Квадратичные вычеты и дроби

Определение 1. Пусть Z_p множество остатков при делении на простое число p и $a \in Z_p, a \neq 0$. Тогда можно определить величину $\frac{c}{a}$ — это элемент $b \in Z_p$ такой, что $ba \underset{p}{\equiv} c$.

Упражнение 1. а) Докажите, что б) $\frac{a}{1} \underset{p}{\equiv} a$; $\frac{1}{a}\frac{1}{b} \underset{p}{\equiv} \frac{1}{ab}$;в) $\frac{c}{d}\frac{b}{a} \underset{p}{\equiv} \frac{bc}{ad}$;) $\frac{1}{a}+\frac{1}{b} \underset{p}{\equiv} \frac{a+b}{ab}$.

Определение 2. Число $r \underset{p}{\not\equiv} 0$ называется *квадратичным вычетом* модулю p (простое нечётное), если существует такое целое a такое, что $r \underset{p}{\equiv} a^2$.

Задача 1. Докажите, что квадратное уравнение $ax^2 + bx + c = 0, a \neq 0$ по простому модулю $p > 2$ имеет решение тогда и только тогда, когда $D = b^2 - 4ac$ квадратичный вычет по модулю p.

Задача 2. Докажите, что произведение:
а) кадратичного вычета на квадратичный вычет это квадратичный вычет;
б) кадратичного вычета на квадратичный невычет это квадратичный невычет;
в) квадратичный невычета на квадратичный невычет это квадратичный вычет.
г) Если a квадратичный вычет, то $\frac{1}{a}$ тоже квадратичный вычет и наоборот.

Задача 3. Пусть p — нечетное простое число. а) Докажите, что если a — квадратичный вычет по модулю p, то $a^{\frac{p-1}{2}} \underset{p}{\equiv} 1$.
б) Докажите, что произвдение всех квадратичных вычетов сравнимо либо с 1 либо с -1.
в) Докажите, что что если a — квадратичный невычет по модулю p, то $a^{\frac{p-1}{2}} \underset{p}{\equiv} -1$. *Указание: вспомните как доказывалась МТФ и теорема Эйлера.*

Определение 3. Пусть p простое число. *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.

Утверждение 1. Из задачи **2** следует, что если p нечетно, то $\left(\frac{a}{p}\right) \underset{p}{\equiv} a^{\frac{p-1}{2}}$.

Задача 4. а) При каких p вычет -1 является квадратичным вычетом по модулю p (где p — нечетное простое число)?

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

Задача 5. Мы знаем, что любой ненулевой остаток $a \in Z_p$ задаёт перестановку элементов в Z_p по правилу $b \to ab$. Пусть a квадратичный вычет, найдите чётность перестановки, связанной с a.

Задача 6. Докажите, что для любого простого p существует такое натуральное n, что $2^n + 3^n + 6^n - 1$ делится на p.

Задача 7. Решите в целых числах

$$\begin{cases} a^2 + b^2 = 5cd \\ c^2 + d^2 = 5ab \end{cases}$$