

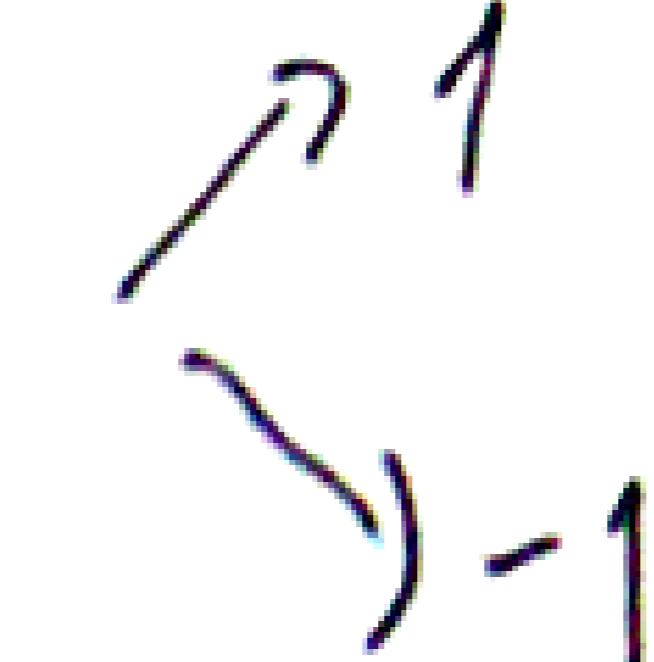
$n \rightarrow a \in \{1, \dots, n-1\}$

$$a^{\frac{n-1}{2}} \bmod n$$

1

-1

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n$$


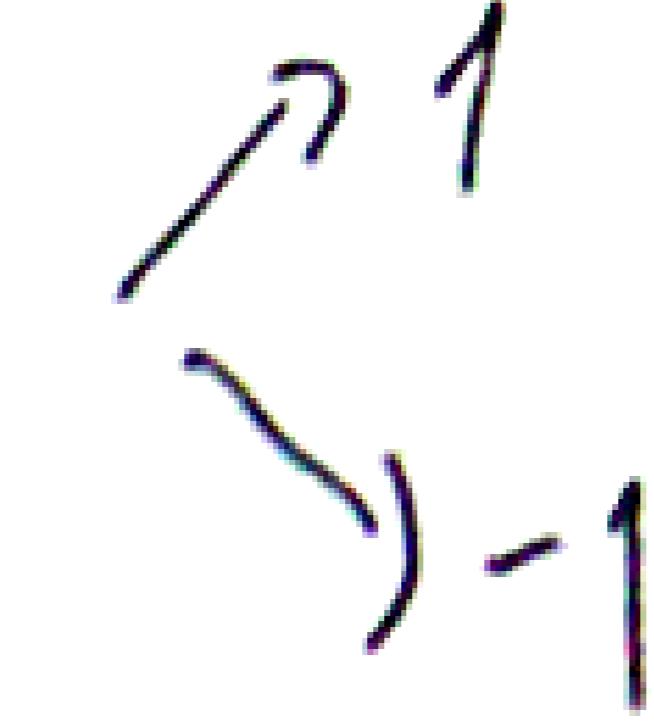
$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|\mathcal{S}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n$$


$$36 = 2^2 \cdot 3^2$$

$$a \in \mathbb{Z}_n^*$$

$$Q^{\frac{n-1}{2}} \bmod n = -1$$

$$|\mathcal{S}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(\mathcal{S}_n, \cdot)$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$S_n = S_n^+ \cup S_n^- \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$a^{\frac{n-1}{2}} \bmod n = 1$$

$$a \in \mathbb{Z}_n^*$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(S_n, \cdot)$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$S_n = S_n^+ \cup S_n^- \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \pmod{n} = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot)$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad (a \cdot b)^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad \Rightarrow a^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \pmod{n}$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$S_n = S_n^+ \cup S_n^- \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$a^{\frac{n-1}{2}} \bmod n = 1$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot)$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$(a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$= a^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} 1 \\ -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad (a \cdot b \equiv 1 \bmod n)$$

p.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot)$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$(a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad = a^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} 1 \\ -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

p.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot)$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$(a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \equiv a^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} 1 \\ -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

u.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$a \cdot b \in S_n$$

$$(a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$= a^{\frac{n-1}{2}} \bmod n$$

$$= b^{\frac{n-1}{2}} \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

u.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad (a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \Rightarrow a^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

u.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$$

$$a \in \mathbb{Z}_n^*$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad (a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \Rightarrow a^{\frac{n-1}{2}} \bmod n$$

$b^{\frac{n-1}{2}} \bmod n$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} \nearrow 1 \\ \searrow -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

u.d. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$\rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad (a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \begin{aligned} &\equiv a^{\frac{n-1}{2}} \bmod n \\ &\quad b^{\frac{n-1}{2}} \bmod n \end{aligned}$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} 1 \\ -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

z.B. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad (a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \equiv a^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$n \rightarrow a \in \{1, \dots, n-1\}$$

$$a^{\frac{n-1}{2}} \bmod n \begin{cases} 1 \\ -1 \end{cases}$$

$$36 = 2^2 \cdot 3^2$$

$$a \in S_n \rightarrow a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n$$

$$\exists b \quad a \cdot b \equiv 1 \bmod n$$

z.B. $b \in S_n \quad b^{\frac{n-1}{2}} \bmod n$

$\Rightarrow a^{\frac{n-1}{2}} \cdot b^{\frac{n-1}{2}} \equiv 1 \bmod n$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \bmod n = -1$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{|S_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathbb{Z}_n^*, \cdot)$$

$$(S_n, \cdot) \Rightarrow |S_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in S_n$$

$$a \cdot b \in S_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad (a \cdot b)^{\frac{n-1}{2}} \bmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \bmod n \quad \Rightarrow a^{\frac{n-1}{2}} \bmod n$$

