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

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

$\searrow -1$

$$n \mapsto \alpha \in \{1, \dots, n-1\}$$

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

$$1 \leftarrow \quad \swarrow \quad \searrow \quad -1$$

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

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

$(S_n, \cdot)$

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

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

$\searrow -1$

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

$S_n = S_n^+ \cup S_n^-$

$S_n \rightarrow -1$

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

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

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

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

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

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

$(S_n, \cdot)$

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

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

$\searrow -1$

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

$S_n = S_n^+ \cup S_n^-$ $\rightarrow -1$

$\downarrow$

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

$S_n = S_n^+ \cup S_n^-$

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

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

$\searrow -1$

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

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

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

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

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

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

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

$n \cdot \alpha \equiv 1 \bmod m$

$m \cdot \beta \equiv 1 \bmod n$

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

$m \cdot \beta \equiv 1 \bmod n$

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

$c \equiv a \bmod m$

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

$m \beta \equiv 1 \bmod n$

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

$c \equiv a \bmod m$

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

$m \cdot \beta \equiv 1 \bmod n$

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

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

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

$a, b \in S_n$ $\quad a \cdot b \in S_n$

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

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

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

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

$$n \cdot d \equiv 1 \bmod m$$
$$m \cdot \beta \equiv 1 \bmod n$$

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

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

$n = n_1 \cdot n_2$

$$c \equiv a \bmod n_1$$
$$c \equiv 1 \bmod n_2$$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$n = n_1 \cdot n_2$

$c \equiv a \mod n_1$

$c \equiv 1 \mod n_2$

$c^{\frac{n-1}{}}$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

(*) $c \equiv a \mod n_1$

(*) $c \equiv 1 \mod n_2$

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

$d \equiv \beta \mod n$

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

$\mod n_1$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

$(k \cdot n_2) \cdot n_1 = \alpha - \beta$

$n_1 / \alpha - \beta$

$\alpha \equiv \beta \mod n_1$

$n / \alpha - \beta$

$k \cdot n = \alpha - \beta$

$k \cdot n_1 \cdot n_2 = \alpha - \beta$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

$(k \cdot n_2) \cdot n_1 = \alpha - \beta$

$n_1 / \alpha - \beta$

$\alpha \equiv \beta \mod n$

$\Downarrow$

$\alpha \equiv \beta \mod n_1$

$n / \alpha - \beta$

$k \cdot n = \alpha - \beta$

$k \cdot n_1 \cdot n_2 = \alpha - \beta$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

$(k \cdot n_2) \cdot n_1 = \alpha - \beta$

$n_1 \mid \alpha - \beta$

$\alpha \equiv \beta \mod n$

$\Downarrow$

$\alpha \equiv \beta \mod n_1$

$n_1 \mid \alpha - \beta$

$k \cdot n = \alpha - \beta$

$k \cdot n_1 \cdot n_2 = \alpha - \beta$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

$(k \cdot n_2) \cdot n_1 = \alpha - \beta$

$n_1 \mid \alpha - \beta$

$\alpha \equiv \beta \mod n$

$\Downarrow$

$\alpha \equiv \beta \mod n_1$

$n \mid \alpha - \beta$

$k \cdot n = \alpha - \beta$

$k \cdot n_1 \cdot n_2 = \alpha - \beta$

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

$$n \cdot \alpha \equiv 1 \bmod m$$
$$m \cdot \beta \equiv 1 \bmod n$$

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

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

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

① $c \equiv a \bmod n_1$

② $c \equiv 1 \bmod n_2$

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

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

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

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

$$m \cdot \alpha \equiv 1 \bmod n$$
$$m \cdot \beta \equiv 1 \bmod n$$

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

$$c \equiv a \bmod m$$
$$c \equiv b \bmod n$$

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

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

① $c \equiv a \bmod n_1$

② $c \equiv 1 \bmod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

α^{-1}

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

$1 \mod n_1$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

$\alpha \cdot \beta$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

α^{-1}

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

$m \cdot \beta \equiv 1 \bmod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

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

① $c \equiv a \bmod n_1$

② $c \equiv 1 \bmod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

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

$m \cdot \beta \equiv 1 \mod n$

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$225 = 15^2 = \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$ $\quad \frac{1}{\ln n}$

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

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

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

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

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

$c \equiv a \bmod m$

$c \equiv b \bmod n$

$225 = 15^2$

$= \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

$n = n_1 \cdot n_2$

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

① $c \equiv a \bmod n_1$

② $c \equiv 1 \bmod n_2$

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

$m \cdot \beta \equiv 1 \bmod n$

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

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

$MCD(N_1, N_2) = P$

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

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

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

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$225 = 15^2$

$= \underbrace{3^2}_{n_1} \cdot \underbrace{5^2}_{n_2}$

$n = n_1 \cdot n_2$

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

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$MCD(N_1, N_2) = P$ ✗

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

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

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

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

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

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

$C \equiv a \bmod m$

$C \equiv b \bmod n$

$225 = 15^2$

$= 3^2 \cdot 5^2$

$n_1 \quad n_2$

$n = n_1 \cdot n_2$

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

$m \cdot d \equiv 1 \bmod m$

$m \cdot \beta \equiv 1 \bmod n$

① $C \equiv a \bmod n_1$

② $C \equiv 1 \bmod n_2$

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

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

$MCD(N_1, N_2) = P$

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

$C^{\frac{n-1}{2}} \equiv 1 \bmod n \rightarrow C^{\frac{n-1}{2}} \equiv 1 \bmod n_1$

$Q^{\frac{n-1}{2}} \equiv 1 \bmod n_1$

$MCD(m,n) = 1$

$c \equiv a \mod m$

$c \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

a, b

$N = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

$n = n_1 \cdot n_2$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

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

$MCD(N_1, N_2)$.

