# Квадратичные вычеты

**Определение.** Пусть $n$ — натуральное число, $a$ — целое, взаимно простое с $n$. Число $a$ называется *квадратичным вычетом* по модулю $n$, если найдется целое $x$, такое что $x^2 \equiv a \pmod{n}$. В противном случае, число $a$ называется *квадратичным невычетом*.

**Определение.** *Символом Лежандра* числа $a$ по простому модулю $p > 2$ называется выражение, обозначаемое $\left(\frac{a}{p}\right)$, и принимающее значение 0, если $a$ кратно $p$, значение 1, если $a$ квадратичный вычет по модулю $p$, и значение $-1$, если $a$ невычет.

Далее во всех задачах рассматриваются квадратичные вычеты по нечетному простому модулю $p$.

**1.** **(а)** Докажите, что существует ровно $\frac{p-1}{2}$ вычетов и $\frac{p-1}{2}$ невычетов.
**(б)** Чему равно произведение всех квадратичных вычетов по модулю $p$? А всех квадратичных невычетов?

**2.** **(а)** Докажите, что произведение двух вычетов — вычет.
**(б)** Докажите, что произведение вычета на невычет — невычет.
**(в)** Докажите, что произведение двух невычетов — вычет.

**Следствие:** $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

**3.** **(а)** Докажите, что если $a$ квадратичный вычет, то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
**(б)** Докажите, что если $a$ квадратичный невычет, то $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.
*Подсказка:* Надо воспользоваться задачами 1б) и 2.

Таким образом получаем **критерий Эйлера**: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

**4.** Вычислите $\left(\frac{2+57+1543}{179}\right)$.

**5.** Даны целые числа $a, b$ и нечетное простое число $p$. Известно, что $(a, p) = 1$. Найдите, чему равна $\sum\limits_{i=0}^{p-1} \left(\frac{ax+b}{p}\right)$.

**6.** Решите уравнение в натуральных числах: $4xy - x - y = z^2$.

**7.** Докажите, что не существует натуральных чисел $m, n > 2$, таких что $\frac{m^2+1}{n^2-5}$ является целым числом.