Примеры вычислений в коммутативных кольцах

А2◇1 (поле $\mathbb{F}_p$). Пусть $\mathbb{F}_p \overset{\text{def}}{=} \mathbb{Z}/p\mathbb{Z}$, где $p \in \mathbb{N}$ — простое. **а)** Покажите, что $\mathbb{F}_p$ — поле.

б) Решите в $\mathbb{F}_p$ уравнение $x^2 = 1$, вычислите произведение всех ненулевых элементов этого поля и докажите *теорему Вильсона*: натуральное $p \geqslant 2$ просто, если и только если оно делит $(p-1)! + 1$.

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

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

д*) Выпишем $\mathbb{F}_p$ в виде: $-(p-1)/2\,,\ \dots\,,\ -1\,,\ 0\,,\ 1\,,\ \dots\,,\ (p-1)/2$. Докажите *лемму Гаусса*: $a \in \mathbb{F}_p$ тогда и только тогда является квадратом, когда число «положительных» чисел этой записи, становящихся «отрицательными» при умножении на a, чётно.

А2◇2. При каких p в $\mathbb{F}_p$ разрешимы уравнения[1] **а)** $x^2 = -1$ **б)** $x^2 = 2$

А2◇3 (взаимная простота). Пусть $ax + by = 1$ в некотором коммутативном кольце A. Справедливы для произвольного $m \in A$ импликации: **а)** $a|mb \Rightarrow a|m$ **б)** $a|m \ \&\ b|m \Rightarrow ab|m$.

А2◇4 (кольца вычетов). Составьте таблицы умножения для колец $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/6\mathbb{Z}$, $\mathbb{Z}/7\mathbb{Z}$ и $\mathbb{Z}/8\mathbb{Z}$. В каждом из этих колец найдите все обратимые элементы, все квадраты, все делители нуля и все нильпотенты. Для обратимых элементов постройте таблицу обратных.

А2◇5 (функция Эйлера). Обозначим через $\varphi(n)$ число обратимых элементов кольца $\mathbb{Z}/n\mathbb{Z}$.

а) Верно ли, что $k \pmod n$ обратим в $\mathbb{Z}/n\mathbb{Z} \iff \text{нод}(n,k) = 1$ в $\mathbb{Z}$.

б) Выясните, является ли $\varphi(n)$ *мультипликативным характером*[2] и покажите, что для $n = p_1^{k_1} \cdots p_n^{k_n}$ (где все p_i просты и различны)

$$\varphi(m) = \varphi\left(p_1^{k_1}\right)\varphi\left(p_2^{k_2}\right)\cdots\varphi\left(p_n^{k_n}\right) = m\cdot\left(1 - \frac{1}{p_1}\right)\cdots\left(1 - \frac{1}{p_n}\right).$$

в) Найдите все m такие, что $\varphi(m) = 10$.

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

Евклидовы кольца. Коммутативное кольцо A с единицей и без делителей нуля называется *евклидовым*, если на нём существует *евклидова норма* (или *высота*) — функция $A \setminus \{0\} \xrightarrow{\nu} \mathbb{Z}_{\geqslant 0}$, такая что $\forall\, a, b \in A$ $\nu(ab) \geqslant \nu(a)$ и при $b \neq 0$ $\exists\, q, r \in A : a = bq + r$, причём либо $r = 0$, либо $\nu(r) < \nu(b)$.

А2◇6. Покажите, что в евклидовом кольце $\nu(ab) = \nu(a)$ тогда и только тогда, когда b обратим.

А2◇7 (алгоритм Евклида). Пусть A — евклидово кольцо, $a, b \in A$, и $\nu(a) > \nu(b)$. Рассмотрим (какую-нибудь) последовательность элементов $r_n \in A$, в которой $r_1 = a$, $r_2 = b$ и при $n > 2$ $r_n = r_{n-2} - q_{n-1} r_{n-1}$ есть «остаток» от деления r_{n-2} на r_{n-1} (такой, что либо $\nu(r_{n-1}) > \nu(r_n)$, либо $r_n = 0$). Докажите, что

а) последний ненулевой r_d делит a и b и делится на любой общий делитель[3] a и b;

б) $\forall\, a, b \in A\ \exists\, x, y \in A : ax + by = \text{нод}(a,b)$

в) Подберите такие x, y и найдите $\text{нод}(a,b)$ для $(a,b) = (\,8\,385\,403\,,\ 2\,442\,778\,)$ в кольце $\mathbb{Z}$ и $(a,b) = (x^5 - 1, x^4 + x^2 + 1)$ в кольце $\mathbb{Q}[x]$.

А2◇8. Найдите все обратимые элементы следующих подколец поля $\mathbb{C}$:

а) $\mathbb{Z}[i] \overset{\text{def}}{=} \{\, a + bi \in \mid a, b \in \mathbb{Z}\,,\ i^2 = -1 \}$ **б)** $\mathbb{Z}[\omega] \overset{\text{def}}{=} \{ a + b\omega \in \mathbb{C} \mid a, b \in \mathbb{Z}\,,\ \omega^2 + \omega + 1 = 0\,\}$

и выясните, являются ли эти кольца евклидовыми относительно высоты $\nu(z) = |z|^2$.

А2◇9*. Разложите 5 на простые множители в кольце $\mathbb{Z}[i]$. Какие простые $p \in \mathbb{Z}$ остаются простыми и в $\mathbb{Z}[i]$?

А2◇10*. Есть ли среди фактор колец кольца $\mathbb{Z}[i]$ поле характеристики **а)** 2 **б)** 3, и если да, то сколько в нём может быть элементов?

А2◇11*. При каком простом p существует ненулевой гомоморфизм $\mathbb{Z}[i] \longrightarrow \mathbb{Z}/p\mathbb{Z}$?

---

[1] ответы: в (а) — $p = 2$ и $p \equiv 1 \pmod 4$; в (б) — когда $(p^2 - 1)/8$ чётно

[2] $\mathbb{Z} \xrightarrow{f} \mathbb{C}$ называется *мультипликативным характером*, если $f(mn) = f(m)f(n)$ $\forall\, m, n$ с $\text{нод}(m,n) = 1$

[3] всякий элемент с такими свойствами называется *наибольшим общим делителем* a и b и обозначается $\text{нод}(a,b)$