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:

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

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. $\square$

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 образхзом:

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

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 $\varepsilon_x \in \{0, 1\}, r_x \in \{1, 2, \ldots, p_1\}$. Тогда $x \neq y \Rightarrow r_x \neq r_y$.*