# *Квадратичные вычеты*

**Определение.** Ненулевой остаток $a$ при делении на $p$ называется квадратичным вычетом по модулю $p$ если сравнение $x^2 \equiv a \pmod p$ 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 произведение квадратичного вычета и квадратичного невычета — квадратичный невычет.

   в) 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) Если $a$ - квадратичный невычет, то $a^{\frac{p-1}{2}} \equiv -1 \pmod p$

4. Докажите, что -1 является квадратичным вычетом по модулю простого нечётного числа $p$ тогда и только тогда, когда $p \equiv 1 \pmod 4$

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

6. Докажите, что если при некоторых целых $a$ и $b$ число $a^2 + b^2$ делится на $p$, где $p = 4k + 3$ — простое, то $a$ и $b$ делятся на $p$.

7. Докажите, что простых чисел вида $4k + 1$ бесконечно много

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