Subgroups

Monday, March 2, 2026 9:17 PM

Recall: Groups

Subgroups

12] Exer. $(\mathbb{Z}_{10}, +)$. Find a subgroup of size

① 5

$H = \{0, 2, 4, 6, 8\}$

② 4

$H = \{0, 1, 9, \ldots ?\}$

③ 2

$H = \{0, 5\}$

④ 1

$H = \{0\}$

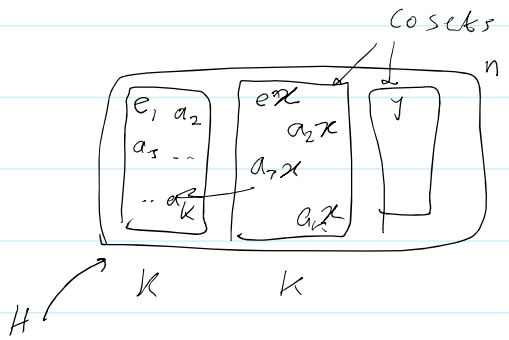
⑤ 3

$H = \{0, 4, \ldots ?\}$

13] Thrm: (Lagrange Theorem)

if H is a subgroup of a finite group G, then $|H|$ divides $|G|$

Proof: idea



14] Prop. Let H be a subgroup of G, then

① $\forall a, b \in H$, $ab \in H$

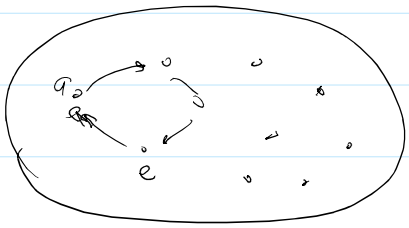
② $e \in H$

③ $\forall a \in H,\ a^{-1} \in H$

15] Prop - Let G be a finite group of order n. For all $a \in G$

① $\text{ord}(a) \mid n$

② $a^n = e$



16] Def^n. (Euler's phi function)

The totient of $n > 0$, denoted by $\phi(n)$ or $\varphi(n)$, is

$$\varphi(n) = \{ |\mathbb{Z}_n^*| \}, \text{ where } \mathbb{Z}_n^* = \{ x \mid 0 \le x < n, \gcd(x, n) = 1 \}$$

e.g. $\varphi(7) = 6$ $\quad \mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

$\varphi(6) = 2$ $\quad \mathbb{Z}_6^* = \{1, 5\}$

$\varphi(2) = 1$ $\quad \mathbb{Z}_2^* = \{1\}$

$\varphi(1) = 1$ $\quad \mathbb{Z}_1^* = \{0\}$ $\quad \gcd(0, 1) =$

17] Algorithm $\phi(n)$

1. $\phi(1) = 1$
2. if $n = p^e$ (power of prime), $\phi(n) = (p-1)\, p^{e-1}$
3. if $\gcd(m, n) = 1$, $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$

18] e.g. $\phi(8) = \phi(2^3) = (2-1) \cdot 2^2 = 4$ $\quad \varphi$

$\phi(25) = (5-1)\, 5^1 = 20$ $\quad \varphi\ \varphi$

$\phi(35) = \phi(7) \cdot \phi(5) = 6 \times 4 = 24$ $\quad \varphi$

$\phi(105) = \varphi(35)\, \varphi(3) = 24 \cdot 2 = 48$

$\varphi(100) = \varphi(2^2)\, \varphi(5^2) = (2-1) \cdot 2 \cdot (5-1) \cdot 5 = 40$

19] Thm. (Euler's theorem)

In $\mathbb{Z}_m^*$, the order of the group $\phi(m)$,

$\forall a \in \mathbb{Z}_m^*$, we have $a^{\phi(m)} = 1$. Hence:

> if $k \equiv j \pmod{\phi(m)}$, then $a^k \equiv a^j \pmod{m}$

20] e.g. ① in $\mathbb{Z}_5^*$

$2^{46} \xrightarrow{\bmod \phi(5)} \equiv 2^2 \equiv 4 \pmod 5$

21] e.g.

① $26^{50} \pmod{15}$ (mod $\phi(15) = 8$)

$\equiv 11^2$

$\equiv (-4)^2 \equiv 1 \pmod{15}$

$\phi(15) = (5-1)(3-1) = 8$

② $463^{91} \pmod{15}$

$\equiv 13^3 \equiv (-2)^3 \equiv -8 \equiv 7 \pmod{15}$

③ $15^{1234500} \cdot 14^{1234520} \pmod{19}$

$\equiv (-5)^2 \equiv --$

Hint

$(-4)(-5) \equiv 1$

$20 \equiv 1$

Quiz Material:

ch: 3, 5, 6, 7, 8 (Forouzan)

AES

see the slides

Perfect secrey (BR 1.4 + 2.2)

Affine cipher

Modular Arithmetic	P02-Modular Arithmetic.pptx
Number Theory	P03-Symmetric-key Encryption.pptx
Linear Congruences	P04-Block Cipher and DES.pptx
Fermat Little Theorem	
Perfect Secrecy	
Pseudoprimes	