Квадратичные вычеты

Определение. Число a называется *квадратичным вычетом* по модулю простого p, если сравнение $x^2 \equiv a \pmod p$ имеет решение. Символ Якоби пишется как $\left(\frac{a}{p}\right)$ и равен единице, если a — вычет, и минус единице в противном случае.

1. Докажите, что сравнение $x^2 \equiv a^2 \pmod p$ имеет относительно x ровно два решения при любом a не делящемся на простое p.

2. Докажите, что по нечетному простому модулю p имеется ровно $\frac{p-1}{2}$ невычетов.

3. Докажите, что многочлен степени n со старшим членом не делящимся на p имеет среди вычетов по модулю p не более n корней.

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

5. **(a)** Опишите все p, для которых -1 является квадратичным вычетом.
(b) Опишите все p, для которых 2 является квадратичным вычетом.

6. Докажите: **(a)** $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=0}^{(p-1)/2} \left[\frac{2ak}{p}\right]}$; **(b)** $\left(\frac{a}{p}\right) = (-1)^{\sum\limits_{k=0}^{(p-1)/2} \left[\frac{ak}{p}\right]}$;

(c) *Квадратичный закон взаимности.*
Для простых нечетных p и q докажите $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

(d) Как квадратичный закон взаимности позволяет быстро вычислять символ Якоби?

7. Докажите, что уравнение $4xy - x - y = z^2$ не имеет решений в натуральных числах, но имеет бесконечно много решений в целых.

8. Решите в целых числах $x^3 + 7 = y^2$.