$b^{\frac{n-1}{2}} \bmod n$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod m$$

$$c \equiv b \pmod n$$

$$n \cdot d \equiv 1 \pmod m$$

$$m \cdot B \equiv 1 \pmod n$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \pmod n = -1$$

$$|\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathcal{S}_n, \cdot) \Rightarrow |\mathcal{S}_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in \mathcal{S}_n \quad a \cdot b \in \mathcal{S}_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod n \quad (a \cdot b)^{\frac{n-1}{2}} \pmod n$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod n \quad \begin{aligned} &\equiv a^{\frac{n-1}{2}} \pmod n \\ &\equiv b^{\frac{n-1}{2}} \pmod n \end{aligned}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \pmod{n} = -1$$

$$|\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathcal{S}_n, \cdot) \Rightarrow |\mathcal{S}_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in \mathcal{S}_n$$

$$a \cdot b \in \mathcal{S}_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$$

$$(a \cdot b)^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad \Rightarrow a^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \pmod{n}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \pmod{n} = -1$$

$$|\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathcal{S}_n, \cdot) \Rightarrow |\mathcal{S}_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in \mathcal{S}_n$$

$$a \cdot b \in \mathcal{S}_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad (a \cdot b)^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad \begin{cases} a^{\frac{n-1}{2}} \pmod{n} \\ b^{\frac{n-1}{2}} \pmod{n} \end{cases}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \pmod{n} = -1$$

$$|\mathbb{Z}_n^*|$$

$$\frac{|\mathcal{S}_n|}{|\mathbb{Z}_n^*|} \leq 1$$

$$(\mathcal{S}_n, \cdot) \Rightarrow |\mathcal{S}_n| \mid |\mathbb{Z}_n^*|$$

$$a, b \in \mathcal{S}_n \quad a \cdot b \in \mathcal{S}_n$$

$$a^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad (a \cdot b)^{\frac{n-1}{2}} \pmod{n}$$

$$b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n} \quad \begin{cases} a^{\frac{n-1}{2}} \pmod{n} \\ b^{\frac{n-1}{2}} \pmod{n} \end{cases}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$c \equiv a \pmod{n_1}$$

$$c \equiv 1 \pmod{n_2}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$c \equiv a \pmod{n_1}$$

$$c \equiv 1 \pmod{n_2}$$

$$c \stackrel{n=1}{\equiv}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{*} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{x} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$MCP(m, n) = 1$$

$$C \equiv a \bmod m$$

$$c \equiv b \pmod{y}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$C = a \cdot n \cdot \alpha + b \cdot m \cdot \beta$$

6.2 mod m

C a b mud m

$$a \in \mathbb{Z}_n^*$$

$$\frac{n-1}{2} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

CEAN & CASH

$$0 \leq a \leq n_1$$

$$D \in \mathbb{Z} \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

net
C 111
mud m

debt was in

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

?

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2 \quad c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

$$(k \cdot n_1) \cdot n_1 \equiv d \cdot \beta \pmod{n_1}$$

$$n_1/d \cdot \beta$$

$$d \equiv \beta \pmod{n}$$

$\pmod{n_1}$

$$n_1 \mid d - \beta$$

$$k \cdot n \equiv d - \beta$$

$$k \cdot n_1 \cdot n_2 \equiv d - \beta$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$\Rightarrow d$

? β

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2 \quad c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

$$(k \cdot n_1) \cdot n_1 = d \cdot \beta \quad \begin{array}{l} k \cdot n \equiv d \cdot \beta \\ n_1/d \cdot \beta \end{array}$$

$$\begin{array}{l} d \equiv \beta \pmod{n} \\ \downarrow \\ d \equiv \beta \pmod{n_1} \\ n \mid d - \beta \end{array}$$

$$k \cdot n \equiv d - \beta$$

$$k \cdot n_1 \cdot n_2 \equiv d - \beta$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2 \quad c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n_2}$$

$$(k \cdot n_1 \cdot n_2 \cdot d \cdot \beta) \pmod{n}$$

$$n_1/d \cdot \beta$$

$$k \cdot n \equiv d \pmod{n}$$

$$k \cdot n_1 \cdot n_2 \equiv d \pmod{n}$$

$$\begin{aligned} d &\equiv \beta \pmod{n} \\ d &\equiv \beta \pmod{n_1} \\ d &\equiv \beta \pmod{n_2} \end{aligned}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2 \quad c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv b \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n_2}$$

$$(k \cdot n_1) \cdot n_2 = d \cdot \beta \quad k \cdot n = d \cdot \beta$$

$$\therefore n_1/d = \beta$$

$$\begin{cases} d \equiv \beta \pmod{n} \\ d \equiv \beta \pmod{n_2} \\ n \nmid d - \beta \end{cases}$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

so

$$a \in \mathbb{Z}_n^* \quad a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2 \quad c \in \mathbb{Z}_n^*, c \notin \mathbb{Z}_{n_1}$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n_1-1}{2}} \equiv -1 \pmod{n_1}$$

α^{-1}

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot B$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

$\Rightarrow a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$\times \quad c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

+ α^{*1}

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

- $\alpha^{(1)}$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$\times \quad c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$\alpha \neq 1$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$\text{X} \quad c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

- α^{-1}

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot B$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

- ok

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n_1}$$

$$\alpha = 12^\circ$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$225 = 15^2$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$1 \pmod{n_1}$$

- 12 * 12

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$\begin{aligned} 225 &= 15^2 \\ &= 3^2 \cdot 5^2 \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n_1-1}{2}} \equiv 1 \pmod{n_1}$$

