Целые числа и вычеты

АЛ1◇1. Найдите все целые решения уравнения $28\,x + 30\,y + 31\,z = 365$.

АЛ1◇2. Найдите все натуральные числа, кратные тридцати и имеющие ровно тридцать различных натуральных делителей[1].

АЛ1◇3. В кольце $\mathbb{Z}/(360)$ найдите все решения уравнений **а)** $x^2 = 1$ **б*)** $x^3 = 1$ **в*)** $x^2 = 49$.

АЛ1◇4 (функция Эйлера). Обозначим через $\varphi(n)$ количество обратимых элементов в кольце $\mathbb{Z}/(n)$. Покажите, что **а)** $\varphi(mn) = \varphi(m)\varphi(n)$ для взаимно простых m, n

б) $\varphi(m) = m \cdot \left(1 - p_1^{-1}\right) \cdots \left(1 - p_n^{-1}\right)$ для $m = p_1^{k_1} \cdots p_n^{k_n}$, где все p_i просты и различны.

в) Найдите все $n \in \mathbb{N}$ с $\varphi(n) = 10$.

АЛ1◇5. Какой остаток от деления на 179 имеет число $2021^{2022^{2023}}$?

АЛ1◇6 (порядки вычетов). Покажите, что вычет $a \in \mathbb{Z}/(n)$ обратим если и только если существует такое $k \in \mathbb{N}$, что $a^k = 1$ в $\mathbb{Z}/(n)$. Наименьшее такое k называется *порядком* обратимого вычета a. Найдите порядок произведения $a = a_1 \ldots a_n$ обратимых вычетов попарно взаимно простых порядков $k_1, \ldots, k_n$ и для любых двух обратимых вычетов a и b порядков k и m постройте вычет порядка НОК(k, m).

АЛ1◇7 (первообразные корни). Обратимый вычет порядка $\varphi(n)$ в $\mathbb{Z}/(n)$ называется *первообразным корнем* по модулю n. **а)** Существует ли первообразный корень в $\mathbb{Z}/(21)$?

б*) Докажите существование первообразного корня по любому простому модулю.

в*) Пусть r — первообразный корень по простому модулю $p > 2$. Докажите, что существует такое $t \in \mathbb{N}$, что $(r + pt)^{p-1} = 1$ в $\mathbb{Z}/(p)$, но $(r + pt)^{p-1} \neq 1$ в $\mathbb{Z}/(p^2)$, и вычет $r + pt$ является первообразным корнем в $\mathbb{Z}/(p^k)$ для всех $k \in \mathbb{N}$.

г*) Докажите существование первообразного корня в $\mathbb{Z}/(2p^k)$ для простых $p > 2$ и $k \in \mathbb{N}$.

АЛ1◇8 (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 если и только если оно делит $(m-1)! + 1$.

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

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

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

д*) (лемма Гаусса о квадратичных вычетах) Выпишем элементы поля $\mathbb{F}_p$ в виде «числовой прямой»: $-(p-1)/2, \ldots, -1, 0, 1, \ldots, (p-1)/2$. Покажите, что $a \in \mathbb{F}_p$ является квадратом если и только если количество «положительных» точек, которые становятся «отрицательными» от умножения на a, чётно.

АЛ1◇9. Найдите все обратимые элементы в кольцах

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

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

АЛ1◇10*. Есть ли среди фактор колец[2] кольца $\mathbb{Z}[i]$ поле характеристики **а)** 2 **б)** 3, и если да, то сколько элементов может быть в таком поле?

АЛ1◇11*. При каких простых p существует ненулевой гомоморфизм колец $\mathbb{Z}[i] \to \mathbb{Z}/(p)$?

АЛ1◇12*. Разложите 5 на неприводимые[3] множители в кольце $\mathbb{Z}[i]$. Какие простые $p \in \mathbb{Z}$ остаются неприводимыми в $\mathbb{Z}[i]$?

---

[1] Включая единицу и само число.

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

[3] Элемент q коммутативного кольца с единицей называется *приводимым*, если он является произведением двух необратимых элементов.

Персональный табель _____. **Листок № 1 (01.09.2022)**

(напишите свои имя, отчество и фамилию)

№	дата	кто принял	подпись
1			
2			
3а			
б			
в			
4а			
б			
в			
5			
6			
7а			
б			
в			
г			
8а			
б			
в			
г			
д			
9а			
б			
10а			
б			
11			
12			