Основы комбинаторики и теории чисел

Григорян Сергей

13 февраля 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:

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

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:

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

$\square$

Следствие.

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

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:

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

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

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

$$\Rightarrow p_1q_1 = |S| = |S_1| + |S_2| = \sum_{x=1}^{q_1} \left\lfloor \frac{px}{q} \right\rfloor + \sum_{y=1}^{p_1} \left\lfloor \frac{qy}{p} \right\rfloor$$

□

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:

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

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

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

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 $k = 1$:

$$1110\dots0$$

$$0111\dots0$$

Эти два слова могут исказиться до $1111\dots0$, т. е. мы их не сможем различить. С другой стороны:

$$1110\dots0$$

$$0011\dots0$$

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 $M \le \frac{2d}{2d-n}$*

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.