Кольца вычетов

Задача 1. Приведите пример бинарной операции на множестве, удовлетворяющей всем аксиомам абелевой группы, кроме:
а) ассоциативности; **б)** существования нейтрального и обратного элемента;
в) существования обратного элемента; **г)** коммутативности.
д) Приведите пример пары бинарных операций на множестве, для которой выполнены все аксиомы кольца, кроме дистрибутивности.

Задача 2. Найдите все целые решения уравнения **а)** $5x + 7y = 11$; **б)** $26x + 32y = 60$;
в) $28x + 30y + 31z = 365$.

Задача 3. Чему равно 17-е натуральное число, дающие остатки
а) 2 и 7 при делении на 57 и 179 ответственно?
б) 2, 4, 6, 8 от деления на 5, 9, 11, 14?

Задача 4. Составьте таблицы умножения для колец $\mathbb{Z}/n\mathbb{Z}$ для $n = 4, 5, 8$. В каждом из этих колец перечислите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов найдите обратные.

Задача 5. Пусть $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, где $p \in \mathbb{Z}_{\geqslant 0}$ — простое число.
а) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$. Вычислите произведение всех ненулевых элементов в $\mathbb{F}_p$ и докажите *теорему Вильсона*: натуральное число $p > 2$ является простым если и только если $(p-1)!+1$ делится на p.

б) Какие значения принимают многочлены $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на $\mathbb{F}_p$ и на квадратах из $\mathbb{F}_p$?

в) Сколько в $\mathbb{F}_p$ ненулевых квадратов? Всегда ли в $\mathbb{F}_p$ разрешимо уравнение $x^2 + y^2 = -1$?

г) Запишем элементы $\mathbb{F}_p$ в виде $-\frac{p-1}{2}, -\frac{p-3}{2}, \ldots, 0, 1, \ldots, \frac{p-1}{2}$.
Докажите *лемму Гаусса*: число $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» при умножении на a, чётно.

Задача 6. При каких p уравнения **а)** $x^2 = -1$; **б)** $x^2 = 2$ разрешимы в $\mathbb{F}_p$?

Задача 7. Множество остатков взаимнопростых с n будем обозначать $(\mathbb{Z}/n\mathbb{Z})^\times$. Определим функцию Эйлера формулой $\varphi(n) = |\mathbb{Z}/n\mathbb{Z}^\times|$.
а) Докажите *теорему Эйлера*: $a^{\varphi(n)} = 1$ для любого $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.
б) Покажите что $\varphi(n) = n(1 - p_1^{-1}) \ldots (1 - p_k^{-1})$, если $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, где p_i — различные простые числа.
в) Найдите остаток от деления $(3^{101} + 5^{101})^{1000}$ на 75.
г) Найдите сумму всех дробей вида $\frac{k}{n}$, $k < n$, где k и n — взаимно просты.

Задача 8. а) Сколько решений в кольце $\mathbb{Z}/360\mathbb{Z}$ имеет уравнение $x^2 = 2$?
б) Сколько решений в кольце $\mathbb{Z}/n\mathbb{Z}$ имеет уравнение $x^2 = 1$?

Задача 9. (Первообразные корни) **а)** Пусть ξ — первообразный корень по модулю простого $p > 2$. Докажите, что существует такое число $k \in \mathbb{N}$, что $(\xi + pk)^{p-1} = 1$ в $\mathbb{Z}/p\mathbb{Z}$, но $(\xi + pk)^{p-1} \neq 1$ в $\mathbb{Z}/p^2\mathbb{Z}$ и класс $\xi + pk$ является первообразным корнем по модулю p^m для всех $m \in \mathbb{N}$.

б) Докажите существование первообразного корня по модулю $2p^k$ для всех простых p и всех $k \in \mathbb{N}$.

в) Покажите, что первообразный корень в $\mathbb{Z}/n\mathbb{Z}$ существует только для $n = 2, 4, p^k, 2p^k$, где $p > 2$ — простое, $k \in \mathbb{N}$. Иными словами, группа $\mathbb{Z}/n\mathbb{Z}^\times$ циклическая только при $n = 2, 4, p^k, 2p^k$.
г) Найдите количество первообразных корней в $\mathbb{Z}/n\mathbb{Z}$. Если a — первообразный корень по модулю n, как выражаются все остальные первообразные корни?
д) Найдите минимальный простой делитель числа $1^{60} + \ldots + 33^{60}$.

Задача 10. Пусть $f : A \to B$ — ненулевой гомоморфизм коммутативных колец с единицами. Верно ли, что $f(1) = 1$? А если в B нет делителей нуля?

Задача 11. Введём на множестве X функций $f\colon \mathbb{Z}_{>0} \to \mathbb{R}$ две операции:

(1) поточечное сложение: $(f+g)(n) = f(n) + g(n)$;
(2) свёртка Дирихле: $(f * g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

Докажите, что $(X, +, *)$ — коммутативное кольцо с единицей. Опишите все обратимые элементы. Найдите обратный элемент к функции

$$1 : \mathbb{Z}_{>0} \xrightarrow{n\mapsto 1} \mathbb{R}.$$