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

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

$\frac{n-1}{2} \equiv -1 \mod n_1$

α^{17}

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

$n = n_1 \cdot n_2$

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

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

① $c \equiv a \bmod n_1$

② $c \equiv 1 \bmod n_2$

$c \equiv a \bmod m$

$c \equiv b \bmod n$

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

$m \cdot \beta \equiv 1 \bmod n$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$MCD(N_1, N_2) = P$

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

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

$a^{\frac{n-1}{2}} = -1 \bmod n_1$

α^{-1}

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

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

$n = n_1 \cdot n_2$

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

① $C \equiv a \mod n_1$

② $C \equiv 1 \mod n_2$

$C \equiv a \mod m$

$C \equiv b \mod n$

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

$m \cdot \beta \equiv 1 \mod n$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$MCD(N_1, N_2) = P$ ✗

$C^{\frac{n-1}{2}} \equiv -1 \mod n$ ✗

$C^{\frac{n-1}{2}} \equiv 1 \mod n \rightarrow C^{\frac{n-1}{2}} \equiv 1 \mod n_1$

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

a^{12}

$MCD(m,n) = 1$

a, b

$C \equiv a \bmod m$

$C \equiv b \bmod n$

$n \cdot \alpha \equiv 1 \bmod m$

$m \cdot \beta \equiv 1 \bmod n$

$\Pi(n)$: número de primos hasta n

$$\lim_{n\to\infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$N = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$MCD(N_1, N_2) = P$

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

$n = n_1 \cdot n_2$

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

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

① $C \equiv a \bmod n_1$

② $C \equiv 1 \bmod n_2$

$C^{\frac{n-1}{2}} \equiv -1 \bmod n$ ✗

$C^{\frac{n-1}{2}} \equiv 1 \bmod n \rightarrow C^{\frac{n-1}{2}} \equiv 1 \bmod n_1$

$Q \equiv 1 \bmod n_1$

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

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

$n = n_1 \cdot n_2$

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

① $C \equiv a \mod n_1$

② $C \equiv 1 \mod n_2$

$C \equiv a \mod m$

$C \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$MCD(N_1, N_2) = P$

$C^{\frac{n-1}{2}} \equiv -1 \mod n$

$C^{\frac{n-1}{2}} \equiv 1 \mod n \rightarrow C^{\frac{n-1}{2}} \equiv 1 \mod n_1$

$Q^{\frac{n-1}{2}} \equiv -1 \mod n_1$

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

$n = n_1 \cdot n_2$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

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

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

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

$c \equiv a \mod m$

$c \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

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

$MCD(N_1, N_2) = P$ ✗

$MCD(m,n) = 1$

a, b

$C \equiv a \bmod m$

$C \equiv b \bmod n$

$n \cdot \alpha \equiv 1 \bmod m$

$m \cdot \beta \equiv 1 \bmod n$

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

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

$MCD(N_1, N_2) := P$

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

$n = n_1 \cdot n_2$

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

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

① $C \equiv a \bmod n_1$

② $C \equiv 1 \bmod n_2$

$n = a^b$

$n = 2^b$

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

$C^{\frac{n-1}{2}} \equiv 1 \bmod n \rightarrow C^{\frac{n-1}{2}} \equiv 1 \bmod n_1$

