Основы комбинаторики и теории чисел

Григорян Сергей

6 февраля 2025 г.

Содержание

1 Лекция 1

1.1 Квадратичные вычеты и невычеты

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 $\forall i, b_i = 0$ □

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:

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

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:

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

□

Следствие.

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

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:

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

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

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

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

□