## Алгебраические структуры и кольца вычетов.

**Задача 1. а)** Докажите, что множества $\mathbb{Z}$ и $2\mathbb{Z}$ изоморфны как абелевы группы относительно сложения. Изоморфны ли они как кольца?
**б)** Изоморфны ли как абелевы группы $(\mathbb{R},+)$ и $(\mathbb{Q},+)$? $(\mathbb{Q},+)$ и $(\mathbb{Z},+)$?

**Задача 2. а)** Докажите, что любая подгруппа $(\mathbb{Z},+)$ имеет вид $n\mathbb{Z}$, где $n \geq 0$.
**б)** Найдите обратный элемент к $[157]$ в кольце $\mathbb{Z}/235\mathbb{Z}$ и все целые решения уравнения $157x+235y = 11$.

**Задача 3.** Убедитесь, что $\mathbb{Z}[\sqrt{5}] = \{a+b\sqrt{5} \mid a, b \in \mathbb{Z}\}$ является коммутативным кольцом с единицей без делителей нуля (*областью целостности*). Покажите, что это кольцо не является факториальным.

**Задача 4. а)** Чему равно 17-е натуральное число, дающие остатки 2, 4, 6, 8 от деления на 5, 9, 11, 14?
**б)** Сколько решений в кольце $\mathbb{Z}/360\mathbb{Z}$ имеет уравнение $x^2 = 2$?
**в)** Сколько решений в кольце $\mathbb{Z}/n\mathbb{Z}$ имеет уравнение $x^2 = 1$?

**Задача 5.** Рассмотрим группу обратимых элементов $(\mathbb{Z}/n\mathbb{Z})^\times$. 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 $\varphi(n) = n(1-p_1^{-1})\dots(1-p_k^{-1})$, где $n = p_1^{\alpha_1}\dots p_k^{\alpha_k}$, $p_i$ — различные простые числа.

**Задача 6.** 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: $(f*g)(n) = \sum_{d|n} f(d)g(\frac{n}{d})$.

**а)** Докажите, что $(X,+,*)$ — коммутативное кольцо с единицей (какая функция является единицей этого кольца?). Опишите все обратимые элементы.
**б)** Найдите обратный элемент к функции

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

Этот элемент называется *функцией Мёбиуса.*

**Задача 7. а)** Пусть $\xi$ — первообразный корень по модулю простого $p > 2$. Докажите, что $\xi$ или $\xi+p$ является первообразным корнем по модулю $p^2$.
**б)** Докажите, что если $\xi$ – первообразный корень по модулю $p$ и $p^2$, то $\xi$ – первообразный корень по модулю $p^k$ для любого $k > 0$.

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

**г)** 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 $n = 2, 4, p^k, 2p^k$.
**д)** Найдите количество первообразных корней в $\mathbb{Z}/n\mathbb{Z}$. Если $a$ — первообразный корень по модулю $n$, как выражаются все остальные первообразные корни?