Квадратичные вычеты

1. Пусть x – кв. вычет по взаимно простым модулям n, $m \in \mathbb{N}$. Докажите, что x – кв. вычет по модулю nm.

2. Пусть x – кв. вычет по нечётному простому модулю p. Докажите, что x – кв. вычет по модулю p^n, $n \in \mathbb{N}$.

3. Пусть x – квадратичный вычет по модулю 8. Докажите, что x – квадратичный вычет по модулю 2^n, $n \in \mathbb{N}$.

4. Дано простое число p. Докажите, что существует такое целое число x, что $x^2 - x + 3 \vdots p$, если и только если существует такое целое число y, что $y^2 - y + 25 \vdots p$.

5. Докажите, что среди чисел $1, 2, \ldots, p-1$ ровно $\frac{p-1}{2}$ квадратичных вычетов по простому модулю $p > 2$.

6. Пусть p – нечётное простое число. Докажите, что

a) (`Эйлер`) число $a \in \mathbb{Z}$ – квадратичный вычет по модулю p тогда и только тогда, когда $a^{\frac{p-1}{2}} \equiv 1 \bmod p$;

b) для любых a, $b \in \mathbb{Z}$ верно равенство $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

7. Докажите, что $\frac{x^2+1}{y^2-5} \notin \mathbb{Z}$ при все целых x, $y > 2$.

8. Существует ли такое $n \in \mathbb{N}$, что множество $\{n, n+1, \ldots, n+1997\}$ можно разбить на несколько собственных подмножеств с равными произведениями элементов?

9. (`Золоторёв`) Пусть p – нечётное простое число и $p \nmid a$. Рассмотрим перестановку $\pi_{a,p}\colon i \to ai \bmod p$ остатков от деления на p. Докажите, что $\left(\frac{a}{p}\right) = 1$, если перестановка $\pi_{a,p}$ чётная, и $\left(\frac{a}{p}\right) = -1$, если нечётная.

10. Пусть p и q – различные нечётные простые числа. Докажите, что $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$ и $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

11. Пусть p – простое число, а $d \in \mathbb{N}$ делит $[(p+1)/4]$. Докажите, что d – квадратичный вычет по модулю p.