Квадратичные вычеты

Определение 1. Определение. Пусть $m > 1$ — натуральное число, a — целое число, взаимно простое с m. Число a называется *квадратичным вычетом* по модулю m, если существует целое число x такое, что $a \equiv x^2 \pmod{m}$. Иначе число a называется *квадратичным невычетом* по модулю m.

Определение 2. *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.

1. Докажите, что для данного нечётного простого модуля p

(а) существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов.

(б) произведение двух квадратичных вычетов — вычет;

(в) произведение вычета на невычет — невычет;

(г) произведение двух невычетов — вычет.

Полезный факт. Из задачи 1 следует, что $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

2. **(а)** Вычислите произведение всех квадратичных вычетов по модулю простого нечётного числа p. А ещё вычислите произведение всех квадратичных невычетов.

(б) **Критерий Эйлера.** Докажите, что $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

3. Найдите $\left(\frac{-2}{11}\right)$, $\left(\frac{-4}{17}\right)$, $\left(\frac{52}{29}\right)$

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

(б) 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.

(в) Докажите, что простых чисел вида $4k + 1$ бесконечно много.

5. Целое число a таково, что $a^2 - 6a + 3$ делится на некоторое простое p. Докажите, что существует целое число b такое, что $b^2 - 2b - 53$ делится на p.

6. Докажите, что уравнение $4xy - x - y = z^2$ не имеет решений в натуральных числах.