





11

6

7

8 9

11





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

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

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

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

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

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

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

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

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

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

$$\{a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1\}$$

~

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

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

$$\left\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \right\}$$

≥

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

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

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

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

$$\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \}$$

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

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

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

$$\phi(1) = 0$$

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

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

$$\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \}$$

$$\underline{\mathbb{Z}}^* \sim \{ a \in \{1, \dots, n-1\} \mid \text{MCD}(a, n) > 1 \}$$

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

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

$$\phi(1) = 0$$

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

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

$$\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \}$$

2

n

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

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

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

$$\phi(1) = 0$$

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

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

$$\left\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \right\}$$

$$\geq X_n$$

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

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

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

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

$$\phi(1) = 0$$

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

$$\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \}$$

$$\geq X_n$$

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

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

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

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

$$\phi(1) = 0$$

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

$$\left\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \right\} \geq X_n$$

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

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

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

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

$$\phi(1) = 0$$

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

$$\left\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \right\}$$

$$\geq X_n$$

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \begin{array}{l} \text{MCD}(a, n) > 1 \\ a^{n-1} \not\equiv 1 \pmod{n} \end{array} \quad \begin{array}{l} \phi(1) = 0 \\ \phi(n) = |\mathbb{Z}_n^*| \end{array}$$
$$\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \}$$
$$\geq X_n$$

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \begin{array}{l} \text{MCD}(a, n) > 1 \\ a^{n-1} \not\equiv 1 \pmod{n} \end{array} \quad \begin{array}{l} \phi(1) = 0 \\ \phi(n) = |\mathbb{Z}_n^*| \end{array}$$

$$a^{15} \pmod{16} \quad \left\{ a \in \{1, \dots, n-1\} \mid a^{n-1} \pmod{n} \neq 1 \right\}$$

$\geq X_n$

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

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

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

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

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

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

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

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

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

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

$$\begin{matrix} n-1 \\ \vdots \\ a^{n-1} \end{matrix}$$

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

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

$$n \text{ es primo}, \quad J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

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

$$n \text{ es primo}, |J_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

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

$$n \text{ es primo}, J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

$$\begin{matrix} n-1 \\ \vdots \\ a \end{matrix}$$

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

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

$$n \text{ es primo}, |J_n| = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

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

$$n \text{ es primo}, \quad J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

$$\begin{matrix} n-1 \\ \vdots \\ 1 \end{matrix}$$

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

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

$$n \text{ es primo}, J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

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

$$n \text{ es primo}, J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

$$\begin{matrix} n-1 \\ \vdots \\ a^{n-1} \end{matrix}$$

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

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

$$n \text{ es primo}, |J_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

$$\begin{matrix} n-1 \\ \vdots \\ a^{n-1} \end{matrix}$$

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

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

$$n \text{ es primo}, J_n = \mathbb{Z}_n^*$$

$$\text{Ist komposit: } |J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

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

$\frac{11}{109}$

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

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

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

$\circ^{n-1} =$

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

11  
109

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

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

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

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

$$|\bar{J}_n| \mid |\mathbb{Z}_n^*| \\ 11 \\ 1000$$

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

$$n \text{ es primo}, \quad |J_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |\bar{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

$\text{MCD}(a, n) > 1$   
 $a^{n-1} \equiv 1 \pmod{n}$

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

↓      ↓  
 1000      1000

$$\mathbb{J}_n = \{ a \in \mathbb{Z}_n^* \mid a^{n-1} \pmod{n} = 1 \}$$

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

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

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

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

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

$\text{MCD}(a, n) > 1$   
 $a^{n-1} \equiv 1 \pmod{n}$

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & 1000 \end{array}$$

$$\mathbb{J}_n = \{ a \in \mathbb{Z}_n^* \mid a^{n-1} \equiv 1 \pmod{n} \}$$

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

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

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ 11 & 1000 \end{array}$$

$$\mathbb{J}_n = \{ a \in \mathbb{Z}_n^* \mid a^{n-1} \pmod{n} = 1 \}$$

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

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

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

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

$$\mathbb{Z}_{16}^* = \{ 3, 5, 7, 9, 11, 13, 15, 1 \} \quad \text{MCD}(a, n) > 1$$