$\alpha \rightarrow 0$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot B$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$d = 1$$

$$B = 1$$

$$225 = 15^2 \\ = 3^2 \cdot 5^2$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$\times$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

$$\rightarrow a = b$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$\begin{aligned} 225 &= 15^2 \\ &= 3^2 \cdot 5^2 \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad X$$

$$X \quad c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

• $\alpha \rightarrow 0$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$a \neq b$$

$$d \neq \beta$$

$$n \neq m$$

$$225 = 15^2 \\ = 3^2 \cdot 5^2$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad X$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$\alpha > 0$$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$c = a \cdot n \cdot d + b \cdot m \cdot \beta$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$\alpha \neq 0$

$\beta \neq 0$

$\alpha, \beta \in \mathbb{Z}_n^*$

$\alpha, \beta \in \mathbb{Z}_n^*$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad X$$

$$X \quad c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$\Rightarrow \alpha^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$

$$\text{MCD}(m, n) = 1 \quad a, b$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \beta \equiv 1 \pmod{n}$$

$$225 = 15^2 \\ = 3^2 \cdot 5^2$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\left(\frac{n}{\ln n}\right)} \approx 1$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$



$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n_1-1}{2}} \equiv 1 \pmod{n_1}$$

- ok \times

$$\text{MCD}(m, n) = 1$$

a, b

$$N_1 = P \cdot Q$$

$$N_2 = P \cdot R$$

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{aligned} 225 &= 15^2 \\ &= 3^2 \cdot 5^2 \\ &\quad \square_{n_1} \quad \square_{n_2} \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

X

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{p_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{p_1}$$

$\rightarrow \alpha \sim D$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$\begin{array}{c} \cancel{N_1 \neq P \cdot Q} \\ N_2 \neq P \cdot R \end{array}$$

$$\begin{aligned} 225 &= 15^2 \\ &= 3^2 \cdot 5^2 \\ &\quad \boxed{n_1} \quad \boxed{n_2} \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1 \quad \text{MCD}(N_1, N_2) = P$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{P}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{P}$$

$$\alpha^{-1}$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{array}{l} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$\begin{aligned} 225 &= 15^2 \\ &= 3^2 \cdot 5^2 \\ &\quad \boxed{n_1} \quad \boxed{n_2} \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1 \quad \text{MCD}(N_1, N_2) = P$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$\rightarrow \alpha^{-1}$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$\begin{array}{l} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$\begin{aligned} 22S &= 1S^2 \\ &= 3^2 \cdot S^2 \\ &\quad \boxed{n_1} \quad \boxed{n_2} \end{aligned}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1 \quad \text{MCD}(N_1, N_2) = P$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{N_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{N_1}$$

$$\alpha^{-1}$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

* α^{*17}

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n_1-1}{2}} \equiv 1 \pmod{n_1}$$

α^{k+1}

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{array}{l} \textcircled{1} \quad c \equiv a \pmod{n_1} \\ \textcircled{2} \quad c \equiv 1 \pmod{n_2} \end{array}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$\alpha \neq 0$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1 \quad \text{MCD}(N_1, N_2) = P$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{N_1}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N_1}$$

• $\alpha^{*}(t)$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{N} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$\alpha \sim \beta$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n} \quad \times$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$d \sim \Omega$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot b \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$n = a^b$$

$$n = 2^b$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\frac{1}{\ln n}$$

\dots

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n}$$

$$\alpha = 0$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1} \quad \times$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot b \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$\therefore N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad \because n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$n = 2^b$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1 \quad \text{MCD}(N_1, N_2) = P$$

$$\frac{1}{\ln n}$$

$$c^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c^{\frac{n-1}{2}} \equiv 1 \pmod{n} \rightarrow c^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$a^{\frac{n-1}{2}} \equiv 1 \pmod{n_1}$$

$$\alpha = 1$$

$$b = \log_2 n$$

$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \cdot B \equiv 1 \pmod{n}$$

