Квадратичные вычеты

Определение. Пусть $m > 1$ — натуральное число и a — целое число, взаимно простое с m. Число a называется квадратичным вычетом по модулю m, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \ (mod\ m)$. В противном случае число a называется квадратичным невычетом по модулю m.

Обсуждаем вместе

1. Докажите, что если p — нечетное простое число, то по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов.

   Таким образом можно сделать вывод, что квадратичное сравнение вида $x^2 \equiv a \ (mod\ p)$ *при простых* p *имеет либо ноль решений, либо два решения, либо одно решение в случае* $a \equiv 0 \ (mod\ p)$.

2. Какое условие надо наложить на a, b, c, чтобы можно было утверждать, что сравнение $ax^2 + bx + c \equiv 0 \ (mod\ p)$, где $a \not\equiv 0 \ (mod\ p)$, имеет одно, два решения?

3. Докажите, что для данного модуля p
   (a) произведение двух квадратичных вычетов — вычет;
   (b) произведение вычета на невычет — невычет;
   (c) произведение двух невычетов — вычет.

4. **(a)** Докажите, что если a — квадратичный вычет по модулю p,
   то $a^{\frac{p-1}{2}} \equiv 1 \ (mod\ p)$.
   (b) Докажите, что если a — квадратичный невычет по модулю p,
   то $a^{\frac{p-1}{2}} \equiv -1 \ (mod\ p)$.

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

Из задачи 4 следует, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$.

Задачи для самостоятельного решения

1. **(a)** Докажите, что $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.
   (b) Вычислите $\left(\frac{-2}{11}\right), \left(\frac{-4}{17}\right), \left(\frac{52}{29}\right)$.

2. **Теорема Жирара.** Пусть $x^2 + y^2$ делится на простое число $p = 4k + 3$. Докажите тогда, что x и y делятся на p.

3. Для простого p найдите значение выражения

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

4. Докажите, что многочлен $x^4 + 1$ — приводим над $\mathbb{Z}_p$ при любом p.

5. Докажите, что для любого простого p найдется натуральное x такое, что $x^8 - 16$ делится на p.

6. Рассмотрим перестановку

$$\begin{pmatrix} 1 & 2 & 3 & \dots & p-1 \\ a & 2a & 3a & \dots & (p-1)a \end{pmatrix}$$

   по модулю p для некоторого $a \not\equiv 0 \ (mod\ p)$. Как связана чётность этой перестановки с $\left(\frac{a}{p}\right)$?

7. Докажите, что если n — нечетное натуральное число, то любой делитель числа $2^n - 1$ имеет вид $8k \pm 1$.

8. Рассмотрев $2 \cdot 4 \cdot 6 \cdot \dots \cdot (p-1)$ докажите, что $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

9. Пусть F_n — n-ое число Фибоначчии. Докажите, что $F_p - \left(\frac{5}{p}\right)$ делится на p при всех простых $p > 5$.