_{2^{n-1}} & (-1) \cdot H_{2^{n-1}} \end{pmatrix}$$

Определение 2.2. $A_n * B_m$ — **кронекеровское умножение** квадратных матриц A_n и B_m, задаваемое следующим образом:

$$A_n * B_m = \begin{pmatrix} a_{11} \cdot B & \dots & a_{1n} \cdot B \\ \vdots & \vdots & \vdots \\ a_{n1} B & \dots & a_{nn} \cdot B \end{pmatrix} = C_{mn}$$

Теорема 2.2. *Если A, B — матрицы Адамара, то $A * B$ — тоже матрица Адамара.*

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

Доказательство. Рассмотрим матрицу $Q = \big(q_{ij}\big)$:

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

Покажем, что скалярное произведение $\forall$ двух строк равно -1:

$$\sum_{b=1}^{p}\left(\frac{a-b}{p}\right)\left(\frac{a'-b}{p}\right) = \left[\begin{matrix} c = a-b \\ a'-b = a'+a-b-a = c+a'-a \end{matrix}\right] =$$

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

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

Тогда искомая матрица:

$$H_{p+1} = \begin{pmatrix} 1 & \dots & 1 \\ \vdots & Q' & \\ 1 & & \end{pmatrix}$$

где Q' матрица Q, где вместо 0 стоят -1. Покажем, что это действительно матрица Адамара. Для двух строк a и a' скалярное произведение равно:

$$-1 + 1 - \left(\frac{a-a'}{p}\right) - \left(\frac{a'-a}{p}\right) =$$

$$= -\left(\underbrace{\left(\frac{-1}{p}\right)}_{-1} + 1\right)\left(\frac{a'-a}{p}\right) = 0$$

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

$\square$

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

Замечание. *В книжке Н. Холла "Комбинаторика"есть отдельная глава про матрицы Адамара (стоит прочитать).*

2.1.4 Плотность порядков матриц Адамара

Теорема 2.5 (б/д)**.**

$$\forall \varepsilon > 0, \exists n_0, \forall n \geq n_0$$

на отрезке $[n, (1+\varepsilon)n]$ есть порядок матрицы Адамара.

Переформулировка:

$$\exists f\colon f(n) = o(n)$$

на отрезке $[n, n + f(n)]$ есть порядок матрицы Адамара.

2.1.5 Коды, исправляющие ошибки

Есть передатчик, приёмник и канал связи. По этому каналу связи передаются бинарные строки длины n. На канале есть помехи, т. е. произвольный бит может поменять значение. Пусть мы знаем, что кол-во ошибок $\leq k$.

Вопрос: как организовать словарь кодовых слов (строк, которых мы передаём), что, несмотря на ошибки, приёмник сможет однозначно понять исходное слово по искажённому?

Например, пусть наш словарь состоит из двух строк и $k = 1$:

$$1110\ldots0$$

$$0111\ldots0$$

Эти два слова могут исказиться до $1111\ldots0$, т. е. мы их не сможем различить. С другой стороны:

$$1110\ldots0$$

$$0011\ldots0$$

Всегда можно различить, т. к. они не могут исказиться до одного и того же.

Определение 2.3. **Расстояние Хэмминга** между двумя векторами — это кол-во несовпадающих координат.

Основная задача кодирования: выбрать максимальное кол-во слов так (при заданных n и k), чтобы **расстояние Хэминга между любыми двумя словами было** $> 2k$.

2.1.6 (n, M, d)-код

Определение 2.4. (n, M, d)-код — тройка объектов, в которой:

- n – длина кодового слова;
- M — кол-во кодовых слов;
- d — минимальное Хэммингово расстояние.

Теорема 2.6 (Граница Плоткина)**.** *Пусть дан* (n, M, d)*-код, причём* $2d > n$*. Тогда* $M \leq \frac{2d}{2d-n}$

Доказательство. Будет доказана в следующий раз □

Замечание. *Матрицы Адамар дают неулучшаемую границу размера словаря.*

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

$$\Rightarrow \left(n-1, n, \frac{n}{2}\right) \text{-код}$$

Рассмотрим код из строк матрицы Адамара, заметим, что он достигает границы Плоткина.