$$\begin{array}{c} N_1 = P \cdot Q \\ N_2 = P \cdot R \end{array}$$

$$N_1 = P \cdot Q$$

$$N_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

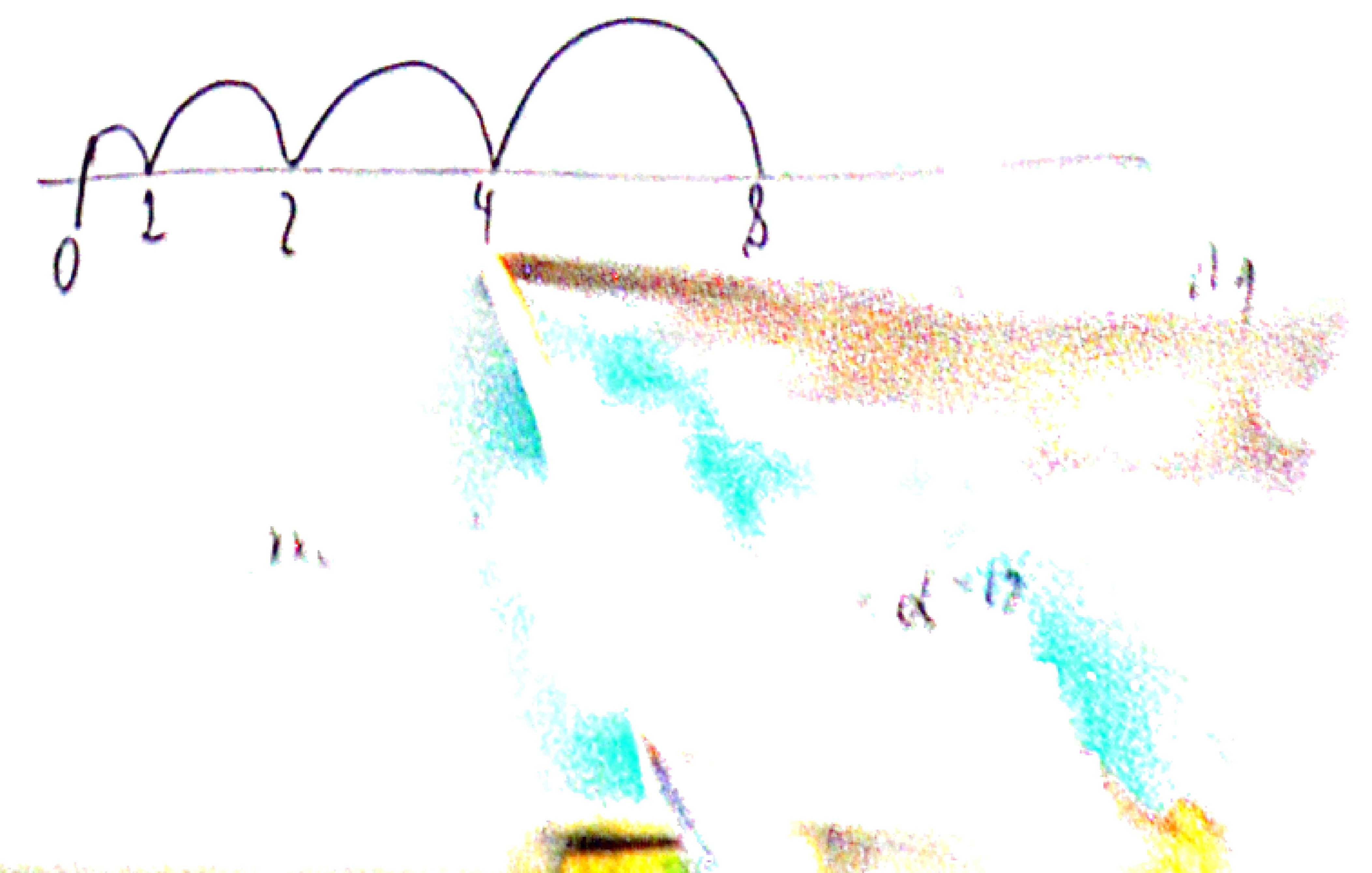
$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$n = a^b$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

$$\frac{1}{\ln n}$$



$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} \text{N}_1 = P \cdot Q \\ \text{N}_2 = P \cdot R \end{array}$$

$$\text{N}_1 = P \cdot Q$$

$$\text{N}_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

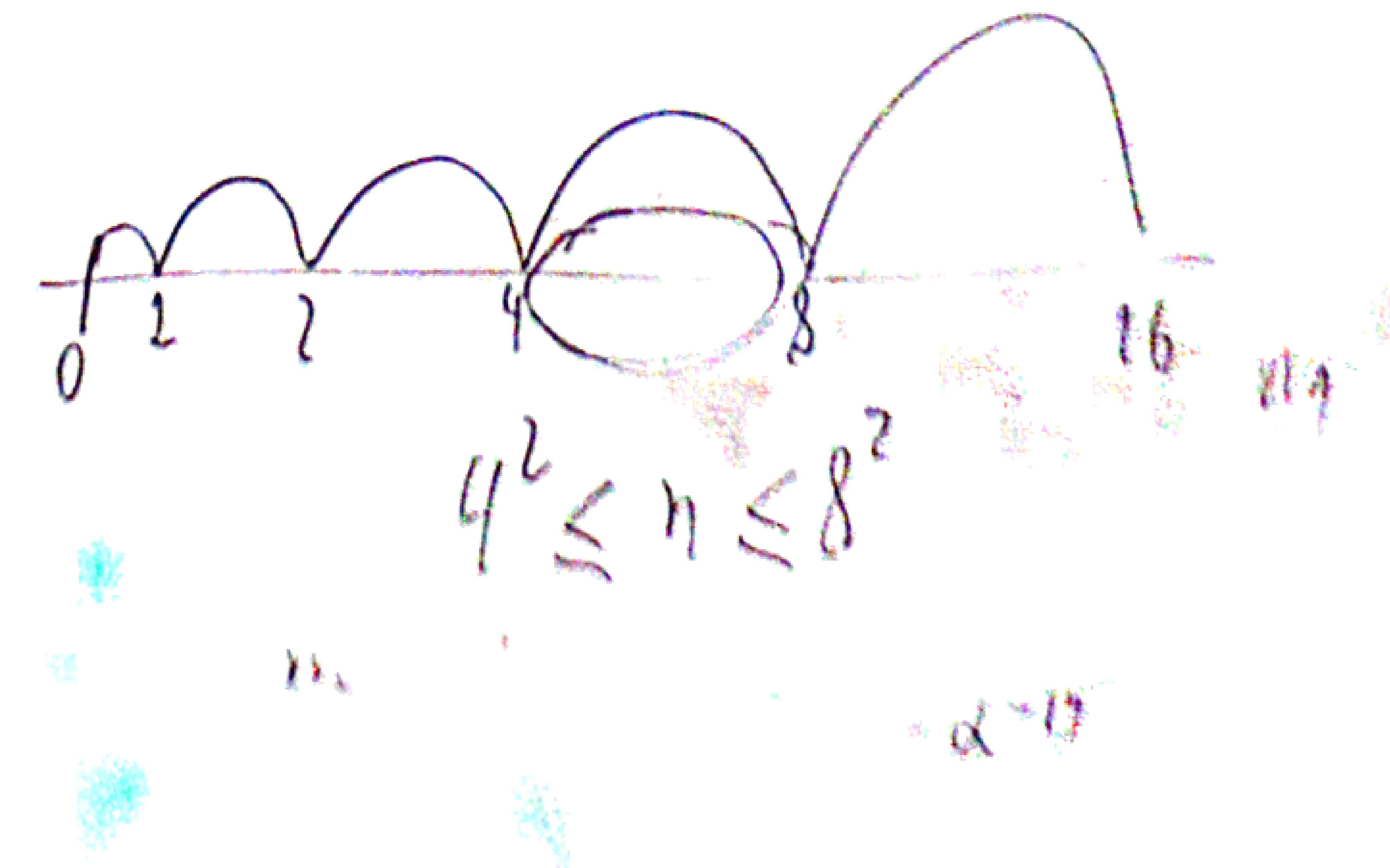
$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{aligned} \textcircled{1} & \quad c \equiv a \pmod{n_1} & n = a^b \\ \textcircled{2} & \quad c \equiv 1 \pmod{n_2} & , \end{aligned}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$$



