Примеры коммутативных колец

A2◇1 (кольца вычетов). Составьте таблицы умножения для колец $\mathbb{Z}/(m)$ с $4 \leqslant m \leqslant 8$. В каждом из этих колец перечислите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты, а для обратимых элементов укажите таблицу обратных.

A2◇2. В кольце $\mathbb{Z}/(360)$ найдите все решения уравнений **а)** $x^2 = 1$ **б)** $x^3 = 1$ **в)** $x^2 = 49$.

A2◇3. Чему равно третье по величине натуральное число, одновременно дающее остатки 2, 4, 6, 8 от деления, соответственно, на 5, 7, 8, 9?

A2◇4. Найдите все целые решения уравнения $28\,x + 30\,y + 31\,z = 365$.

A2◇5 (функция Эйлера). Обозначим через $\varphi(n)$ число обратимых элементов кольца $\mathbb{Z}/(n)$.

а) Покажите, что $\varphi(mn) = \varphi(m)\varphi(n)$ для взаимно простых m, n, и для $m = p_1^{k_1} \cdots p_n^{k_n}$, где все p_i просты и различны, $\varphi(m) = m \cdot \left(1 - p_1^{-1}\right) \cdots \left(1 - p_n^{-1}\right)$.

б) Найдите все n с $\varphi(n) = 10$.

A2◇6 (теорема Эйлера). Вычислите $a^{\varphi(n)}$ для произвольного обратимого $a \in \mathbb{Z}/(n)$.

A2◇7 (простое поле). Рассмотрим поле $\mathbb{F}_p \stackrel{\text{def}}{=} \mathbb{Z}/(p)$, где $p > 2$ — целое простое число.

а) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов из $\mathbb{F}_p$ и докажите *теорему Вильсона*: натуральное $m \geqslant 2$ просто $\iff m \mid ((m-1)! + 1)$.

б) Опишите множество значений многочленов $x^p - x$, x^{p-1} и $x^{\frac{p-1}{2}}$ на всём поле $\mathbb{F}_p$ и на множестве квадратов поля $\mathbb{F}_p$.

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

г*) (лемма Гаусса о квадратичных вычетах) Выпишем элементы поля $\mathbb{F}_p$ в виде

$$-(p-1)/2,\ \ldots\ , -1,\ 0,\ 1,\ \ldots\ ,\ (p-1)/2\,.$$

Покажите, что число $a \in \mathbb{F}_p$ является квадратом если и только если количество «положительных» элементов этой записи, которые становятся «отрицательными» от умножения на a, чётно.

д*) При каких p в $\mathbb{F}_p$ разрешимы уравнения: 1) $x^2 = -1$ 2) $x^2 = 2$?

A2◇8. Найдите все обратимые элементы в кольцах

а) (Гауссовы числа) $\mathbb{Z}[i] \stackrel{\text{def}}{=} \{\, a + bi \in \mathbb{C} \mid a, b \in \mathbb{Z},\ i^2 = -1 \}$

б) (числа Кронекера) $\mathbb{Z}[\omega] \stackrel{\text{def}}{=} \{a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z},\ \omega^2 + \omega + 1 = 0\}$.

A2◇9. Покажите, что всякий ненулевой гомоморфизм колец $\mathbb{Q} \to \mathbb{Q}$ или $\mathbb{R} \to \mathbb{R}$ тождествен.

A2◇10*. Есть ли среди фактор колец[1] кольца $\mathbb{Z}[i]$ поле характеристики **а)** 2 **б)** 3, и если да, то сколько элементов может быть в таком поле?

A2◇11*. При каких простых p существует ненулевой гомоморфизм колец $\mathbb{Z}[i] \to \mathbb{Z}/(p)$?

A2◇12*. Разложите 5 на неприводимые[2] множители в кольце $\mathbb{Z}[i]$. Какие неприводимые $p \in \mathbb{Z}$ остаются таковыми и в $\mathbb{Z}[i]$?

---

[1] Кольцо B называется *фактор кольцом* кольца A, если имеется сюръективный гомоморфизм колец $A \twoheadrightarrow B$.

[2] Элемент q коммутативного кольца с единицей называется *неприводимым*, если равенство $q = ab$ влечёт обратимость a или b.