3 Основная теорема арифметики

Теорема 3.1 (ОТА). *1)*

$$\forall n > 1, \exists! p_1, \dots, p_s \colon n = p_1 p_2 \dots p_s$$

где $p_1, \dots, p_s$ *— простые (не обязательно различные) числа (единственность с точностью до порядка)*

2) Пусть p_i — i-ое простое число, тогда:

$$\forall n, \exists!(\alpha_1, \ldots, \alpha_n, \ldots), \alpha_i \in \mathbb{Z}_+, n = \prod_{i=1}^{\infty} p_i^{\alpha_i}$$

<u>Определение</u> 3.1. $\nu_p(n)$ — максимальная степень p, т. ч. $n \vdots p^{\nu_p(n)}$, но $n \not\vdots p^{\nu_p(n)+1}$

<u>Замечание</u>.

$$n \vdots m \iff \forall p, \nu_p(n) \geq \nu_p(m)$$
$$n = m \iff \forall p, \nu_p(n) = \nu_p(m)$$

Использование:

1) Оценка $\pi(x)$ — кол-во простых $\leq x$

2) Криптография: $q \cdot p \longleftrightarrow n$

Доказательство. 1) Существование (ММИ по n):

- База, n — простое $\Rightarrow n = n$
- Переход: $n = mk = (p_1 \ldots p_s) \cdot (q_1 \ldots q_l)$

2) I) Напрямую. От противного, возьмём наименьшее n, для которого есть > 1 разложение:

$$n = p_1 \ldots p_s = q_1 \ldots q_k$$

$$p_1 \leq p_2 \leq \ldots \leq p_s$$
$$q_1 \leq q_2 \leq \ldots \leq q_k$$

Если $p_1 = q_1$, тогда $\frac{n}{p_1} = p_2 \ldots p_s = q_2 \ldots q_k$, т. е. у нас есть меньшее число, у которого > 1 разложения $\Rightarrow\perp$. Тогда $p_1 \neq q_1$. Следовательно:

$$n \geq p_1 p_2 \geq p_1^2$$
$$n \geq q_1^2$$
$$n \geq \max(p_1^2, q_1^2) \geq q_1(p_1 + 2) > q_1 p_1 + 1$$

Пусть $q_1 > p_1 \Rightarrow q_1 \geq p_1 + 2$. Тогда у числа $n - p_1q_1$, по предположению индукции, существует единственное разложение.

$$1 < n - p_1q_1 = \tau_1 \dots \tau_m = p_1(p_2 \dots p_s - q_1) = q_1(q_2 \dots q_k - p_1)$$

$$\Rightarrow (n - p_1q_1) \vdots p_1 \Rightarrow q_2 \dots q_k \vdots p_1 \Rightarrow \perp$$

– Через лемму Евклида:

Лемма 3.2 (Евклид)**.**

$$mn \vdots p \Rightarrow \left[\begin{array}{l} m \vdots p \\ n \vdots p \end{array}\right.$$

Лемма 3.3 (Переформулировка)**.**

$$\begin{cases} (m,k) = 1 \\ mn \vdots k \end{cases} \Rightarrow n \vdots k$$

Покажем, что из леммы Евклида следует ОТА:

$$n = p_1 \dots p_s = q_1 \dots q_k$$

$$n = q_1 Q \vdots p_1 \Rightarrow \left[\begin{array}{l} q_1 \vdots p_1 \Rightarrow q_1 = p_1 \\ Q \vdots p_1 \end{array}\right.$$

Получаем противоречие с min выбором n:

Доказательство переформулировки:

$$mx + ky = 1, nm \vdots k$$

$$mnx + kny = n \Rightarrow n \vdots k$$

□

Определение 3.2. $I \subset \mathbb{Z}$ — идеал в $\mathbb{Z}$, если:

1) $\forall a, b \in I, a + b \subset I$
2) $\forall a \in I, \forall b \in \mathbb{Z}, ab \in I$

Доказательство леммы Евклида через Идеалы:

Заф. $m; I = \{ a \mid ma \vdots p \}$. Легко понять, что это идеал, причём $0, n, p \in I$. Пусть $d = \min I$, покажем, что $I = \{ cd \mid c \in \mathbb{Z} \}$:

Доказательство. $a \in I, a = qd + r, 0 < r < d \Rightarrow r \in I$ — противоречие с выбором d $\square$

Т. к. $p \in I$, то:

