Гаттаров Тимур Б05-304 (15/02/2024)

Задача 1. *Пусть G - группа нечетного порядка. Докажите, что каждый её элемент является квадратом некоторого другого.*

Решение. Так как порядок каждого элемента является делителем порядка группы, то все порядки нечётны. Пусть $e = a^{2p+1}$. Тогда $a = ae = a^{(2p+1)+1} = a^{(p+1)^2}$ □

Задача 2. *Докажите, что элементы abc, bca, cab имеют одинаковый порядок (в случае, если каждый из них имеет конечный порядок).*

Решение. Пусть $(abc)^k = e$

$$(abc)^k = abcabcabc...abcabc = e$$

Домножим справа на c^{-1}:

$$(abc)^k = abcabcabc...abcab = ec^{-1} = c^{-1}e$$

Домножим слева на c:

$$cabcabcabc...abcab = e = (cab)^k$$

Аналогично доказывается для bca до множением на a^{-1} слева и на a справа. □

Задача 3. *Пусть порядок x равен 38. Найдите порядки x^9 и x^6.*

Решение. Порядок $m_1 = x^9$, $m_1 = \frac{38}{\text{НОД(38, 9)}} = 38$. Порядок $m_2 = x^6$, $m_2 = \frac{38}{\text{НОД(38, 6)}} = 19$. □

Задача 4. *Пусть $C_n =< a >$ и НОД $(k, n) = 1$. Докажите, что $\exists b : b^k = a$.*

Решение. Воспользуемся леммой доказанной на семинаре:

> Пусть $< a >= C_n$ и $b = a^k$. Доказать, что элемент b тогда и только тогда будет образующим группы $\langle a \rangle$, когда числа n и k взаимно просты.

Тогда имеем a^k - образующий жлемент. Из определения образующиего элемента получаем: $\exists t : (a^k)^p = a$. Продолжим равенство и явно предъявим b:

$$(a^k)^p = a = a^{kp} = (a^p)^k$$

Получили $\exists p : b^k = (a^p)^k = a$.
□

Задача 5. *Докажите, что любая группа простого порядка циклическая.*

Решение. Так как порядок элемента является делителем порядка группы, то в нашем случае порядок элемента либо 1, либо какое-то простое число p. Тогда если порядок элемента $ord(a) = 1$, то $a = e$, иначе если $ord(a) = p$ (все остальные элементы) $\forall b \exists k \in Z : a^k = b, k = p$ и тогда группа циклическая по определению. □

Задача 6. *Найдите количество элементов в группе* $\mathbb{Z}_{108}^*$.

Решение. Посчитаем значение функции Эйлера $\varphi(108)$:

$$\varphi(108) = \varphi(2^2) \cdot \varphi(3^3) = (2^2 - 2) \cdot (3^3 - 3^2) = 36$$

□

Задача 7. *Пусть* $d \mid n$. *Докажите, что в* C_n *ровно* $\varphi(d)$ *элементов порядка* d. *Используя этот факт докажите, что* $\sum_{d|n} \varphi(d) = n$

Решение. Рассмотрим элемент a^p. Аналогично Задаче 3 $d = ord(a^p) = \frac{n}{\text{НОД}(n,p)}$. Перепишем в удобном в виде:

$$\text{НОД}(n,p) = \frac{n}{d} = k$$

$$\text{НОД}(d, \frac{pd}{n}) = \text{НОД}(d, \frac{p}{k}) = 1$$

Тогда всего чисел $\frac{p}{k} < d$ и взаимно простых с d $\varphi(d)$.

Воспользуемся тем что порядок каждого элемента группы является делителем числа d. Тогда $\sum_{d|n} \varphi(d)$ является суммой колечества элементов по всем порядкам, которая равна количеству элементов группе n. □