

Recall: Group order $|G|$
 Element order $\text{ord}(a)$

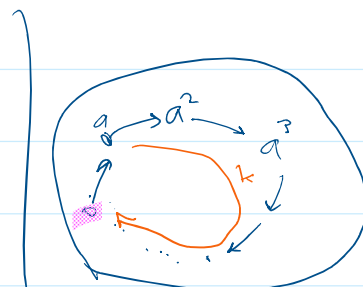
Online

+B#507

1] Prop. let $a \in G$, $|G| = n$

① $\text{ord}(a) \mid n$

② $a^n = e$



$a^k = e$

$k \mid n \Rightarrow n = c \cdot k$

$(a^k)^c = e$

$k = \text{ord}(a)$

2] Defⁿ. (the Euler Phi function)

The totient of a positive integer n , denoted by $\phi(n)$, is the number of nonnegative integers $< n$ and coprime to n .

i.e. $\phi(n) = |\mathbb{Z}_n^*|$ where $\mathbb{Z}_n^* = \{x \mid 0 \leq x < n \text{ and } \gcd(x, n) = 1\}$

e.g. $\phi(5) = |\mathbb{Z}_5^*| = |\{1, 2, 3, 4\}| = 4$

$\mathbb{Z}_2^* = \{1\} \Rightarrow |\mathbb{Z}_2^*| = 1 \Rightarrow \phi(2) = 1$

$\mathbb{Z}_1^* = \{0\} \Rightarrow |\mathbb{Z}_1^*| = 1 \Rightarrow \phi(1) = 1$

3] Alg. $\phi(n)$

① $\phi(1) = 1$

② if n is prime or prime power, $\phi(p^a) = (p-1)p^{a-1}$

③ if $\gcd(n, m) = 1$, $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$

$5^3 = 125$

$0, \dots, 124$

$125/5 = 5^2$

$125 - 25 = 100$

4] e.g.

$\phi(17) = 16$

$\phi(49) = \phi(7^2) = 6 \cdot 7 = 42$

$\phi(16) = \phi(2^4) = 1 \cdot 2^3 = 8$

$$\phi(105) = \phi(3) \phi(35) = \phi(3) (\phi(5) \phi(7)) = 2 \cdot 4 \cdot 6 = 48$$

$$\mathbb{Z}_{105}^* = 48$$

$$\phi(200) = \phi(2^3 \cdot 5^2) = 1 \cdot 2^2 \cdot 4 \cdot 5^1 = 80 \quad \text{+B\#507}$$

5] Thrm (Euler's Theorem)

$$\text{In } \mathbb{Z}_m^*, \quad |\mathbb{Z}_m^*| = \phi(m) \Rightarrow \forall a \in \mathbb{Z}_m^*, \quad a^{\phi(m)} = 1$$

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

6] e.g.

$$2^{46} \pmod{5} \Rightarrow \phi(5) = 4$$

$$\equiv 2^{44} \cdot 2^2 \equiv (2^4)^{11} \cdot 2^2 \equiv 1^{11} \cdot 2^2 \equiv 4 \pmod{5}$$

7] e.g.

$$14^{52} \pmod{11}$$

$$\phi(11) = 10$$

$$\begin{array}{c} \text{mod } 10 \\ \downarrow \end{array} \quad \begin{array}{c} \text{mod } 11 \\ \downarrow \end{array} \quad 3^2 \equiv 9 \pmod{11}$$

e.g.

$$463^{91} \pmod{15}$$

$$\Rightarrow \phi(15) = 2 \cdot 4 = 8$$

$$\begin{array}{c} \text{mod } 15 \\ \downarrow \end{array} \quad \begin{array}{c} \text{mod } 8 \\ \downarrow \end{array}$$

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

8] Defⁿ. Let G be a group, and $H \subseteq G$. Then H is called a subgroup of G if H is a group under the operation induced by G .

e.g. $\mathbb{Z}_{10} = \{0, 1, \dots, 9\}$

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

$$H_1 = \{0\}$$

$$H_2 = \{0, 5\}$$

$$H_3 = \{0, -, -\}^{\times}, \quad H_4 = \{0, ---\}^{\times}$$

9] Thm (Lagrange Theorem)

if H is a subgroup of G , then

$|H|$ divides $|G|$

10] Prop let G be a group with identity e

and H be a subgroup of G . then

① $\forall a, b \in H, ab \in H$

② $e \in H$

③ $\forall a \in H, a^{-1} \in H$.