$$\text{MCD}(m, n) = 1$$

a, b

$$c \equiv a \pmod{m}$$

$$c \equiv b \pmod{n}$$

$$n \cdot d \equiv 1 \pmod{m}$$

$$m \beta \equiv 1 \pmod{n}$$

$$\begin{array}{c} \text{N}_1 = P \cdot Q \\ \text{N}_2 = P \cdot R \end{array}$$

$$\text{N}_1 = P \cdot Q$$

$$\text{N}_1 = P \cdot Q$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

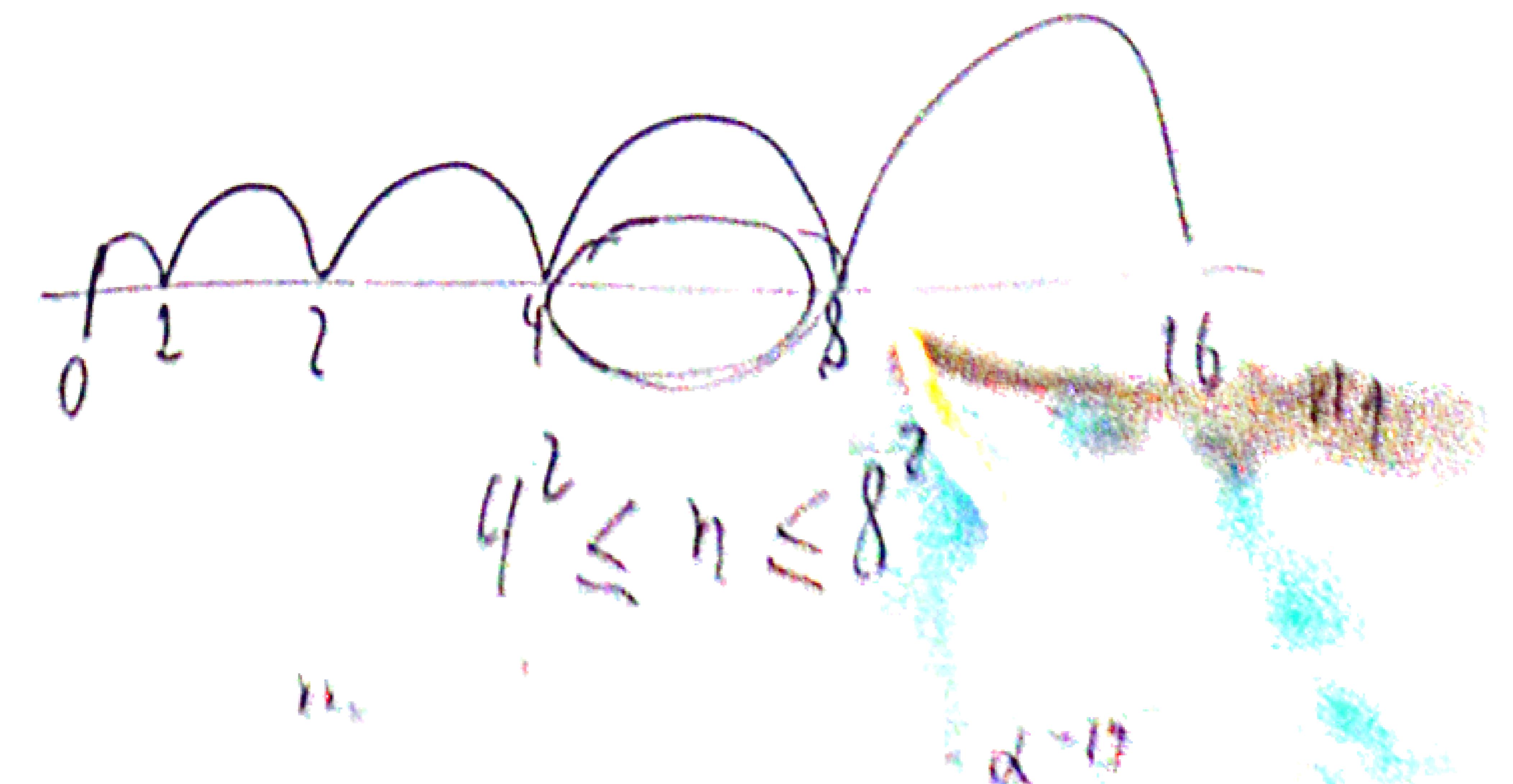
$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{aligned} \textcircled{1} & \quad c \equiv a \pmod{n_1} & n = a^b \\ \textcircled{2} & \quad c \equiv 1 \pmod{n_2} & , \end{aligned}$$

