Гаттаров Тимур Б05-304 (23/02/2024)

Задача 1. *Найдите число решений $x_{15} = e$ в группе C_{54}. Выпишите эти решения, если a - образующий группы.*

Решение. Всего таких решений НОД$(15, 54) = 3$. Решением уравнения будут a^k : $54|15k$.

$$k_{min} = \frac{\text{НОК}(54, 15)}{15} = 18$$

Решения уравнения: $x = \{a^0, a^{18}, a^{36}\}$ □

Задача 2. *Найти все первообразные корни в* $\mathbb{Z}_{37}^*$

Решение. Подсчитаем количеством элементов в $\mathbb{Z}_{37}^*$:

$$\varphi(37) = 36$$

Тогда по теореме Лагранжа возможные порядки a: $2, 4, 6, 9, 12, 18, 36$. Покажем, что 2 первообразный элемент. Достаточно показать, что $a^{12} \not\equiv 1 \bmod 37$ и $a^{18} \not\equiv 1 \bmod 37$.

$$2^{18} = 32^3 \cdot 2^3 \equiv (-5)^3 \cdot 8 \equiv 25 \cdot (-40) \equiv (-12) \cdot (-3) \equiv 36 \bmod 37$$
$$2^{12} = 32^2 \cdot 2^2 \equiv (-5)^2 \cdot 4 \equiv 25 \cdot 4 \equiv 26 \bmod 37$$

Все остальные первообразные корни представимы в виде 2^p, где НОД $(p, 36) = 1$. Их количество $\varphi(\varphi(37)) = (3^2 - 3) \cdot (2^2 - 2) = 12$.

Ответ: $\{2^1,\ 2^5,\ 2^7,\ 2^{11},\ 2^{13},\ 2^{17},\ 2^{19},\ 2^{23},\ 2^{25},\ 2^{29},\ 2^{31},\ 2^{35}\}$

□

Задача 3. *Вычислить* $12^{257} \bmod 17$

Решение.

$$12^{257} = 12 \cdot 12^{256} = 12 \cdot 3^{256} \cdot 2^{128} \cdot 2^{128} = 12 \cdot 18^{128} \cdot 16^{32} \equiv 12 \cdot 1^{128} \cdot (-1)^{32} \bmod 17 = 12$$

□

Задача 4. *Делится ли* $25^{54} - 1$ *на* 107?

Решение. Воспользуемся малой теоремой Ферма:

Теорема 0.1. *Малая теорема Ферма*
Пусть $a, p \in \mathbb{N}, \text{GCD}(a, p) = 1, p-$ *простое. Тогда* $a^{p-1} \equiv 1 \bmod p$.

$$25^{54} = 5^{108} = 25 \cdot 5^{107-1} \equiv 25 \cdot 1 \bmod 107 \equiv 25 \bmod 107$$

Из полученного очевидно, что $25^{54} - 1$ не делится на 107. □

Задача 5. *Докажите, что в группе S_8 нет элементов порядка 56. Постройте элемент порядка 56 в какой-нибудь симметрической группе.*

Решение. Воспользуемся утверждением: *Порядок перестановки равен НОК длин всех циклов в её цикловом представлении.*

Чтобы поличить НОК = 15, необходимо наличие циклов длины 7 и 8 в S_8. Но $7+8 = 15 > 8$. Пример элемента порядка 56 в группе S_{15}:

$$(1, 2, ...7, 8)(9, 10, ...14, 15).$$

□

Задача 6. *Пусть $a = (154)(23), b = (12)(5364), a, b \in S_6$*

1. *Запишите перестановки в стандартном виде*
2. *Вычислите $a \circ b$*
3. *Найдите x, если $a \circ x = b$*
4. *Запишите ответы в цикловом представлении*

Решение.

1.

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 2 & 1 & 4 & 6 \end{pmatrix}$$

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 3 & 4 \end{pmatrix}$$

2.

$$c = a \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 6 & 4 & 2 & 1 \end{pmatrix}$$

3.

$$a^{-1} = \begin{pmatrix} 5 & 3 & 2 & 1 & 4 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 1 & 6 \end{pmatrix}$$

$$x = a^{-1} \circ b = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 1 & 2 & 5 \end{pmatrix}$$

4.

$$a \circ b = (136)(25)$$

$$x = (136524)$$

□