1) $d = 1$, то тогда $m \vdots p$

2) $d = p, n \in I$, то тогда $n \vdots p$

$\square$

$\square$

4 Лекция 3

4.1 Доказательство границы Плоткина

(n, M, d) — код

- n — размерность
- M — кол-во слов
- d — минимальное хэммингово расстояние

Теорема 4.1 (Плоткина)**.** *Если* $2d > n$*, то:*

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

Доказательство. Рассмотрим (n, M, d)-код, и запишем его слова как строки в матрице $M \times n$:

$$\begin{pmatrix} a_{11} & a_{12} & a_{13} & \dots & a_{1n} \\ a_{21} & a_{22} & a_{23} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_{M1} & a_{M2} & a_{M3} & \dots & a_{Mn} \end{pmatrix}$$

$$a_{ij} \in \{0, 1\}$$

$$\sum_{k=1}^{n} \sum_{i<j} |a_{ik} - a_{jk}| = \sum_{i<j} \underbrace{\sum_{k=1}^{n} |a_{ik} - a_{jk}|}_{\text{Хэммингово расстояние между } i\text{-ым и } j\text{-ым словами}} \geq \sum_{i<j} d =$$

$$= \frac{M(M-1)}{2} d$$

Обозначим для данного k буквой x число единиц в k-ом столбце. Тогда:

$$\sum_{k=1}^{n} \underbrace{\sum_{i<j} |a_{ik} - ajk|}_{=x(M-x) \leq \frac{M^2}{4}} \leq \frac{nM^2}{4}$$

Получаем:

$$M \frac{M-1}{2} d \leq \frac{nM^2}{4}$$

$$2(M-1)d \leq nM$$

$$2Md - 2d \leq nM$$

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

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

□

4.2

Вспомним задачу прошлого семестра:

Задача 4.1. 30 чисел. Выбраны $M_1, \dots, M_{15}$ — их 5-сочетания. Можно ли покрасить эти 30 чисел в красные и синие цвета, чтобы для $\forall i$ в M_i были и красные, и синие числа.

Зачем-то, давайте ответим, возможно ли раскрасить так, чтобы в каждом M_i разность кол-ва красных и синих шаров была по модулю ≤ 1? Пока что, сформулируем теорему:

Теорема 4.2. *Пусть* $R_n = \{1, 2, \dots, n\}$. *Пусть:*

$$M_1, \dots, M_n \subseteq R_n, \text{(какие-то подмножества)}$$

Тогда $\exists$ *раскраска* R_n *в красные и синие пвета, при которой, для* $\forall i$ *в* M_i *разность между количеством красных и синих чисел по модулю* $\le 6\sqrt{n}$

Теорема доказывается в 4-ом семестре через матрицы Адамара. Пока что, покажем, что эта границы неулучшаема.

Обозначение. χ — *раскраска* R_n *в два цвета:*

$$\chi\colon R_n \to \{-1, +1\}$$

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

Тогда утв-е теоремы звучит как:

$$\forall M_1, \dots, M_n \exists \chi\colon \forall i\, |\chi(M_i)| \le 6\sqrt{n}$$

Теорема 4.3. *Коль скоро существует матрица Адамара порядка n существует, то:*

$$\exists M_1, \dots, M_n \forall \chi\colon \exists i\, |\chi(M_i)| \ge \frac{\sqrt{n}}{2}$$

Доказательство. Рассмотрим H, построим по ней совокупность $M_1, \dots, M_n$. Возьмём каждую строки матрицы H, построим соответствие:

$$M_i = \{ j \mid 1 \le j \le j \wedge H_{ij} = 1 \}$$

Покажем выполнение теоремы для этого набора. Наше утв-е эквивалентно следующему:

$$\forall \overline{v} \in \{+1, -1\}^n \,\exists \text{ координата вектора } \left(\frac{H+J}{2}\right)\overline{v}\colon\ |\overline{v}| \ge \frac{\sqrt{n}}{2}$$

$$J \text{ — матрица из единиц}$$

Покажем выполнимость утв-я сначала для $H\overline{v}$ вместо $\left(\frac{H+J}{2}\right)\overline{v}$

$$H = \begin{pmatrix} \overline{h_1} & \overline{h_2} & \dots & \overline{h_n} \end{pmatrix} \text{ — векторы-столбцы}$$

$$(H\overline{v}, H\overline{v}) = (v_1\overline{h_1} + v_2\overline{h_2} + \ldots v_n\overline{h_n}, v_1\overline{h_1} + v_2\overline{h_2} + \ldots + v_n\overline{h_n}) =$$

Выбирая ортонормированный базис, получаем:

$$= v_1^2(\overline{h_1}, \overline{h_1}) + \ldots + v_n^2(\overline{h_n}, \overline{h_n}) = (\overline{h_1}, \overline{h_1}) + \ldots + (\overline{h_n}, \overline{h_n}) = n^2$$

$$H\overline{v} = (L_1, \ldots, L_n)$$

$$(H\overline{v}, H\overline{v}) = L_1^2 + \ldots + L_n^2 = n^2 \Rightarrow \exists i\colon\ |L_i| \geq \sqrt{n}$$