$\hookrightarrow$

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

$ J_n $	$ \mathbb{Z}_n^* $
500	1000
11	1000

$\therefore$   $n$  es primo,  $|J_n| = |\mathbb{Z}_n^*$

Let's compute:  $|J_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

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

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

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

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

$$\begin{matrix} n-1 \\ \circ \end{matrix}$$

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

↓ ↓

500 100

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

$$n \text{ es primo}, |\mathbb{J}_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |\mathbb{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

$$\frac{15}{30} \leq \frac{1}{2}$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & 1000 \end{array}$$

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

$$n \text{ es primo}, |\mathbb{J}_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |\mathbb{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{I} \\ 1000 & 0 \end{array}$$

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

$$n \text{ es primo}, |\mathbb{J}_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |\mathbb{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{II} \\ 1000 & 0 \end{array}$$

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

$$n \text{ es primo}, |\mathbb{J}_n| = |\mathbb{Z}_n^*|$$

$$\text{Ist komposit: } |\mathbb{J}_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{II} \\ 1000 & 0 \end{array}$$

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

$$\cdot(G, \cdot) : G \times G \rightarrow G$$

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

$$\text{exists } e \cdot a = a \cdot e = a$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II.} & \text{1000} \end{array}$$

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

$$\begin{array}{l} \cdot(G, \cdot) : G \times G \rightarrow G \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ \text{exists } e \cdot a = e \cdot a = a \end{array}$$

$$\begin{array}{l} ((\cancel{G}, \cancel{\cdot})) \\ (\mathbb{Z}, +) \end{array}$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{II} \\ 1000 & 0 \end{array}$$

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

$$\begin{array}{l} \cdot(G, \cdot) : G \times G \rightarrow G \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ \text{exists } e \cdot a = e \cdot a = a \end{array}$$

$$\begin{array}{c} (\text{NG}) \\ (\mathbb{Z}, +) \end{array}$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{II} \\ 1000 & 0 \end{array}$$

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

$$\begin{array}{l} \cdot(G, \cdot) : G \times G \rightarrow G \\ (a \cdot b) \cdot c = a \cdot (b \cdot c) \\ \text{exists } e \cdot a = a \cdot e = a \end{array}$$

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

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & 1000 \end{array}$$

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & \text{I} \\ 1000 & 0 \end{array}$$

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

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

$$-a, n-a$$

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

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

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

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

$$\begin{array}{c|c} |\mathbb{J}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ \text{II} & 1000 \\ 0 & 0 \end{array}$$

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

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

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

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

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

$$1+9 \equiv 0 \pmod{10}$$

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

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

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

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

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

$$\begin{array}{c|c} |\mathbb{Z}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ 11 & 1000 \end{array}$$

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

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

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

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

$$\begin{array}{c|c} |\bar{\mathbb{Z}}_n| & |\mathbb{Z}_n^*| \\ \downarrow & \downarrow \\ 500 & 1000 \\ 11 & 1000 \end{array}$$

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

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

$$3 \cdot 7 \equiv 1 \pmod{10}$$

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

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

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

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

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

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

$$\begin{array}{c|c} [\bar{j}_n] & |\mathbb{Z}_n^* \\ \downarrow & \downarrow \\ 500 & 1000 \\ 11 & 1000 \end{array}$$

