CS 235: Algebraic Algorithms, Spring 2021

Discussion 6

Tuesday, March 30th, 2021.

Problem 1. Cosets and Quotient Groups:

(a) Find all cosets of subgroup $\langle 4 \rangle$ of $\mathbb{Z}_{12}$.

(b) Find the index of the quotient group $\mathbb{Z}_{24}/\langle 3 \rangle$. What are its elements?

b) $\langle a \rangle = \{ka,\ k \in \mathbb{Z}\}$ (+ - op) ✓

$\langle a \rangle = \{a^k,\ k \in \mathbb{Z}\}$ ($\cdot$ - op)

$\langle 3 \rangle = \{0, 3, 6, 9, 12, 15, 18, 21\}$

$\Rightarrow \text{index} = \dfrac{|\mathbb{Z}_{24}|}{|\langle 3 \rangle|} = \dfrac{24}{8} = 3$

$\therefore$ # of cosets of $\langle 3 \rangle$ in $\mathbb{Z}_{24} = 3$

$\mathbb{Z}_{24}/\langle 3 \rangle = \{\langle 3 \rangle, 1 + \langle 3 \rangle, 2 + \langle 3 \rangle\}$

a) $\langle 4 \rangle = \{0, 4, 8\}$ in $\mathbb{Z}_{12} = \{0, 1, \ldots, 11\}$

$\langle 4 \rangle = \{0, 4, 8\}$ $\quad 1 + \langle 4 \rangle = \{1, 5, 9\}$

$\langle 4 \rangle + 0$ $\quad 2 + \langle 4 \rangle = \{2, 6, 10\}$

$3 + \langle 4 \rangle = \{3, 7, 11\}$

Problem 2. Group Isomorphism: explain why the following pairs of groups are (or are not) isomorphic.

(a) $\mathbb{Z}_4$ and $\mathbb{Z}$ -> not isomorphic

(b) $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ -> not isomorphic

(c) $\mathbb{Z}_8^*$ and $\mathbb{Z}_{12}^*$ -> isomorphic

fact: $\mathbb{Z}_n$ is cyclic

(a) $\mathbb{Z}_4$ -> has order 4

$\mathbb{Z}$ -> has order ∞

(b) $\mathbb{Z}_2 = \{0,1\}$ -> $\mathbb{Z}_2 \times \mathbb{Z}_2 = \{0,1\} \times \{0,1\}$

$= \{(0,0), (0,1), (1,0), (1,1)\}$

=> order $= 4 =$ ord $(\mathbb{Z}_4)$

Check order of elements

$\mathbb{Z}_4$: ord $(0) = 1$ => $\mathbb{Z}_4$ is cyclic

ord $(1) = 4$ -> $\langle 1 \rangle = \{0,1,2,3\}$

ord $(2) = 2$ -> $\langle 2 \rangle = \{0,2\}$

ord $(3) = 4$ -> $\langle 3 \rangle = \{0,3,2,1\}$

$\mathbb{Z}_2 \times \mathbb{Z}_2$ is not cyclic

$\mathbb{Z}_2$: ord $(0) = 1$ => ord $(0,0) = \text{lcm}(1,1) = 1$

ord $(1) = 2$ ord $(0,1) = \text{lcm}(1,2) = 2$

ord $(1,0) = \text{lcm}(2,1) = 2$

ord $(1,1) = \text{lcm}(2,2) = 2$

(for $\mathbb{Z}_2 \times \mathbb{Z}_2$)

Problem 3. Exponent of a Group: find the exponent of the following groups.

(a) $\mathbb{Z}_{35}$ and $\mathbb{Z}_{15} \times \mathbb{Z}_{35}$

(b) $\mathbb{Z}_{15}^*$ and $\mathbb{Z}_{600}^*$.

(a) $\exp(\mathbb{Z}_n) = n$

$\therefore \mathbb{Z}_n$ is cyclic $\therefore$ ord = exp

$\Rightarrow \exp(\mathbb{Z}_{35}) = 35$

$\exp(\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}) = \operatorname{lcm}(n_1, n_2)$

$\exp(\mathbb{Z}_{15} \times \mathbb{Z}_{35}) = \operatorname{lcm}(15, 35)$

$= 105$

(b) $a^{m} \equiv 1 \pmod{n}$ in $\mathbb{Z}_n^*$

Carmichael function: $(n = p^e)$

$$m = \begin{cases} \varphi(p^e)^{1/2}, & p^e = \{8, 16, 32, \dots\} \\ \varphi(p^e) & \text{otherwise} \end{cases}$$

$\mathbb{Z}_{15}^* = \mathbb{Z}_3^* \times \mathbb{Z}_5^*$ $(15 = 3 \cdot 5)$

$= \operatorname{lcm}(\varphi(3), \varphi(5)) = \operatorname{lcm}(2, 4)$

$= 4$

$\mathbb{Z}_{600}^* = \mathbb{Z}_8^* \times \mathbb{Z}_3^* \times \mathbb{Z}_{25}^* \Rightarrow \exp = 20$