Соответственно, для $\frac{1}{2}H\overline{v}$ получаем оценку $\geq \frac{\sqrt{n}}{2}$. Теперь докажем для $\left(\frac{H+J}{2}\right)\overline{v}$. Рассмотрим $(H+J)\overline{v}$:

$$\lambda = \sum_{i=1}^{n} v_i$$

$$(H+J)\overline{v} = \begin{pmatrix} L_1 + \lambda \\ \ldots \\ L_n + \lambda \end{pmatrix}$$

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

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

$$= n^2 \pm 2\lambda n + \lambda^2 n \Rightarrow$$

Максимум при $\lambda = \mp 1$, но т. к. размер матрица Адамара чётный, то реальный минимум в $\underbrace{\lambda = -2, 0}_{n^2+2\lambda n+\lambda^2 n}$ или $\underbrace{\lambda = 0, 2}_{n^2-2\lambda n+\lambda^2 n}$. В любом случае получаем, что:

$$((H+J)\overline{v}, (H+J)\overline{v}) \geq n^2$$

Следовательно хотя бы одна координата $\geq \sqrt{n}$. Оценка доказана. □

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

5 Лекция 4

5.1 Распределение простых

$$\pi(x) = |\{\, p \leq x \colon p \text{ — простое} \,\}| = \sum_{p \leq x} 1$$

Теорема 5.1 (Асимптотический закон распределения простых чисел (б/д))**.**

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

Доказана Адамаром и Валле-Пуссеном.

Теорема 5.2 (Чебышёв)**.**

$$\forall \varepsilon > 0, \exists x_0, \forall x \geq x_0$$

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

Доказательство. Введём вспомогательные функции:

$$\theta(x) = \sum_{p \leq x} \ln p$$

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

Заметим:

$$\psi(x) \leq \sum_{p \leq x} \ln x$$

Положим:

$$\lambda_1 = \overline{\lim_{x \to +\infty}} \frac{\theta(x)}{x}, \lambda_2 = \overline{\lim_{x \to +\infty}} \frac{\psi(x)}{x}, \lambda_3 = \overline{\lim_{x \to +\infty}} \frac{\pi(x)}{x/\ln x}$$

$$\mu_1, \mu_2, \mu_3 \text{ — то же, что и } \lambda_1, \lambda_2, \lambda_3 \text{, но предел нижний}$$

Лемма 5.3.

$$\lambda_1 = \lambda_2 = \lambda_3, \mu_1 = \mu_2 = \mu_3$$

Доказательство.

$$\theta(x) = \sum_{p \le x} \ln p \le \psi(x) \le \sum_{p \le x} \ln x = (\ln x)\pi(x)$$

$$\Rightarrow \frac{\theta(x)}{x} \le \frac{\psi(x)}{x} \le \frac{\pi(x)}{x/\ln x} \Rightarrow \lambda_1 \le \lambda_2 \le \lambda_3$$

Зафикс. $\beta \in [0, 1)$:

$$\theta(x) = \sum_{p \le x} \ln p \ge \sum_{x^\beta < p \le x} \ln p > \sum_{x^\beta < p \le x} \ln(x^\beta) = \beta \ln x(\pi(x) - \pi(x^\beta)) \ge$$

Т. к. $\pi(x) \le x$:

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

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

Переходя к верхнему пределу по x:

$$\Rightarrow \lambda_1 \ge \beta\lambda_3$$

Затем переходим к sup по β:

$$\lambda_1 \ge \lambda_3 \Rightarrow \lambda_1 = \lambda_2 = \lambda_3$$

Лемма доказана ($\mu_1 = \mu_2 = \mu_3$ — аналогично) □

Рассмотрим C_{2n}^n. Заметим, что $C_{2n}^n < 2^{2n}$:

$$\ln C_{2n}^n \le 2n \ln 2$$

$$C_{2n}^n = \frac{(2n)!}{(n!)^2} \ge \prod_{n < p \le 2n} p$$

$$\Rightarrow \ln C_{2n}^n \ge \sum_{n < p \le 2n} \ln p = \theta(2n) - \mathrm{th}(n)$$

Рассм. $n = 1, 2, 4, 8, \ldots, 2^k$:

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

Сложим нер-ва:

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

Получаем:

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

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

$$2^k < x \leq 2^{k+1}$$

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

$$\Rightarrow \frac{\theta(x)}{x} \leq 4 \ln 2 \Rightarrow \lambda_1 \leq 4 \ln 2 \Rightarrow \lambda_3 \leq 4 \ln 2$$