$\pi(n)$: número de primos hasta n

$$\lim_{n \rightarrow \infty} \frac{\pi(n)}{\ln n} = 1$$

$$\frac{1}{\ln n}$$



$$4^2 \leq n \leq 8^2$$

$$\alpha = 17$$

n is prime

if $\text{neg} = 0$ then return COMP

$$a \in \mathbb{Z}_n^*$$

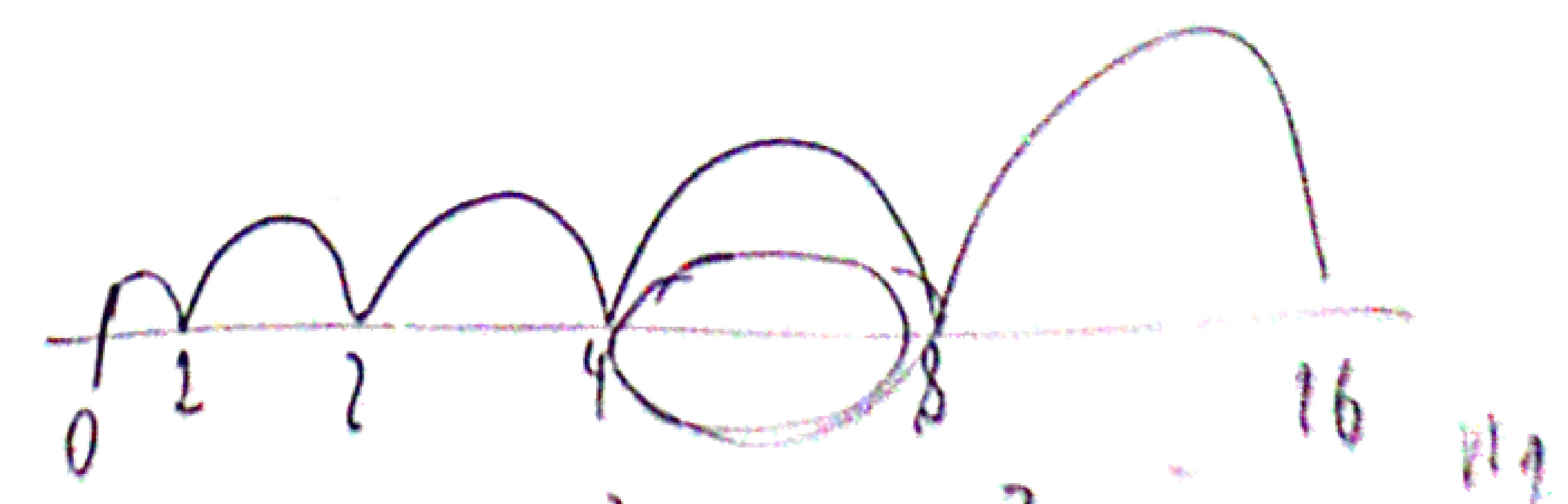
$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$



$$4^2 \leq n \leq 8^2$$

$$O(n^2)$$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, \dots, b_k



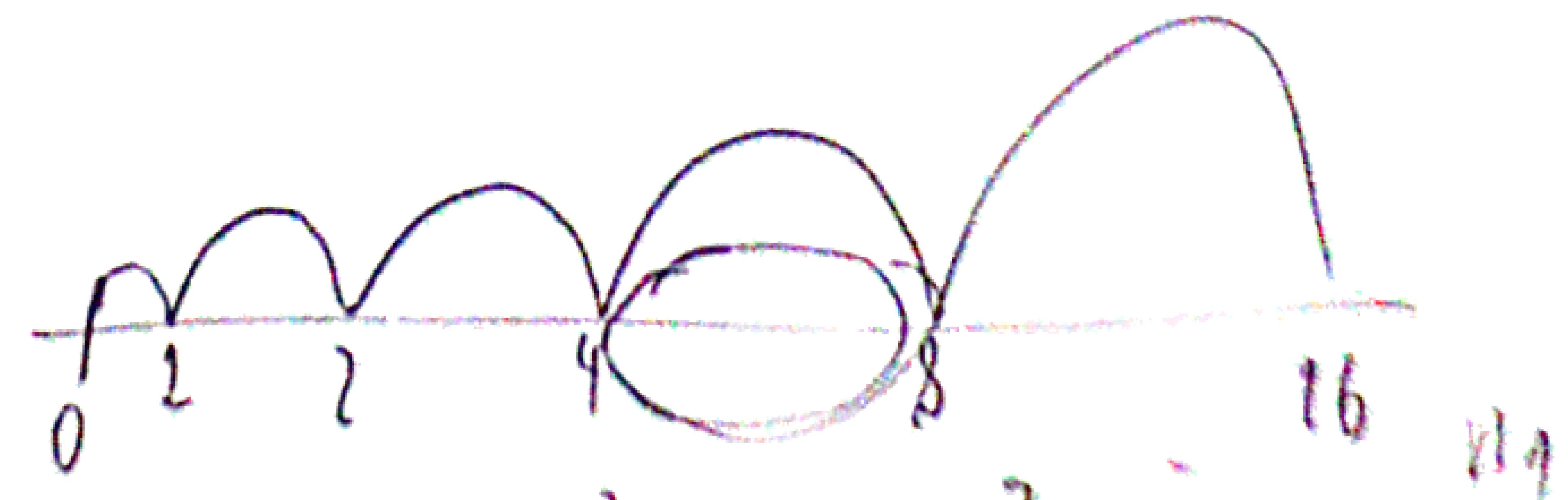
$$a \in \mathbb{Z}_n^*$$

$$\alpha^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

- (1) $c \equiv a \pmod{n_1} \quad n = a^b$
- (2) $c \equiv 1 \pmod{n_2}$



$$4^2 \leq n \leq 8^2$$

n

$\alpha^{\frac{n-1}{2}}$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

- (1) $c \equiv a \pmod{n_1} \quad n = a^b$
- (2) $c \equiv 1 \pmod{n_2}$



$$4^2 \leq n \leq 8^2$$

$O(n^2)$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, \dots, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$



