Сравнения по модулю и уравнения в целых числах

Решим уравнение: $ax + by + cz = d$, где a, b, c, d — целые константы.

Задача 1. a) Покажите, что это уравнение имеет целые решения $\iff d \vdots \text{НОД}(a, b, c)$.

b) Пусть (x_0, y_0, z_0) — некоторое решение. Тогда все решения имеют вид

$$(x_0, y_0, z_0) + \alpha(x_1, y_1, z_1) + \beta(x_2, y_2, z_2),$$

где $(x_1, y_1, z_1), (x_2, y_2, z_2)$ — некоторые фиксированные решения уравнения $ax + by + cz = 0$, а $\alpha, \beta \in \mathbb{Z}$ — произвольные.

c) Найдите число решений уравнения $ax + by = d$ в $\mathbb{Z}/c\mathbb{Z}$.

d) Решите уравнение $6x + 10y + 15z = 2017$ в целых числах.

Задача 2. Пусть $(G, \cdot)$ — коммутативная группа. Рассмотрим отображение $\phi_d \colon G \to G$, $\phi_d(x) = x^d$. Обозначим $G^d := \operatorname{im} \phi_d$.

a) Покажите, что ϕ_d — гомоморфизм групп. Покажите, что из $g \in G$ извлекается корень степени $d \iff$ образ g при отображении $G \to G/G^d$ равен нулю. Как найти все корни?

Говорят, что этот образ в G/G^d есть препятствие к существованию корня.

b) Пусть группа G конечная. Проверьте, что $|\ker \phi_d| = |G/G^d|$.

c) Пусть $p \in \mathbb{N}$ — простое. Убедитесь в том, что для $G = (\mathbb{Z}/p\mathbb{Z})^*$ группа препятствий G/G^2 изоморфна группе из двух элементов $(\{\pm 1\}, \cdot)$ и при этом отображение $G \to G/G^2$ соответствует отображению $x \mapsto x^{\frac{p-1}{2}}$.

Пусть $G = \langle g \rangle_n = \{e, g, g^2, \ldots, g^{n-1}\}$ — циклическая группа порядка n.

Задача 3. Найдите для G все

a°) порождающие элементы;

b°) элементы порядка k;

c°) решения уравнения $x^k = e$;

d) подгруппы и факторгруппы;

e) эндоморфизмы (т.е., гомоморфизмы групп $G \to G$);

f) автоморфизмы (т.е., изоморфизмы групп $G \to G$).

В каждом пункте посчитайте, сколько их.

Задача 4. a) Покажите, что любая под- и факторгруппа циклической группы циклическая.

b) Пусть H_1, H_2 — подгруппы порядков n_1 и n_2 соответственно в циклической группе G порядка n. Найдите порядки подгрупп $H_1 \cap H_2$ и $H_1 H_2 = \{h_1 h_2 \mid h_i \in H_i\}$ в G.

Задача 5. Пусть $p \in \mathbb{N}$ — простое. Покажите, что

a) сравнение $x^d \equiv a \pmod p$ имеет решения $\iff a \equiv 0$ или $a^f \equiv 1 \pmod p$, где $f = \frac{p-1}{\text{НОД}(d, p-1)}$;

b) если решения существуют, то их число равно $\text{НОД}(d, p-1)$.

c) Что есть группа препятствий в этом случае?

Задача 6. Решите сравнения $a^\circ)\, x^3 \equiv 5 \pmod{17}$; $b^\circ)\, x^{12} \equiv 4 \pmod{17}$; c) $x^3 \equiv 5 \pmod{289}$; d) $x^{12} \equiv 4 \pmod{289}$; e) $x^{27} \equiv 27 \pmod{41}$.

Задача 7. Пусть $p \in \mathbb{N}$ — простое, а числа $a \in \mathbb{Z}, d \in \mathbb{N}$ взаимно просты с p. Докажите, что для любого $k \in \mathbb{N}$ имеется биекция между решениями уравнения $x^d = a$ по модулю p и решениями уравнения $x^d = a$ по модулю p^k.

Вычислим группы обратимых элементов в $\mathbb{Z}/p^k\mathbb{Z}$, где p простое.

Задача 8. Пусть $p \geqslant 3$. Покажите, что

a) Порядок числа $1+p$ в $(\mathbb{Z}/p^k\mathbb{Z})^*$ равен p^{k-1}.

b) В $(\mathbb{Z}/p^k\mathbb{Z})^*$ имеется ровно $p-1$ такой элемент x, что $x^{p-1} \equiv 1$.

c) В $(\mathbb{Z}/p^k\mathbb{Z})^*$ имеются элементы порядка $p-1$.

d) Группа $(\mathbb{Z}/p^k\mathbb{Z})^*$ изоморфна $\mathbb{Z}/p^{k-1}\mathbb{Z} \times \mathbb{Z}/(p-1)\mathbb{Z}$ и является циклической.

Найдите какой-нибудь образующий элемент в e) $(\mathbb{Z}/17\mathbb{Z})^*$, f) $(\mathbb{Z}/41^2\mathbb{Z})^*$, g) $(\mathbb{Z}/125\mathbb{Z})^*$.

Задача 9. Пусть $p = 2$. Покажите, что

a) При $k \geqslant 3$ порядок числа 3 в $(\mathbb{Z}/2^k\mathbb{Z})^*$ равен 2^{k-2}.

b) Элемент -1 имеет порядок 2 и не лежит в порождённой 3 подгруппе в $(\mathbb{Z}/2^k\mathbb{Z})^*$.

c) При $k \geqslant 3$ группа $(\mathbb{Z}/2^k\mathbb{Z})^*$ изоморфна $\langle 3\rangle_{2^{k-2}} \times \langle -1\rangle_2 = \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ и не является циклической.