Заметим:

$$C_{2n}^n > \frac{2^{2n}}{2n+1} \text{ — среднее арифм. С-шек}$$

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

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

$$= \prod_{p \leq 2n} p^{\underbrace{\left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right)}_{\leq 1} + \underbrace{\left(\left\lfloor \frac{2n}{p^2} \right\rfloor - 2 \left\lfloor \frac{n}{p^2} \right\rfloor \right)}_{\leq 1} + \ldots} \leq \prod_{p \leq 2n} p^{\left\lfloor \log_p 2n \right\rfloor} =$$

$$= e^{\psi(2n)}$$

Получили:

$$\ln C_{2n}^n \leq \psi(2n)$$

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

Зафикс. $x \in [2n, 2n+2)$:

$$x \in [2n, 2n+2) \Rightarrow \psi(x) > \psi(2n) \geq 2n \ln 2 - \ln(2n+1) >$$

$$> (x-2) \ln 2 - \ln(x+1)$$

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

$$\mu_2 \geq \ln 2 \Rightarrow \mu_3 \geq \ln 2$$

Ч. Т. Д. □

Теорема 5.4 (Постулат Бертрана)**.**

$$\forall x \geq 2, \exists p \in [x, 2x] = [x, x + x]$$

Давайте вместо правой границы $[x, 2x]$ рассмотрим $[x, x + f(x)]$. Вопрос: при каких $f(x)$ можно расчитывать на $\exists p \in [x, x + f(x)]$ хотя бы при $x \geq x_0$.

Замечание. *АЗРП* $\Rightarrow f(x) = o(x)$. *На сегодняшний день известна оценка* $f(x) = O(x^{0.525})$

Утверждение 5.1 (Гипотеза)**.** $f(x) = O(\ln^2 x)$

6 Лекция 5

6.1 Первообразные корни

$$m \in \mathbb{N}, a \in \mathbb{N}, (a, m) = 1$$

Теорема 6.1 (Эйлера)**.**

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

Определение 6.1. Показатель числа $a \pmod m$ $(\delta(a))$ — это

$$\min k > 0 \colon a^k \equiv 1 \pmod m$$

Утверждение 6.1.

$$\delta(a) | \phi(m)$$

Определение 6.2. a — **первообразный корень** $\mod m$, если

$$\delta(a) = \phi(m)$$

Обозначают как g.

Утверждение 6.2. *Если по* $\mod m$, $\exists$ *первообразный корень* g, *то:*

$$1, g, g^2, \ldots, g^{\phi(m)-1}$$

Образуют ***всю*** *привидённую систему вычетов* $\mod m$.

Утверждение 6.3. *При $m = 2^n, n \geq 3$ первообразных корней $\mod m$ не существует.*

Доказательство.

$$\phi(m) = 2^{n-1}$$

Покажем, что если

$$\begin{cases} a = 2t+1 \\ a^{2^{n-1}} \equiv 1 \pmod m \end{cases} \Rightarrow a^{2^{n-2}} \equiv 1 \pmod m$$

$$a^2 = 4t^2 + 4t + 1 = 4t(t+1) + 1 = 8t_1 + 1$$
$$a^4 = (8t_1+1)^2 = 64t_1^2 + 16t_1 + 1 = 16t_2$$
$$a^8 = 32t_3 + 1$$
$$\Rightarrow a^{2^k} = 2^{k+2}t_k + 1$$

Таким образом:

$$a^{2^{n-2}} = 2^n t_{n-1} + 1 \equiv 1 \pmod 2)^n$$

□

Теорема 6.2. *Первообразные корни $\mod m$ существуют, если и только если $m \in \{2, 4, p^\alpha, 2p^\alpha\}$, где p — нечётные простые.*

Определение 6.3. Дискретный логарим:

$$x = g^b \iff \operatorname{ind}_g b = x \pmod p$$

Докажем теорему для случая $m = p$:

Доказательство. Положим $\tau = [\delta(1), \ldots, \delta(p-1)]$. Тогда:

$$x^\tau \equiv 1 \pmod p), \forall x \in \{1, \ldots, p-1\} \Rightarrow \tau \geq p-1$$

С другой стороны:

$$\tau = \prod_{i=1}^{s} q_i^{\alpha_i}$$

Тогда:

$$\forall i = \overline{1, s}, \exists x_i \colon \delta(x_i) = a_i \cdot q_i^{\alpha_i}$$

<u>Утверждение</u> 6.4.
$$\delta(x_i^\alpha) = q_i^{\alpha_i}$$

<u>Утверждение</u> 6.5.

$$\delta\left(\prod_{i=1}^{s} x_i^{a_i}\right) = \prod_{i=1}^{s} q_i^{\alpha_i} = \tau$$

Отсюда следует, что

$$\tau|(p-1) \Rightarrow \tau \leq p-1 \Rightarrow \tau = p-1$$

Ч. Т. Д. □

Теперь докажем для случая $p^\alpha, \alpha > 1$

Доказательство. Пусть g — первообразый корень $\mod p$. Докажем:

<u>Лемма</u> 6.3.
$$\exists t\colon (g+pt)^{p-1} \equiv 1 + pu, (u,p) = 1$$

Доказательство.

