Кольца вычетов

А1.1. Составьте таблицы умножения для колец $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$, $\mathbb{Z}/8\mathbb{Z}$. В каждом из этих колец найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

А1.2. а) Найдите НОД(x, y), где x — число, составленное из первых пяти цифр вашего мобильного телефона (не считая восьмёрки), а y — из последних пяти цифр, и представьте НОД(x, y) в виде $ax + by$, где $a, b \in \mathbb{Z}$.

б) Найдите НОД многочленов $f = x^5 - 1$ и $g = x^4 + x^2 + 1$ в кольце $\mathbb{Q}[x]$ и представьте его в виде $af + bg$, где $a, b \in \mathbb{Q}[x]$.

А1.3. а) Пусть $a, b \in \mathbb{F}_p$ – ненулевые остатки по модулю p (где p — простое число). Докажите, что число различных элементов вида $a^k b$ не зависит от b и делит $p - 1$.

Указание. Воспользуйтесь тем, что в $\mathbb{F}_p$ можно делить на ненулевые элементы.

б) Докажите *малую теорему Ферма*: $a^p = a \pmod p$ для всякого простого числа p и $a \in \mathbb{Z}$.

в) Найдите число различных раскрасок карусели с p кабинками в a цветов (каждую кабинку в один цвет), и еще раз докажите малую теорему Ферма.

А1.4. а) Докажите, что многочлен степени m с коэффициентами в $\mathbb{F}_p$ имеет в $\mathbb{F}_p$ не более m корней.

Указание. Многочлены с коэффициентами в $\mathbb{F}_p$ можно делить с остатком.

б) Разложите многочлен $x^p - x$ с коэффициентами в $\mathbb{F}_p$ в произведение линейных множителей.

Указание. Воспользуйтесь малой теоремой Ферма.

в) Докажите *теорему Вильсона*: натуральное число p просто тогда и только тогда, когда $(p-1)! + 1$ делится на p.

А1.5. Остаток $a \in \mathbb{F}_p$ называется *квадратичным вычетом*, если существует такой остаток $b \in \mathbb{F}_p$, что $b^2 = a$.

а) Сколько существует квадратичных вычетов по модулю p?

б) Докажите, что -1 не является квадратичным вычетом для $p = 4k + 3$.

в) Докажите, что -1 является квадратичным вычетом для $p = 4k + 1$.

г) Докажите, что простых чисел вида $p = 4k + 1$ бесконечно много.

А1.6. *Функция Эйлера* $\varphi(n)$ сопоставляет натуральному числу n количество натуральных чисел, меньших n и взаимно простых с n (т.е. количество обратимых элементов $\mathbb{Z}/n\mathbb{Z}$). Найдите

а) $\varphi(p)$, где p — простое число;

б) $\varphi(p^k)$, где p — простое число, $k \in \mathbb{Z}$;

в) $\varphi(p_1^{k_1} \cdot \ldots \cdot p_m^{k_m})$, где p_i — различные простые числа.

г) Докажите *теорему Эйлера*: $a^{\varphi(n)} = 1 \pmod n$, если НОД$(a, n) = 1$.

А1.7. *Функция Мебиуса* $\mu(n)$ равна $(-1)^k$, если n есть произведение k попарно различных простых чисел, и равна нулю для всех остальных натуральных чисел (в частности, $\mu(1) = 1, \mu(2) = \mu(3) = -1, \mu(6) = 1, \mu(4) = \mu(12) = 0$).

а) Докажите *формулу обращения Мебиуса*: если $b(n) = \sum\limits_{d|n} a(d)$, то $a(n) = \sum\limits_{d|n} b(d)\mu(\frac{n}{d})$.

б) Выразите $\varphi(n)$ в виде суммы по всем делителям числа n.

А1.8. Сколько решений имеет уравнение $x^2 = 1$ в $\mathbb{Z}/n\mathbb{Z}$, если **а)** n нечетно; **б)** n четно?