# Серия 38. Квадратичные вычеты-1.

**Определение 1.** Ненулевой остаток $a$ при делении на $p$ называется *квадратичным вычетом* по модулю $p$, если сравнение $x^2 \equiv a\,(mod\,p)$ разрешимо и *квадратичным невычетом* в противном случае.

Далее считаем, что $p$ — простое число, большее 2.

**1.** Докажите, что квадратичных вычетов по модулю $p$ ровно $\frac{p-1}{2}$.

**2.** а) Докажите, что произведение двух квадратичных вычетов — квадратичный вычет.
б) Докажите, что частное двух квадратичных вычетов — квадратичный вычет.
в) Докажите, что произведение квадратичного вычета и квадратичного невычета — квадратичный невычет.
г) Докажите, что произведение двух квадратичных невычетов — квадратичный вычет.

**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 $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.

**4.** Простое число $p$ имеет вид $4k+1$. Докажите, что если сумма квадратов двух целых чисел делится на $p$, то каждое из них делится на $p$.

**5.** Докажите, что число $\frac{x^2-1}{y^2-5}$ никогда не является целым при натуральных $x$ и $y$.

**6.** Докажите, что простое число $p$ является делителем числа вида $x^2 - x + 3$ тогда и только тогда, когда $p$ является делителем числа вида $y^2 - y + 25$.

**7.** Докажите, что для любого простого $p$ существуют такие целые $a$ и $b$, что $a^2 + b^2 + 1$ делится на $p$.

**8.** Сколько существует пар последовательных квадратичных вычетов по модулю $p$?

**9.** Несколько команд сыграли однокруговой волейбольный турнир. Скажем, что турнир оказался *сбалансированным*, если для каждой пары команд нашлись хотя бы $k$ команд, которые выиграли у них обеих. Пусть $p = 4k+3$ — простое число. Докажите, что возможен сбалансированный турнир на $p$ командах.