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

$$= 1 + pb + (p-1)\cdot g^{p-2}\cdot pt + p^2\cdot a =$$
$$= 1 + p(b + (p-1)g^{p-2}\cdot t + pa)$$

Т. к. $(p-1)g^{p-2}\cdot t$ пробегает полную систему вычетов, то такое t найдётся.
□

Пусть теперь $\delta = \delta(g+pt) \pmod p)^\alpha$. Хотим доказать, что:

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

$$(g+pt)^\delta \equiv 1 \pmod p \Rightarrow (g+pt)^\delta \equiv 1 \pmod p$$

$$\Rightarrow \delta \vdots (p-1)$$

С другой стороны, $\delta|p^\alpha(p-1) \Rightarrow \delta = p^k(p-1)$

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

$$(g+pt)^{p(p-1)} = (1+pu)^p = 1 + p^2u + p^3a =$$
$$= 1 + p^2\underbrace{(u+pa)}_{u_1}, (u_1, p) = 1$$

И т. д. получаем:

$$(g+pt)^{p^k(p-1)} = (1+pu_{k-1})^p = 1 + p^{k+1}u_k, (u_k, p) = 1$$

Т. к.

$$\delta = \delta(g+pt) \Rightarrow 1 + p^{k+1}u_k \equiv 1(\mod p^\alpha)$$

Отсюда следует, что $k+1 = \alpha \Rightarrow k = \alpha - 1$ □

Случай $2p^\alpha$ слишком тривиальный, чтобы его рассматривать.

$$\phi(2p^\alpha) = \phi(p^\alpha)$$

Т. е. если $g+pt$ — нечёт, то всё ок, иначе берём $g + pt + p^\alpha$

Доказательство того, что по другим модулям нет первообразных корней остаётся студенту.

Теорема 6.4 (Шевалле)**.** *Пусть* $F(x_1, \ldots, x_n)$ *— многочлен от* n *переменных,* $\deg F < n$*. Пусть* p *— простое, тогда* N_p *— число решений сравнения:*

$$F(x_1, \ldots, x_n) \equiv 0 \pmod p$$

Тогда $N_p \equiv 0 \pmod p$

Доказательство. Заметим, что:

$$N_p \equiv \sum_{x_1=1}^{p} \ldots \sum_{x_n=1}^{p} \big(1 - F^{p-1}(x_1, \ldots, x_n)\big) =$$

$$= p^n - \sum_{x_1=1}^{p} \ldots \sum_{x_n=1}^{p} F^{p-1}(x_1, \ldots, x_n)$$

$$F^{p-1}(x_1, \ldots, x_n) = \ldots + cx_1^{\alpha_1} \ldots x_n^{\alpha_n} + \ldots$$

Достаточно доказать, что на p делится любая сумма вида:

$$\sum_{x_1=1}^{p} \ldots \sum_{x_n=1}^{p} x_1^{\alpha_1} \ldots x_n^{\alpha_n} =$$

$$= \left(\sum_{x_1=1}^{p} x_1\right) \dots \left(\sum_{x_n=1}^{p} x_n\right)$$

- Случай 1: Если среди α_i есть ноль, то соответствующая сумма $= p \Rightarrow$ всё произведение делится на p

- Случай 2: Пусть $p = 2$, тогда $\alpha_1 + \ldots + \alpha_n \leq n - 1 \Rightarrow$ выполняется случай 1.

- Случай 3: Пусть $p \geq 3$:

  $$\alpha_1 + \ldots + \alpha_n \leq (p-1)(n-1)$$

  Пусть $\forall i, \alpha_i \geq 1 \Rightarrow \exists i \colon 1 \leq \alpha_i \leq p - 2$

  $$S = \sum_{x_i=1}^{p} x_i^{\alpha_i}$$

  Возьмём g — первообразный корнень $\mod p$, тогда:

  $$g^{\alpha_i} S = \sum_{x_i=1}^{p} (gx)^{\alpha_i} \equiv S \pmod p$$

  $$\Rightarrow S \underbrace{(g^{\alpha_i} - 1)}_{\neq 0} \equiv 0 \pmod p \Rightarrow S \equiv 0$$

□

6.1.1 Немного о шифровании

Есть Алиса, Боб и Ева. Алиса и Боб хотят передевать сообщение, чтобы Ева их не смогла подслушать. Алиса выбирает число a, меньшее заданного p (простое, порядка 10^{200}, известно всем участникам), и вычисляет:

$$g^{\alpha} \pmod p.$$

Результат отправляет Бобу. Боб задумывает $b < p$, вычисляет $g^b \pmod p$, отправляет Алисе. У Алисы и Боба есть g^a и g^b, из которых они оба получают g^{ab}. Это число будет ключом, который Алиса и Боб будут использовать при переписке.

