Квадратчные вычеты

Соглашение. В этом листике p — простое число.

Задача 0 (Напоминание).
а) Пусть a взаимно просто с p. Докажите, что числа $a, 2a, 3a, \ldots, (p-1)a$ дают все ненулевые остатки по модулю p.
б) **(Малая теорема Ферма)** Докажите, что $a^{p-1} \equiv 1 \mod p$.

Задача 1. а) Для каждого ненулевого остатка a по простому модулю p существует единственный обратный остаток, т.е. такой остаток b, что $ab \equiv 1 \mod p$. Обозначение: $b = a^{-1}$.
б) Остатки по простому модулю можно делить, т.е. сравнение $ax \equiv b \mod p$ имеет единственное решение.

Определение 1. Ненулевой вычет a называется *квадратичным вычетом* по простому модулю p, если существует b такое, что $a \equiv b^2 \mod p$. В противном случае a называется *квадратичным невычетом.*

Таким образом, вычеты по модулю p разбиваются на 3 группы: нулевой вычет, квадратичные вычеты и квадратичные невычеты.

Задача 2. Найдите все квадратичные вычеты по модулю 5, 7, 11, 13.

Задача 3. а) Докажите, что для ненулевого остатка c квадратное сравнение $x^2 \equiv c \mod p$ имеет ровно два решения по модулю p или не имеет их вовсе.
б) Сколько существует квадратичных вычетов по модулю p?

Задача 4. а) Докажите, что произведение двух квадратичных вычетов — квадратичный вычет.
б) Докажите, что обратный к квадратичному вычету тоже вычет.
в) Для каких остатков a верно, что $a \equiv a^{-1}$?

Задача 5 (Мультиплиактивность). а) Докажите, что произведение квадратичного вычета и квадратичного невычета — квадратичный невычет.
б) Докажите, что произведение двух квадратичных невычетов — квадратичный вычет.

Задача 6. а) При каких p количество квадратичных вычетов чётно?
б) Докажите, что -1 квадратичный вычет тогда и только тогда, когда $p = 4k + 1$.

Указание: Используя задачу 4б попробуйте разбить квадратичные вычеты на пары.
в) Используя теорему Вильсона о том, что $(p-1)! \equiv -1 \mod p$, предложите формулу для корня из -1 при $p = 4k + 1$.

Задача 7. а) Какие простые числа встречаются в разложении выражений вида $n^2 + 1$ на простые множители?
б) Докажите, что простых чисел вида 4k+1 бесконечно много.

Задача 8. Докажите, что сравнение $ax^2 + bx + c = 0$

- имеет два решения по модулю p, если дискриминант — квадратичный вычет,
- не имеет решений, если дискриминант — квадратичный невычет,
- имеет ровно одно решение по модулю p, если дискриминант равен нулю по модулю p.

Задача 9 (Теорема Жирара). Пусть $x^2 + y^2$ делится на простое число p вида $4k + 3$. Докажите, что x и y делятся на p.

Задача 10. Какой остаток дает сумма квадратичных вычетов по модулю p?