$$4^2 \leq n \leq 8^2$$

$$d = 12$$

n es primo

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

n es compuesto

$$a \in \mathbb{Z}_n^*$$

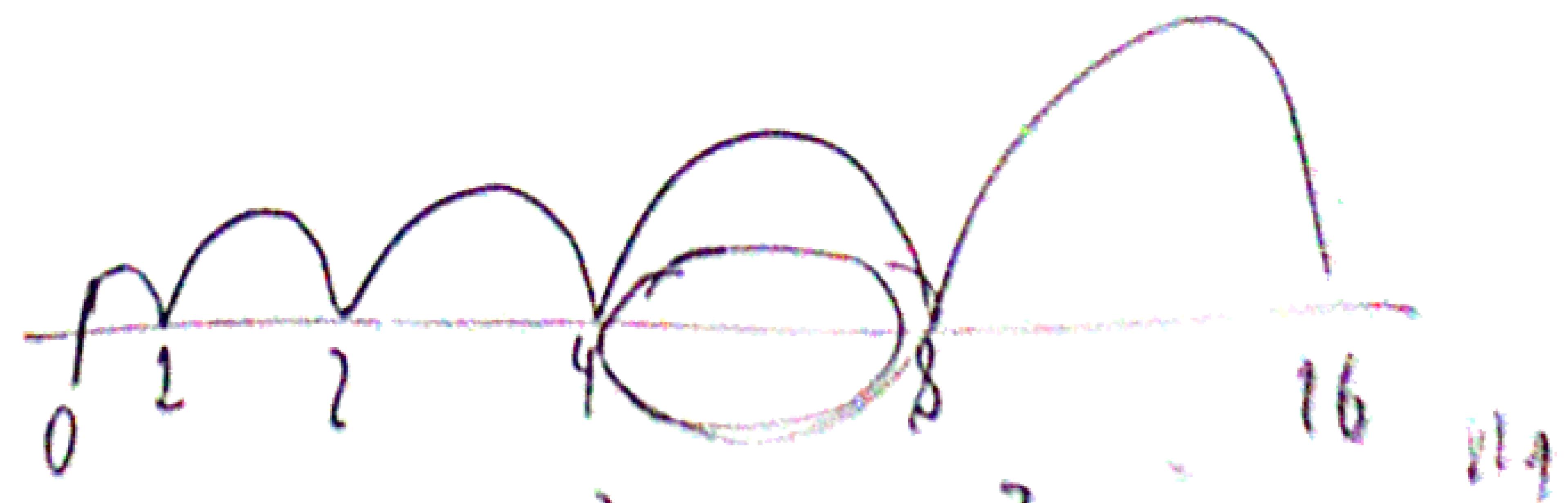
$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad \because n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$



$$4^2 \leq n \leq 8^2$$

$$d \sim 17$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁) →, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 \leq n \leq 8^2$$

m

$$\alpha^{17}$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁) \dots, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad \because n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 < n < 8^2$$

n

$$O(n^2)$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$n = n_1 \cdot n_2$$

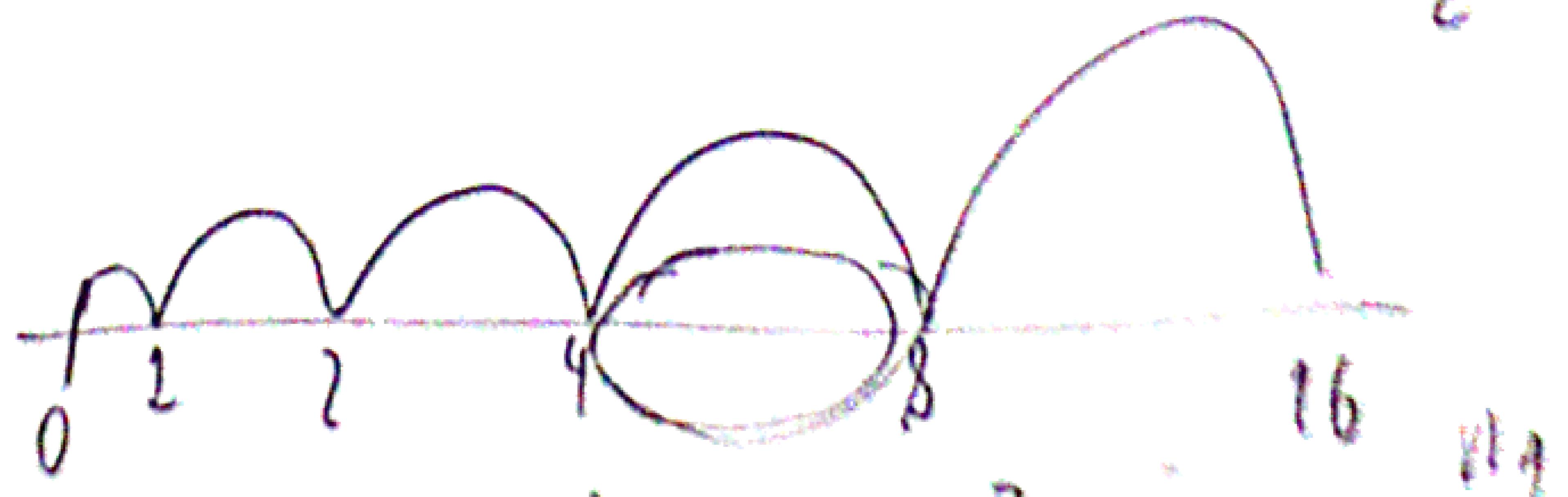
$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 \leq n \leq 8^2$$

$$\alpha^{12}$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 \leq n \leq 8^2$$

m

$$\alpha = \pi$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁) \dots, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

$$\Pr(A \cap B) \leq \Pr(A)$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

