

Квадратичные вычеты

Зафиксируем простое число p . Для числа a , не делящегося на p , рассмотрим сравнение $x^2 \equiv a \pmod{p}$. Если это сравнение имеет решение, то число a называется *квадратичным вычетом* по модулю p , в противном случае — *квадратичным невычетом* по модулю p . Достаточно часто слово «квадратичный» мы будем опускать.

1. Пусть $p > 2$. Докажите, что
 - (a) по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов;
 - (b) произведение двух квадратичных вычетов — вычет;
 - (c) произведение вычета на невычет — невычет;
 - (d) произведение двух невычетов — вычет.
2. Докажите, что все квадратичные вычеты являются корнями многочлена $x^{\frac{p-1}{2}} - 1 \in \mathbb{F}_p[x]$, а все невычеты — корнями многочлена $x^{\frac{p-1}{2}} + 1 \in \mathbb{F}_p[x]$

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

Из задач 1 и 2 следует, что $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$, а также $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

3. Докажите, что если $x^2 + 1$ делится на p , то p имеет вид $4k + 1$.
4. Решите в целых числах уравнение $z(y^2 - 5) = x^2 + 1$.
5. Докажите, что уравнение $4xy - x - y = z^2$
 - (a) не имеет решений в натуральных числах;
 - (b) имеет бесконечно много решений в целых числах.
6. Решите в целых числах уравнение $x^3 + 7 = y^2$.
7. Дано натуральное a , не делящееся на простое p . Рассмотрим перестановку чисел $0, 1, \dots, p-1$, на i -м месте которой стоит остаток ai от деления на p . Докажите, что эта перестановка чётна при $\left(\frac{a}{p}\right) = 1$ и нечётна при $\left(\frac{a}{p}\right) = -1$.
8. Докажите, что $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.