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

$$3 \cdot 7 \equiv 1 \pmod{10}$$

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

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

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

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

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

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

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

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

$$(\mathbb{Z}_{10}, +) \quad \{0, -1, 9\}$$

$$1 + 9 \equiv 0 \pmod{10}$$

$$(\mathbb{Z}_{n+1}^*, \cdot)$$

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

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

$$\downarrow$$
$$\text{MCD}(a \cdot b, n) = 1$$

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

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

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

$$(\mathbb{Z}_{n+1}^*, \cdot)$$

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

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

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

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

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

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

$$(\mathbb{Z}_{10}, +) \quad \{0, -1, 9\}$$

$$1 + 9 \equiv 0 \pmod{10}$$

$$(\mathbb{Z}_{n+1}^*, \cdot)$$

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

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

$$\downarrow$$
$$\text{MCD}(a \cdot b, n) = 1$$

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

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

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

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

$$1 + 9 \equiv 0 \pmod{10}$$

$$(\mathbb{Z}_{n+1}^*, \cdot)$$

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

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

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

$$a \cdot c \equiv 1 \pmod{n}$$

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

$$(a \cdot b) \cdot (d \cdot c) \equiv 1 \pmod{n}$$

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

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

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

$$(\mathbb{Z}_{10}, +) \quad \{0, -1, 9\}$$

$$1 + 9 \equiv 0 \pmod{10}$$

$$(\mathbb{Z}_{n+1}^*, \cdot)$$

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

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

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

$$a \cdot c \equiv 1 \pmod{n}$$

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

$$(a \cdot b) \cdot (c \cdot d) \equiv 1 \pmod{n}$$

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

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

$(\mathbb{J}_n, \cdot)$  is a group

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

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

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

$$a \cdot c \equiv 1 \pmod{n}$$

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

$$(a \cdot b) \cdot (d \cdot c) \equiv 1 \pmod{n}$$

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

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

$(\mathbb{J}_n, \cdot)$  is a group

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

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

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

$$a \cdot c \equiv 1 \pmod{n}$$

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

$$(a \cdot b) \cdot (b \cdot c) \equiv 1 \pmod{n}$$

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

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

$(\mathbb{J}_n, \cdot)$  is a group

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

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

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

$$a \cdot c \equiv 1 \pmod{n}$$

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

$$(a \cdot b) \cdot (d \cdot c) \equiv 1 \pmod{n}$$

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

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

$(J_n, \cdot)$  es un grupo

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

wd n

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

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

$(J_n, \cdot)$  es un grupo

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

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

wd n

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

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

$(J_n, \cdot)$  es un grupo

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

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

wd n

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

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

$(J_n, \cdot)$  es un grupo

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

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

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

wd n

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

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

$(J_n, \cdot)$  es un grupo

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

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

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

wd N

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

$$\{0, 3, 7, 6\}$$

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

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

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

$$(\{0, 5\}, +) \rightarrow 2 \text{ wdn}$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3 + 3 = 6$$

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

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

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

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

$$(\{0, 5\}, +) \rightarrow 2 \text{ wd } n$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

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

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

$$(\{0, 5\}, +) \rightarrow 2 \text{ wdn}$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

$$\{0, 3, 7, 6, 9, 5, 4, 1, 2, 8\} \quad (\{0, 2, 4, 6, 8\}, +) \rightarrow 5$$

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

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

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

$(\mathbb{J}_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

$$\{0, 3, 7, 6, 9, 5, 4, 1, 2, 8\} \quad (\{0, 2, 4, 6, 8\}, +) \rightarrow 5$$

$$(\{0, 5\}, +) \rightarrow 2 \bmod n$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

$$\{0, 3, 7, 6, 9, 5, 4, 1, 2, 8\} \quad (\{0, 2, 4, 6, 8\}, +) \rightarrow 5$$

$$(\{0, 5\}, +) \rightarrow \text{wd } n$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

$$\{0, 3, 7, 6, 9, 5, 4, 1, 2, 8\} \quad (\{0, 2, 4, 6, 8\}, +) \rightarrow 5$$

$$(\{0, 5\}, +) \rightarrow 2 \text{ wd } n$$

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

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

$(J_n, \cdot)$  es un grupo

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

$$3+3=6$$

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

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

$$\{0, 3, 7, 6, 9, 5, 4, 1, 2, 8\} \quad (\{0, 2, 4, 6, 8\}, +) \rightarrow 5$$

$$(\{0, 5\}, +) \rightarrow 3 \text{ w.n.}$$

$$Z_n \geq \{ \alpha \in \{1, \dots, n-1\} / M(\alpha, n) \} = 1 \}$$

$$\exists n \in \mathbb{N} \exists a \in \mathbb{Z}^n / q^{n-1} \mid (a \cdot b) - (a' \cdot b') \quad \text{mod } n = 1$$