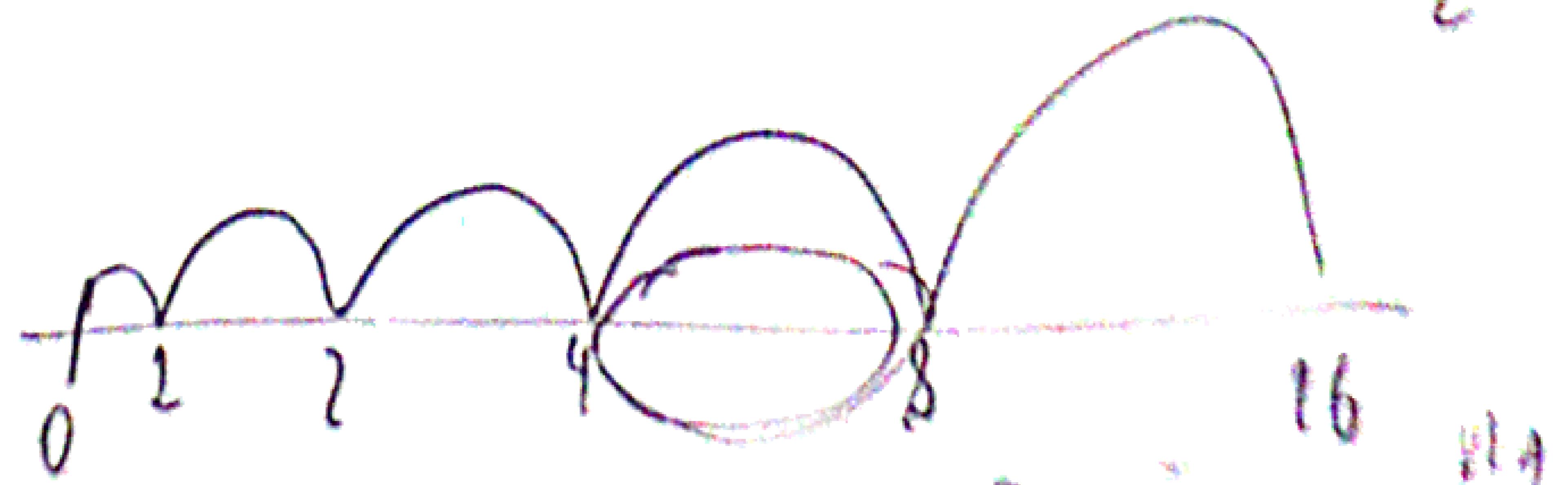
$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 \leq n \leq 8^2$$

$$\alpha^{*D}$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁)—, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k$$

$$\Pr(A \cap B) \leq \Pr(A)$$

$$\Pr(A_1 \cap A_2)$$

$$= \Pr(A_1) \cdot \Pr(A_2)$$

n is composite

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$n = a^b$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$



$$4^2 \leq n \leq 8^2$$

m

$$\approx O^2$$

n es primo

if $\text{neg} = 0$ then return COMP

(b₁)—, b_k

$$\hookrightarrow \left(\frac{1}{2}\right)^k \Pr(A \cap B) \leq \Pr(A)$$

$$\Pr(A_1 \cap A_2)$$

n es compuesto

$$= \Pr(A_1) \cdot \Pr(A_2)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\Pr(A \cap B) = \Pr(A|B) \cdot \Pr(B)$$

19

$\sim O(n^3)$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{\text{1). Pr}(A)} \cdot \Pr(MCD(q_{i,n})=1)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\text{① } c \equiv a \pmod{n_1} \quad \because n = a^b$$

$$\text{② } c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\text{③). Pr}(B)$$

$$= \alpha^{-D}$$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{= \frac{|S_n|}{12}} \cdot \Pr(MCD(q_{i,n})=1)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1}$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$n = a^b$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\textcircled{3} \cdot \Pr(B)$$



19

$$= \alpha^{-1} \beta$$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{=} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$a \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{cases} \textcircled{1} & c \equiv a \pmod{n_1} \\ \textcircled{2} & c \equiv 1 \pmod{n_2} \end{cases} \quad n = a^b$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\textcircled{3}) \cdot \Pr(B)$$

14

$\rightarrow O(n^3)$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\textcircled{3}) \cdot \Pr(B)$$

19

$\propto \alpha^{-k}$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \wedge (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{=} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\textcircled{3} \cdot \Pr(B)$$

19

α^{k+1}

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{=} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\textcircled{3} \cdot \Pr(B)$$

14

$\alpha \rightarrow 0$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \wedge (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{=} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{cases} \textcircled{1} & c \equiv a \pmod{n_1} \\ \textcircled{2} & c \equiv 1 \pmod{n_2} \end{cases} \quad n = a^b$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\textcircled{3}) \cdot \Pr(B)$$

19

$\alpha = 17$

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n})}_{\text{1). } \Pr(A)} \cdot MCD(q_{i,n}) = 1 \cdot \Pr(MCD(q_{i,n}) = 1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot () \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\textcircled{3}. \Pr(B)$$

19

α^{*D}

n is prime

if $\text{neg} = 0$ then return COMP

b_1, b_k

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a \in \mathbb{Z}_n^*$$

$$n = n_1 \cdot n_2$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$c \in \mathbb{Z}_n^*, c \notin S_n$$

$$\textcircled{1} \quad c \equiv a \pmod{n_1} \quad n = a^b$$

$$\textcircled{2} \quad c \equiv 1 \pmod{n_2}$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\textcircled{3}) \cdot \Pr(B)$$

19

$\alpha = 10$

n is prime

if $\text{neg} = 0$ then return COMP

(b₁, ..., b_k)

$$\Pr(MCD(q_{i,n})=1 \mid (b_i \equiv \pm 1 \pmod{n}))$$

$$= \underbrace{\Pr(b_i \equiv \pm 1 \pmod{n} \mid MCD(q_{i,n})=1)}_{=} \cdot \Pr(MCD(q_{i,n})=1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot \left(\right) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \left(\frac{1}{2} \right)$$

$$a^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

$$a \in \mathbb{Z}_n^*, c \notin S_n$$

$$\begin{cases} \textcircled{1} & c \equiv a \pmod{n_1} \\ \textcircled{2} & c \equiv 1 \pmod{n_2} \end{cases} \quad n = a^b$$

$$|S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$(\textcircled{3}) \cdot \Pr(B)$$

19

α^{18}