$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \bmod n$$

$$a^{n-1} \equiv 1 \bmod n$$

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

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \bmod n$$

$$Q^{n-1} \equiv 1 \bmod n$$

$$Q \cdot a^{n-2} \equiv 1 \bmod n$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\{ a \in \{1, \ldots, n-1\} / \; a^{n-1} \bmod n \neq 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \bmod n$$

$$\{ a \in \{1, \dots, n-1\} / \; a^{n-1} \bmod n \neq 1 \}$$

$$\geq$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \mod n \neq 1 \}$$

$$\supseteq$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \mod n \neq 1 \}$$

$$\supseteq$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = \left| \mathbb{Z}_n^* \right|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \mod n \neq 1 \}$$

$$\supseteq$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \bmod n \neq 1 \}$$

$$\geq X_n$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \bmod n \neq 1 \}$$

$$\geq X_\infty$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \bmod n \neq 1 \}$$

$$\geq X_\infty$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$a^{n-1} \not\equiv 1 \mod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \bmod n \neq 1 \}$$

$$\supseteq X_n$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$MCD(a, n) > 1$

$a^{n-1} \not\equiv 1 \bmod n$

$\phi(1) = 0$

$\phi(n) = |\mathbb{Z}_n^*|$

$$\{ a \in \{1, \dots, n-1\} / \ a^{n-1} \bmod n \neq 1 \}$$

$$\supseteq X_\infty$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$a^{n-1} \not\equiv 1 \bmod n$$

$$\phi(1) = 0$$

$$\phi(n) = |\mathbb{Z}_n^*|$$

$a^{15} \bmod 16 \neq 1$

$$\{ a \in \{1, \dots, n-1\} / \; a^{n-1} \bmod n \neq 1 \}$$

$$\supseteq$$

$$\{ a \in \{1, \dots, n-1\} \mid MCD(a, n) > 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$$PGCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier : $J_n = \mathbb{Z}_n^*$
- n est composé : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $\Rightarrow J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $| J_n = \mathbb{Z}_n^*$
- n es compuesto: $| J_n | \leq \frac{1}{2} | \mathbb{Z}_n^* |$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$PGCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$J_n \subseteq \mathbb{Z}_n^*$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier. $\Rightarrow J_n = \mathbb{Z}_n^*$
- n est composé : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$J_n \subseteq \mathbb{Z}_n^*$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $\Rightarrow J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo, $J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $|J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$J_n \subseteq \mathbb{Z}_n^*$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $| J_n = \mathbb{Z}_n^*$
- n es compuesto: $| J_n | \leq \frac{1}{2} | \mathbb{Z}_n^* |$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$J_n \subseteq \mathbb{Z}_n^*$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $\Rightarrow J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$MCD(a, n) > 1$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

a^{n-1} :

$|\bar{J}_n| \mid |\mathbb{Z}_n^*|$

$||$

109

$$\bar{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

n es primo. $|\bar{J}_n = \mathbb{Z}_n^*$

n es compuesto : $|\bar{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$PGCD(a, n) > 1$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

a^{n-1} :

$|\bar{J}_n| \mid |\mathbb{Z}_n^*|$

$|\mathbb{Z}_n^*| = 109$

$$\bar{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier : $|J_n = \mathbb{Z}_n^*$
- n est composé : $|\bar{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$PGCD(a, n) > 1$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

a^{n-1} :

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

$|\mathbb{Z}_n^*| = 1090$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier : $|J_n = \mathbb{Z}_n^*$
- n est composé : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$$PGCD(a, n) > 1$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$|\overline{J}_n| \mid |\mathbb{Z}_n^*|$$

$|\overline{J}_n|$ ↙ ↓ 1000

$|\mathbb{Z}_n^*|$ = 1090

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier : $|\overline{J}_n = \mathbb{Z}_n^*$
- n est composé : $|\overline{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$|\overline{J}_n| \leq |\mathbb{Z}_n^*|$

$500 \quad 1000 \qquad 1090$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $\quad \overline{J}_n = \mathbb{Z}_n^*$
- n es compuesto: $\quad |\overline{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

a^{n-1} :

$|\overline{J}_n| \mid |\mathbb{Z}_n^*|$

$500 \quad 1000 \quad 1000$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $|J_n = \mathbb{Z}_n^*$
- n es compuesto : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$PGCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$a^{n-1} = 1$