Почему Ева не может узнать ключ? А потому, что задача дискретного логарифмирования, т. е. решение ур-я (относитлельно x):

$$g^x \equiv c \pmod p$$

это трудная задача (в вычислительном плане).

7 Лекция 6

7.1 Тесты на простоту

Полиномиальные:

Вероятностные	Детерминированные
Проверяет, что числа простые с "большой вероятностью"	числа Мерсенна $2^p - 1$ AKS(2003)

7.1.1 Тест Ферма на простоту

$$a^{p-1} \equiv 1 \pmod p, \text{ если } p \text{ простое}$$

N — кандидат $\Rightarrow a^{N-1} \overset{?}{\equiv} 1 \pmod N$
Алгоритм:

1. Выбрали N, проверили, что оно не делится на маленькие простые.

2. Выбираем $a < N, (a, N) = 1$, (если (a, N), то N — составное)

$$a^{N-1} \overset{?}{\equiv} 1 \pmod N$$

3. Если $a^{N-1} \not\equiv N \pmod N \Rightarrow N$ — составное

4. Если $a^{N-1} \equiv N \pmod N \Rightarrow$ выбираем следующий остаток b, и т. д.

Рассмотрим $B_F \subseteq \mathbb{Z}_N^*$, где:

$$B_F = \{\, a \in \mathbb{Z}_N^* \mid a^{N-1} \equiv 1 \pmod N \,\}$$

Утверждение 7.1. *Если* $B_F \neq \mathbb{Z}_N^* \Rightarrow |B_F| \leq \frac{1}{2}\,|\mathbb{Z}_N^*|$

Доказательство. По умному: т. к. B_F — подгруппа $\mathbb{Z}_N^*$, то по т. Лагранжа:

$$|\mathbb{Z}_N^*| \vdots |B_F| \Rightarrow |B_F| \le \frac{1}{2}|\mathbb{Z}_N^*| \vee B_F = \mathbb{Z}_N^*$$

Альтернативно:

$$b \notin B_F, a \in B_F \Rightarrow ba \notin B_F$$

Следовательно:

$$\#\{\text{ остатки, проходящие тест Ферма }\} \le \#\{\text{ остальные }\}$$

$\square$

Определение 7.1. N — число Кармайкла, если:

$$B_F = \mathbb{Z}_N^*$$

Замечание. 561 — *минимальное числа Кармайлка.*

Утверждение 7.2. *Если N — не простое и не число Кармайкла, то после k независимых проверок:*

$$P(N\text{ — псевдопростое}) = \frac{1}{2^k}$$

Теорема 7.1. *N — число Кармайкла $\iff$*

1. *$N \not\vdots p^2$ (Ни для какого простого p)*

2. *$N = p_1 \cdot \ldots \cdot p_s$ и для $\forall i$: $(N-1) \vdots (p_i - 1)$*

Доказательство. $\Leftarrow$)

$$a \in \mathbb{Z}_N^* \overset{?}{\Rightarrow} a^{N-1} \overset{?}{\equiv} 1 \pmod N$$

Заметим, что:

$$\forall i\colon a^{N-1} \equiv 1 \pmod p_i$$

Т. к. $a^{p_i - 1} \equiv 1 \pmod p_i$. Следовательно по КТО:

$$\begin{cases} a^{N-1} \equiv 1 \pmod p_1 \\ \vdots \\ a^{N-1} \equiv 1 \pmod p_s \end{cases}$$

$$\Rightarrow a^{N-1} \equiv 1 \pmod N$$

$\Rightarrow$) 1) От противного, пусть:

$$n = p^k \cdot s, k \geq 2$$

$$a^{N-1} \equiv 1 \pmod N \Rightarrow a^{N-1} \equiv 1 \pmod p^k \Rightarrow$$
$$\Rightarrow a^{N-1} \equiv 1 \pmod p^2$$

Пусть g — первообразный корень $\mod p^2$:

$$\operatorname{ord}(g) = p(p-1)$$

Найдём a:

$$\begin{cases} a \equiv g \pmod p^k \\ a \equiv 1 \pmod s \end{cases} \Rightarrow \text{КТО}$$

