Квадратичные вычеты

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

1. Найдите все квадратичные вычеты и невычеты по модулю 11.

2. Пусть p — простое нечётное число. Докажите, что
(a) по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов;
(b) произведение двух квадратичных вычетов — вычет;
(c) произведение вычета на невычет — невычет;
(d) произведение двух невычетов — вычет.

3. Чему может быть равно произведение всех квадратичных вычетов по модулю простого нечётного числа p? А произведение всех квадратичных невычетов?

Определение. Пусть p — простое число. *Символом Лежандра* называется выражение, обозначаемое $(\frac{a}{p})$, равное 1, если a – квадратичный вычет по модулю p; -1, если a – квадратичный невычет по модулю p; и 0, если a делится на p.

4. Докажите, что $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$, где p – простое нечётное число.

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

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. Последовательность натуральных чисел $\{a_n\}$ определяется соотношениями $a_1 = 100$, $a_{n+1} = a_n^{17} + a_n + 2$. Докажите, что a_n не делится на 19 ни при каком n.