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

$|\overline{J}_n|$: 500 ↙ 1000 ↓

$|\mathbb{Z}_n^*| = 1000$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier, $|\overline{J}_n = \mathbb{Z}_n^*|$
- n est composé : $|\overline{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$MCD(a, n) > 1$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$|\overline{J}_n| \mid |\mathbb{Z}_n^*|$

500 100 1000

- n es primo. $|J_n = \mathbb{Z}_n^*$
- n es compuesto: $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

$\frac{1}{2} \leq \frac{1}{2}$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$PGCD(a, n) > 1$

a^{n-1} :

$|\overline{J_n}| \mid |\mathbb{Z}_n^*|$

$|\overline{J_n}|$: 500 à 1000

$|\mathbb{Z}_n^*| = 1090$

$$\overline{J_n} = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier : $|J_n = \mathbb{Z}_n^*$
- n est composé : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$MCD(a, n) > 1$

a^{n-1} :

$|\overline{J}_n| \mid |\mathbb{Z}_n^*|$

$|\overline{J}_n|$ ↙ 500 ↓ 1000 $\mid$ $|\mathbb{Z}_n^*|$ = 1090

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n es primo. $|J_n = \mathbb{Z}_n^*$
- n es compuesto : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$PGCD(a, n) > 1$

a^{n-1} :

$|\overline{J_n}| \mid |\mathbb{Z}_n^*|$

$|\overline{J_n}| \leq 500$ $\quad$ $|\mathbb{Z}_n^*| = 1090$

$$\overline{J_n} = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

- n est premier. $|J_n = \mathbb{Z}_n^*$
- n est composé : $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$MCD(a, n) > 1$

$|\overline{J}_n| \mid |\mathbb{Z}_n^*|$

$|\overline{J}_n| \leq 500$ $\quad$ $|\overline{J}_n| \leq 1000$ $\quad$ $|\mathbb{Z}_n^*| = 1090$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$(G, \cdot)$ $\quad \cdot : G \times G \to G$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

esiste $a \cdot e = e \cdot a = a$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$|\overline{J}_n| \leq |\mathbb{Z}_n^*|$

$|\mathbb{Z}_n^*| = 1000$

$|\overline{J}_n| \leq 500$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$(G, \cdot)$ $\quad \cdot : G \times G \to G$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

existe $a \cdot e = e \cdot a = a$

$(\mathbb{Z}, +)$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$|\overline{J}_n| \leq |\mathbb{Z}_n^*|$

$500 \quad 1000 \quad 1090$

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$(G, \cdot) \quad \cdot : G \times G \to G$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

existe $a \cdot e = e \cdot a = a$

$(\mathbb{Z}, +)$

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

$$\mathbb{Z}_n^* = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$MCD(a, n) > 1$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$|\overline{J}_n| \leq |\mathbb{Z}_n^*|$

500 ↙ 1000 ↓ = 1090

$$\overline{J}_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$(G, \cdot)$ $\quad \cdot : G \times G \to G$

$(a \cdot b) \cdot c = a \cdot (b \cdot c)$

existe $a \cdot e = e \cdot a = a$

~~$(\mathbb{N}, +)$~~

$(\mathbb{Z}, +)$

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

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \mathrm{MCD}(a, n) = 1 \}$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$\mathrm{MCD}(a, n) > 1$$

$$|\overline{J}_n| \;\Big|\; |\mathbb{Z}_n^*|$$

$500 \quad 1000 \qquad = \; 1090$

$(\mathbb{Z}_n, +)$

$$h = \{ 0, \dots, n-1 \} \quad = 1 \}$$

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

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$

$h = \{ 0, \dots, n-1 \} \quad = 1 \}$

$a \in \{0, \dots, n-1\}$

$-a \quad , \quad n - a$

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

500 1000 = 1090

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

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$(\mathbb{Z}_n, +)$

$h = \{ 0, \dots, n-1 \} \quad = 1 \}$

$(\mathbb{Z}_{10}, +) \quad \{0, \dots, 9\} \qquad a \in \{0, \dots, n-1\}$

$1 + 9 \equiv 0 \mod 10 \qquad -a \quad , \quad n - a$

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

500 1000 $\quad$ 1090

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

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

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

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, \cdot)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