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

Получаем:

$$\begin{cases} (N-1) \vdots p(p-1) \\ N \vdots p \end{cases} \Rightarrow \perp!$$

2)

$$N = p_1 \dots p_s$$

$$g_i \text{ — первообразный корень по } \mod p_i$$

Найдём a:

$$\begin{cases} a = g_i \mod p_i \\ a \equiv 1 \mod p_j, j \neq i \end{cases}$$

$$a^{N-1} \equiv 1 \pmod N$$

$$\Rightarrow g_i^{N-1} \equiv 1 \mod p_i$$

$$\Rightarrow (N-1) \vdots \operatorname{ord}(g_i) \Rightarrow (N-1) \vdots (p_i - 1)$$

$\square$

Пример.

$$561 = 3 \cdot 11 \cdot 17$$

$$560 \vdots 2, 10, 16$$

Свойства чисел Кармайкла:

1. Число Кармайкла нечётно

2. Число Кармайкла $N = p_1 \dots p_s, s \geq 3$

3. Если для некоторого k:

$$6k+1, 12k+1, 18k+1 \text{ — простые} \Rightarrow$$

$$\Rightarrow (6k+1)(12k+1)(18k+1) \text{ — число Кармайкла}$$

$$a^{N-1} \equiv 1 \pmod N \Rightarrow a^{\frac{N-1}{2}} \equiv \pm 1 \pmod N$$

$$p \text{ — просто} \Rightarrow a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod p$$

7.1.2 Символ Якоби

<u>**Определение**</u> **7.2.** Если N — нечётно ($N = p_1 \dots p_s$, p_i — нечётное простое, с повторами):

$$\underbrace{\left(\frac{a}{N}\right)}_{\text{Символ Якоби}} = \underbrace{\left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_s}\right)}_{\text{Символы Лежандра}}$$

<u>**Замечание**</u>**.** *Теперь можем написать* $a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod N$

Свойства символа Якоби:

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

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

3. $$\left(\frac{ab}{N}\right) = \left(\frac{a}{N}\right)\left(\frac{b}{N}\right)$$

4. N, M — нечётные, $(N, M) = 1 \Rightarrow$

$$\Rightarrow \left(\frac{N}{M}\right)\left(\frac{M}{N}\right) = (-1)^{\frac{N-1}{2} \cdot \frac{M-1}{2}}$$

7.1.3 Тест Соловея-Штрассена

$$B_{SS} = \{\, a \in \mathbb{Z}_N^* \mid a^{\frac{N-1}{2}} \equiv \left(\frac{a}{N}\right) \pmod N \,\}$$

Теорема 7.2. *1. $B_{SS}(N) = \mathbb{Z}_N^* \iff N$ — простое*

2. N — составное $\Rightarrow |B_{SS}(N)| \le \frac{1}{2}\,|\mathbb{Z}_N^*|$

Доказательство. Доказательство. 2) $B_{SS}(N) \ne \mathbb{Z}_N^*$, опять же по т. Лагранжа.

1) $\Leftarrow$) По св-ву символа Лежандра

$\Rightarrow$) $B_{SS} = \mathbb{Z}_N^* \Rightarrow B_F = \mathbb{Z}_N^*$, т. е. если N — не простое, то N — число Кармайкла:

$$N = p_1 \dots p_s$$

Пусть b — квадратичный невычет по $\mod p_1$:

$$\left(\frac{b}{p_1}\right) = -1$$

$$a\colon \begin{cases} a \equiv b \mod p_1 \\ a \equiv 1 \mod p_2, \dots, p_s \end{cases}$$

$$a \in B_{SS} \Rightarrow a^{\frac{n-1}{2}} = \left(\frac{a}{N}\right) \pmod N$$

$$\left(\frac{a}{N}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_s}\right) \equiv \left(\frac{b}{p_1}\right)\left(\frac{1}{p_2}\right) \dots \left(\frac{1}{p_s}\right) = -1$$

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

Тогда подставим p_2:

$$a^{\frac{N-1}{2}} \equiv 1 \equiv -1 \mod p_2 \Rightarrow \perp!$$

□

□

Замечание.

$$B_{SS} \subseteq B_F$$

Пример. $N = 15 \Rightarrow a^{14} \equiv 1 \mod 15$

$$\mathbb{Z}_{15}^* = \{\, 1, 2, 4, 7, 8, 11, 13, 14 \,\}$$

$$\mathrm{ord}(1) = 1$$

$$14^2 \equiv 1$$