

25. Квадратичный закон взаимности: теория

16 июля

Определение. Пусть p — простое число, $a \not\equiv 0 \pmod{p}$. Говорят, что $a \in \mathbb{F}_p$ является квадратичным вычетом по модулю p , если существует $b \in \mathbb{F}_p$ такой, что $a \equiv b^2 \pmod{p}$. Иначе a называется квадратичным невычетом.

Упражнение. Существует $\frac{p-1}{2}$ различных квадратичных вычетов по модулю p .

Определение. Символом Лежандра назовем выражение $\left(\frac{a}{p}\right)$, равное 1, если a — квадратичный вычет по модулю p ; -1 , если a — квадратичный невычет по модулю p , и 0, если $a \equiv 0 \pmod{p}$.

1. Докажите, что

$$(a) \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}; \quad (b) \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

2. Поймем для каких простых p число $r \not\equiv 0 \pmod{p}$ является квадратичным вычетом.

(a) Рассмотрим множество вычетов $S = \{r \cdot 1, r \cdot 2, r \cdot 3, \dots, r \cdot \frac{p-1}{2}\}$. Докажите, что для каждого ненулевого $a \in \mathbb{F}_p$ ровно один из вычетов $a, p-a$ содержится в S ;

(b) отождествим каждый элемент S с целым числом из множества $\{1, 2, 3, \dots, p-1\}$. Докажите, что $\left(\frac{r}{p}\right) = (-1)^{\nu(p)}$, где $\nu(p)$ — количество элементов в S , больших $\frac{p-1}{2}$.

3. Докажите, что 2 является квадратичным вычетом по модулю p тогда и только тогда, когда $p \equiv \pm 1 \pmod{8}$.

4. Пусть p и q — различные простые нечетные числа. Рассмотрим прямоугольник на целочисленной решетке с вершинами в точках $(1, 1)$, $(1, \frac{q-1}{2})$, $(\frac{p-1}{2}, 1)$, $(\frac{p-1}{2}, \frac{q-1}{2})$. Посчитав точки внутри и на границе этого прямоугольника, докажите, что

$$\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{iq}{p}\right] + \sum_{j=1}^{\frac{q-1}{2}} \left[\frac{jp}{q}\right] = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

5. (a) Пусть p и q — различные простые нечетные числа. В условиях леммы Гаусса (задача 2b) для $a = q$ докажите, что $\nu(q) \equiv \sum_{i=1}^{(p-1)/2} \left[\frac{iq}{p}\right]$.

(b) **Квадратичный закон взаимности.** Пусть p, q — различные нечетные простые числа. Тогда выполнено равенство:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

6. Найдите

$$(a) \left(\frac{3}{239}\right); \quad (b) \left(\frac{1009}{2017}\right); \quad (c) \left(\frac{113}{967}\right).$$