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

500 1000 = 1090

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$(\mathbb{Z}_{10}, \cdot)$

$3 \cdot 7 \equiv 1 \mod 10$

$(\mathbb{Z}_{10}^*, \cdot)$

$\lvert \mathbb{Z}_n \rvert$	$\lvert \mathbb{Z}_n^* \rvert$
500 1000	= 1090

$\mathbb{Z}_{10}^* = \{ 3, 1, 7, 9 \}$

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

$MCD(a, n) > 1$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$(\mathbb{Z}_{10}, \cdot)$

$3 \cdot 7 \equiv 1 \mod 10$

$(\mathbb{Z}_{10}^*, \cdot)$

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

$|\mathbb{Z}_{500}| \mid |\mathbb{Z}_{500}^*|$

$|\mathbb{Z}_{1000}| \mid |\mathbb{Z}_{1000}^*|$

$|\mathbb{Z}_{1000}^*| = 400$

$\mathbb{Z}_{10}^* = \{ 3, 1, 7, 9 \}$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \mathrm{MCD}(a, n) = 1 \}$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

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

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{3, 5, 7, 9, 11, 13, 15, 1\}$

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

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$$

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

$\mathbb{Z}_{16}^* = \{3, 5, 7, 9, 11, 13, 15, 1\}$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$$

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

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

$(\mathbb{Z}_n, +)$

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$(\mathbb{Z}_{10}, +) \quad \{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$

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

$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$

$(\mathbb{Z}_n, +)$

$(\mathbb{Z}_{10}, +)$ $\{0, \dots, 9\}$

$1 + 9 \equiv 0 \mod 10$

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$a \cdot c \equiv 1 \mod n$

$b \cdot d \equiv 1 \mod n$

$(a \cdot b) \cdot (d \cdot c) \equiv 1 \mod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / MCD(a, n) = 1 \}$$

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \}$$

$$(\mathbb{Z}_n, +)$$

$$(\mathbb{Z}_{10}, +) \quad \{0, \dots, 9\}$$

$$1 + 9 \equiv 0 \bmod 10$$

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

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$a \cdot c \equiv 1 \bmod n$

$b \cdot d \equiv 1 \bmod n$

$(a \cdot b) \cdot (d \cdot c) \equiv 1 \bmod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

$(J_n, \cdot)$ es un grupo

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

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$a \cdot c \equiv 1 \bmod n$

$b \cdot d \equiv 1 \bmod n$

$(a \cdot b) \cdot (d \cdot c) \equiv 1 \bmod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

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

$(J_n, \cdot)$ es un grupo

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$a \cdot c \equiv 1 \bmod n$

$b \equiv 1 \bmod n$

$(a \cdot b) \cdot (b \cdot c) \equiv 1 \bmod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ MCD(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

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

$(J_n, \cdot)$ es un grupo

$MCD(a, n) = 1$

$MCD(b, n) = 1$

$\Downarrow$

$MCD(a \cdot b, n) = 1$

$a \cdot c \equiv 1 \bmod n$

$b \cdot d \equiv 1 \bmod n$

$(a \cdot b) \cdot (d \cdot c) \equiv 1 \bmod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \} \qquad (\mathbb{Z}_n^*, \cdot)$$

$(J_n, \cdot)$ est un groupe

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$$

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

$(J_n, \cdot)$ est un groupe

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$

$(\{0\}, +)$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / \; a^{n-1} \bmod n = 1 \}$$

$(J_n, \cdot)$ est un groupe

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$

$(\{0\}, +)$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \ PGCD(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / \ a^{n-1} \bmod n = 1 \}$ $\quad (\mathbb{Z}_n^*, \cdot)$

$(J_n, \cdot)$ est un groupe $\quad (\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$

$(\{0\}, +)$

$(\{0, 2, 4, 6, 8\}, +)$

$\bmod n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$$

$(J_n, \cdot)$ est un groupe

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ → 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$.

