Квадратичные вычеты

Определение. Пусть $p > 2$ — простое число и a — целое число, взаимно простое с p. Число a называется квадратичным вычетом по модулю p, если существует $x \in \mathbb{N}$ такое, что $a \equiv x^2 \pmod{p}$. В противном случае число a называется квадратичным невычетом по модулю p.

1. Докажите, что если p — нечетное простое число, то по модулю p существует ровно $\frac{p-1}{2}$ квадратичных вычетов и столько же невычетов.

Таким образом можно сделать вывод, что квадратичное сравнение вида $x^2 \equiv a \pmod{p}$ *при простых* p *имеет либо ноль решений, либо два решения, либо одно решение в случае* $a \equiv 0 \pmod{p}$.

2. Докажите, что для данного модуля p
(a) произведение двух квадратичных вычетов — вычет;
(b) произведение вычета на невычет — невычет;
(c) произведение двух невычетов — вычет.

3. Будем решать следующее сравнение $x^{p-1} \equiv 1 \pmod{p}$. Из малой теоремы Ферма мы знаем, что у этого сравнения есть корни $x \equiv 1, 2, \ldots, p-1$.
(a) Докажите, что если a — квадратичный вычет по модулю p,
то $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.
(b) Докажите, что если a — квадратичный невычет по модулю p,
то $a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$.

Определение. *Символом Лежандра* называется выражение, обозначаемое $(\frac{a}{p})$, равное 1, если a — квадратичный вычет по модулю p; -1, если a — невычет по модулю p и 0, если a кратно p. Из задачи 3 следует, что $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

4. **(Теорема Жирара)** Пусть x^2+y^2 делится на простое число $p = 4k+3$. Докажите тогда, что x и y делятся на p.

5. Пусть F_n — n-ое число Фибоначчи.
(a) По индукции докажите формулу Бине

$$F_n = \frac{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}}.$$

(b) Докажите, что $F_p - (\frac{5}{p})$ делится на p при всех простых $p > 5$.

6. Докажите, что при натуральных $x, y > 2$ выражение $\frac{x^2+1}{y^2-5}$ не может принимать целые значения.

7. Последняя цифра числа $x^2 + xy + y^2$ равна нулю. Докажите, что две последние цифры этого числа равны нулю.