$i: \mathcal{T}_n \times \mathcal{T}_n \rightarrow \mathcal{T}_n$

On a, b  $\in \mathbb{J}_n$ , witness  $a \cdot b \in \mathbb{J}_n$

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \quad \Rightarrow \quad \begin{aligned} (a \cdot b)^{n-1} &\equiv a^{n-1} \cdot b^{n-1} \\ &\equiv 1 \cdot 1 \equiv 1 \pmod{n} \end{aligned}$$

A scatter plot illustrating the distribution of data points across a 2D plane. The horizontal axis (x) and vertical axis (y) both range from -10 to 10. The data points are represented by small dots, with their color intensity indicating their frequency or density at that specific coordinate. A prominent red dashed circle is drawn around the origin (0,0), highlighting a dense central cluster of points. Several other clusters of varying sizes are scattered across the plot, including a large one near (-8, 2), a medium one near (2, -8), a medium one near (8, 2), a small one near (2, 8), a small one near (-2, -8), and another medium one near (8, -2).

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

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

$(J_n, \cdot)$  es un grupo  $\therefore J_n \times J_n \rightarrow J_n$

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Si  $a \in \mathbb{Z}_n^*$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n}$   $\therefore b \in J_n$

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

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

$(J_n, \cdot)$  es un grupo

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

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

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \rightarrow J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n}$   $\Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n}$   $\Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

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

Sea  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

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

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

Given  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n}$   $\Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L.1. u vs.

$$\downarrow$$

$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\begin{aligned} &=? (a \cdot b)^{n-1} \equiv 1 \pmod{n} \\ &\Rightarrow a^{n-1} \cdot b^{n-1} \equiv 1 \pmod{n} \quad (a^{n-1} \equiv 1 \pmod{n}) \\ &\Rightarrow b^{n-1} \equiv 1 \pmod{n} \Rightarrow b \in J_n. \end{aligned}$$

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \\ b^{n-1} &\equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n} \end{aligned}$$

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Given  $a \in J_n$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS.



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Si  $a \in J_n$ , entonces existe  $b \in J_n$  tal que  $a \cdot b \equiv 1 \pmod{n}$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS.



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Si  $a \in \mathbb{Z}_n^*$ , entonces existe  $b \in \mathbb{Z}_n$  tal que  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS.



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

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

$$b^{n-1} \equiv 1 \pmod{n} \quad \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Given  $a \in J_n$ , there exists  $b \in J_n$  such that  $a \cdot b \equiv 1 \pmod{n}$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS.



$$x \cdot u \equiv y \cdot v \pmod{n}$$

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

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

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

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

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

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

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

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

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Sea  $a \in J_n$ , entonces existe  $b$  s.t.  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$

$$x \equiv y \pmod{n}$$

$$u \equiv v \pmod{n}$$

L. A. UVS.



$$x \cdot u \equiv y \cdot v \pmod{n}$$

$$\stackrel{?}{=} (a \cdot b)^{n-1} \equiv 1 \pmod{n}$$

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

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

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

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ b^{n-1} &\equiv 1 \pmod{n} \end{aligned} \Rightarrow (a \cdot b)^{n-1} \equiv a^{n-1} \cdot b^{n-1} \equiv 1 \cdot 1 \equiv 1 \pmod{n}$$

$$\left( \sum_{p \text{ primo}} \frac{1}{p} \right)$$

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

Si  $a \in \mathbb{Z}_n^*$ , entonces existe  $b$ :  $a \cdot b \equiv 1 \pmod{n} \Rightarrow b \in J_n$