НИС «Основные понятия математики»

Бурман Юрий Михайлович

17 сентября 2020 г. — 8 октября 2020 г.

Квадратичные вычеты

Пусть зафиксировано число m. Будем пытаться понять, какие остатки по модулю m являются полными квадратами. Причём можно считать, что $m = p$ простое и $p > 2$.

Определение 1. Квадратичный вычет — такое число a, что существует такое b, что $b^2 \equiv a \mod p$.

Теорема 1. Если $p \equiv q \mod 4a$, то a — одновременно вычет или невычет по модулям p и q.

Лемма 2. Т. 1 выполняется для $a = -1$, т.е. -1 — вычет при $p = 4k + 3$ и невычет при $p = 4k + 1$.

Определение 2. Символ Лежандра — выражение $\left(\frac{a}{p}\right)$, равное 1, если a — квадратичный вычет по модулю p и -1, если невычет (и не определённое, если $p \mid a$).

Лемма 3. Выполняется $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$ (в частности, отсюда будет следовать **Т. 2**).

Теорема 4. $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ циклическая. То есть, существует $\varepsilon \in \mathbb{F}_p^*$ такое, что $\operatorname{ord} \varepsilon = p - 1$. Оно называется *первообразным корнем.*

Доказательство. Пусть $\operatorname{ord} a = k$. Тогда у всех чисел вида a^l при $(l, p-1) = 1$ порядок k. Заметим, что других чисел с порядком k нет. Действительно, рассмотрим многочлен $x^k - 1$. Его корни — это числа вида a^t и только они, потому что они подходят, а других нет по теореме Безу. Обозначим $\psi(d)$ — количество чисел с порядком d. Мы знаем, что если $\psi(d) \neq 0$ (и $d \mid p-1$), то $\psi(d) = \varphi(d)$. Кроме того, $\sum_{k|p-1} \psi(k) = p - 1$, и $\sum_{k|n} \varphi(k) = p - 1$ для любого n. Это значит, что на самом деле $\psi(d) = \varphi(d)$ для всех $d \mid p - 1$. ■