$\varphi(n)$

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ → 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ | n

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ → 10

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$(\{0\}, +) \to 1$

$\{0; 3, 7, 6, 9, 5$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ | d n

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0,3,7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2\}$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ ↳ 10

$(\{0\}, +) \to 1$

$(\{0,2,4,6,8\}, +) \to 5$

$(\{0,5\}, +) \to 2$ où n

$\mathbb{U}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2, 8\}$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ ↳ 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ où n

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2, 8\}$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ → 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ mod n

$\mathbb{U}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2, 8\}$

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

$(\mathbb{Z}_{/10}, +) = \{0, \dots, 9\}$ ↳ 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, \cdot) \to 5$

$(\{0, 5\}, +) \to$ mod n

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2, 8\}$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ ↳ 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ où n

$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{PGCD}(a, n) = 1 \}$

$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \}$

$(J_n, \cdot)$ est un groupe

$(\{0, 3, 7\}, +)$

$3 + 3 = 6$

$\{0; 3, 7, 6, 9, 5, 4, 1, 2, 8\}$

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

$(\mathbb{Z}_{10}, +) = \{0, \dots, 9\}$ ↳ 10

$(\{0\}, +) \to 1$

$(\{0, 2, 4, 6, 8\}, +) \to 5$

$(\{0, 5\}, +) \to 2$ sdn

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{MCD}(a, n) = 1 \}$$

$$J_n = \{ a \in \mathbb{Z}_n^* / a^{n-1} \bmod n = 1 \} \qquad (\mathbb{Z}_n^*, \cdot) \qquad (a \cdot b) \cdot (a' \cdot b)$$

$(J_n, \cdot)$ es un grupo $\qquad \cdot : J_n \times J_n \longrightarrow J_n$

① Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

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

$\in J_n$

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \mathrm{MCD}(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / \; a^{n-1} \bmod n = 1 \}$ $\quad (\mathbb{Z}_n^*, \cdot)$ $\quad (a \cdot b) \cdot (a \cdot b)$

$(J_n, \cdot)$ es un grupo $\quad \cdot : J_n \times J_n \longrightarrow J_n$

① Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$$a^{n-1} \equiv 1 \bmod n \qquad \Rightarrow \qquad (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$$
$$b^{n-1} \equiv 1 \bmod n \qquad \equiv 1 \cdot 1 \equiv 1 \bmod n$$

② Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$$\mathbb{Z}_n = \{ a \in \{1, \dots, n-1\} / \text{MCD}(a, n) = 1 \}$$

$J_n = \{ a \in \mathbb{Z}_n^* / \; a^{n-1} \bmod n = 1 \}$ $\quad (\mathbb{Z}_n^*, \cdot)$ $\quad (a \cdot b) \cdot (a' \cdot b)$

$(J_n, \cdot)$ es un grupo $\quad \cdot : J_n \times J_n \longrightarrow J_n$

① Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$$a^{n-1} \equiv 1 \bmod n \qquad \Rightarrow \qquad (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$$
$$b^{n-1} \equiv 1 \bmod n \qquad \equiv 1 \cdot 1 \equiv 1 \bmod n$$

② Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe $b : a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$
↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$

$u \equiv r \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot r \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$
↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (LHS)

$u \equiv v \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (Lema 1.6.5)
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

① Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum \frac{1}{p}$ p primos

② Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

↳ $a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (Lemma)

$u \equiv v \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (Lema 1.6.5)
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (Lema 1.6.5)
$u \equiv v \bmod n$
$\Downarrow$
$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$
$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$
$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (LEMA)

$u \equiv v \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (LEMA)

$u \equiv v \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n

$x \equiv y \bmod n$ (Lema 1.0.5)

$u \equiv v \bmod n$

$\Downarrow$

$x \cdot u \equiv y \cdot v \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv 1 \bmod n$

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

$\Rightarrow \boxed{b^{n-1} \equiv 1 \bmod n} \Rightarrow b \in J_n$.

(1) Si $a, b \in J_n$, entonces $a \cdot b \in J_n$

$a^{n-1} \equiv 1 \bmod n$

$b^{n-1} \equiv 1 \bmod n$

$\Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1}$

$\equiv 1 \cdot 1 \equiv 1 \bmod n$

$\sum_{p \text{ primos}} \frac{1}{p}$

(2) Si $a \in J_n$, entonces existe $b \in J_n$ tal que $a \cdot b \equiv 1 \bmod n$

$\hookrightarrow a \in \mathbb{Z}_n^*$, entonces existe b: $a \cdot b \equiv 1 \bmod n$

J_n