



Серия №17. Квадратичные вычеты

12 июля

Теория

Пусть p – нечетное простое число. Рассмотрим уравнение $x^2 \equiv a \pmod{p}$.

Определение. Если для $a \neq 0$ существует решение уравнения, то число a называется квадратичным вычетом по модулю p . В противном случае a – квадратичный невычет.

1. Докажите, что среди ненулевых остатков по модулю p ровно половина являются квадратичными вычетами.
2. Докажите следующие свойства произведений квадратичных вычетов:
 - а) вычет \times вычет = вычет;
 - б) вычет \times невычет = невычет;
 - в) невычет \times невычет = вычет.

Определение. Символом Лежандра называют выражение $\left(\frac{a}{p}\right)$, причем:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{если } a - \text{кв. вычет} \\ -1, & \text{если } a - \text{кв. невычет} \\ 0, & \text{если } a \equiv_p 0 \end{cases}$$

Заметим, что в 2 задаче мы доказали свойство $\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ при $a, b \neq 0$.

3. а) Докажите, что если $a \neq 0$ – квадратичный вычет, то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
б) Докажите, что если a – квадратичный невычет, то $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Критерий Эйлера. Если p – нечетное простое число, то:

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

4. Для остатка $a \neq 0$ рассмотрим множество остатков $A = \left\{a, 2a, \dots, \frac{p-1}{2}a\right\}$. Пусть n – количество остатков в A , больших $\frac{p}{2}$.
 - а) Докажите, что если в A каждый из остатков $k > \frac{p}{2}$ заменить на $p - k$, то полученное множество B совпадает с множеством $\left\{1, 2, \dots, \frac{p-1}{2}\right\}$.
 - б) Докажите, что $a^{\frac{p-1}{2}} \equiv_p (-1)^n$.

Критерий Гаусса. Если p – нечетное простое число, a не делится на p , то:

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

Задачи

5. Вычислите без калькулятора $\left(\frac{3}{41}\right)$ и $\left(\frac{3}{47}\right)$, выбрав наиболее удобный критерий.
6. Докажите, что при любом нечетном простом p найдется такое натуральное число x , что произведение $(x^2 - 13)(x^2 - 17)(x^2 - 221)$ делится на p .

7. Пусть p – нечетное простое, a не делится на p . Докажите, что квадратное уравнение $ax^2 + bx + c \equiv 0$ имеет решения тогда и только тогда, когда дискриминант D является квадратичным вычетом по модулю p .
8. Пусть p – простое число. Докажите, что найдется такое число k , что $k^8 \equiv 16 \pmod{p}$.
9. Пусть $p = 4k + 1$ – простое, $p > 5$. Докажите, что найдутся такие квадратичные невычеты a, b, c (возможно, одинаковые), что $a \equiv b + c \pmod{p}$.