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

БОЛЬШОЕ НАЗВАНИЕ КУРСА

V СЕМЕСТР

Лектор: *Иван Иванович Иванов*

h\nu

Автор: *Павел Дуров*
Проект на Github

осень 2022

Содержание

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:

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

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

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 образхом:

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

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* $1, 2, \ldots \frac{p-1}{2} = p_1$*. Рассмотрим числа* $ax = \varepsilon_x \cdot r_x$*, где* $\varepsilon_x \in \{-1, 1\}, r_x \in \{1, 2, \ldots, p_1\}$*. 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. $r_x, r_y \leqslant \frac{p-1}{2}$. □

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

Доказательство. Если $(ax \mod p) \in \{1, 2, \ldots p_1\}$, то $(-1)^{\left[\frac{2ax}{p}\right]} = 1$, иначе $(-1)^{\left[\frac{2ax}{p}\right]} = -1$. □

Утверждение 1.3.

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

Доказательство.

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

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

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. □

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

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

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

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 $S_1 = \{(x,y) \in S | qy < px\}, S_2 = \{(x,y) \in S | qy > px\}$. 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 ровно $\left[\frac{px}{q}\right]$. Но тогда получаем, что $|S| = |S_1| + |S_2|$, что и требовалось. □