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

$MCD(m,n) = 1$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

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

$n = n_1 \cdot n_2$

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

$n = a^b$

$n = 2^b$

$c \equiv a \mod m$

$c \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

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

$c^{\frac{n-1}{2}} \equiv -1 \mod n$ ✗ $b = \log_2 n$

$MCD(N_1, N_2) = P$ ✗

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

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

α^{-1}

$MCD(m,n) = 1$

$c \equiv a \mod m$

$c \equiv b \mod n$

$n \cdot \alpha \equiv 1 \mod m$

$m \cdot \beta \equiv 1 \mod n$

a, b

$N = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

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

$n = n_1 \cdot n_2$

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

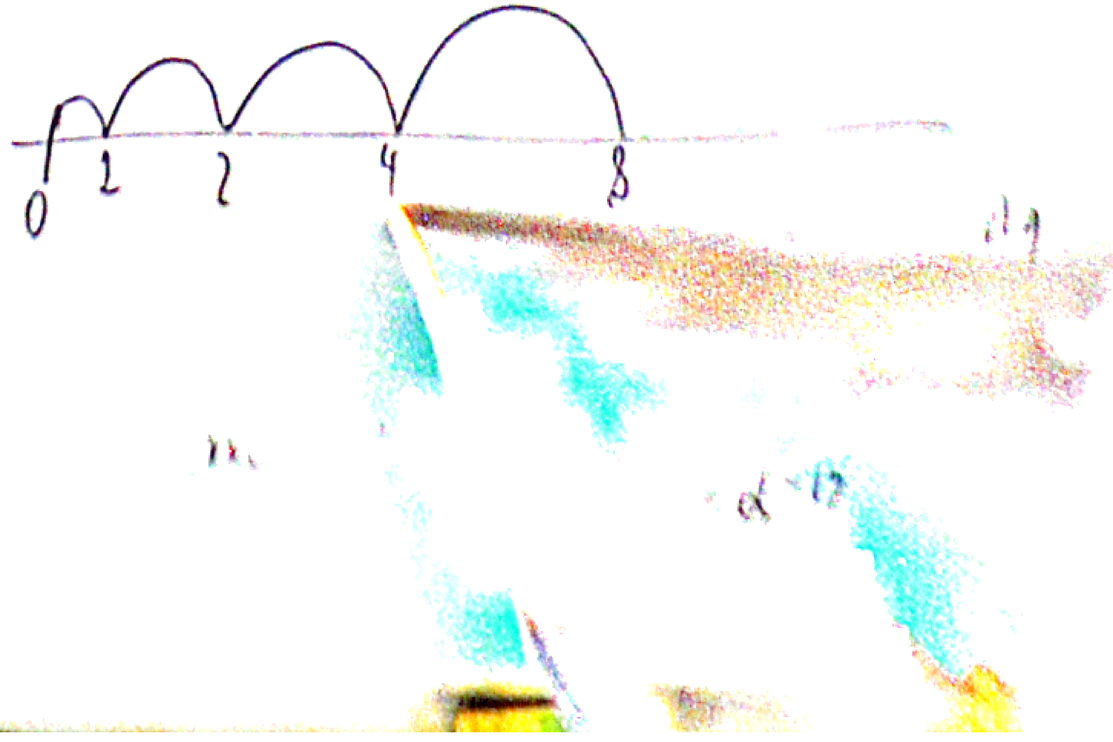
$n = a^b$,

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

$MCD(N_1, N_2) = 1$

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



$MCD(m,n) = 1$

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

a, b

$N = P \cdot Q$

$N_1 = P \cdot R$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

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

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

$n = n_1 \cdot n_2$

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

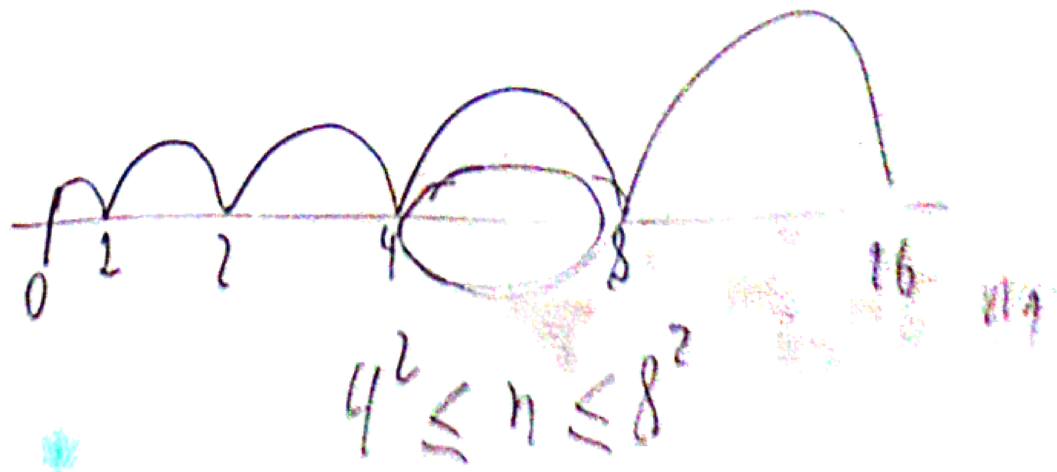
$n = a^b$,

$\Pi(n)$: número de primos hasta n

$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$

$MCD(N_1, N_2) = 1$

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



$4^2 \leq n \leq 8^2$

$MCD(m,n) = 1$

$c \equiv a \mod m$

$c \equiv b \mod n$

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

$m \beta \equiv 1 \mod n$

a, b

$N_1 = P \cdot Q$

$N_2 = P \cdot R$

$N_1 = P \cdot Q$

$N_1 = P \cdot Q$

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

$n = n_1 \cdot n_2$

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

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

① $c \equiv a \mod n_1$

② $c \equiv 1 \mod n_2$

$n = a^b$,

$\Pi(n)$: número de primos hasta n

$$\lim_{n \to \infty} \frac{\Pi(n)}{\left(\frac{n}{\ln n}\right)} = 1$$

$MCD(N_1, N_2) = 1$

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

n es primo

if $neg = 0$ then return COMP

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

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

(1) $c \equiv a \mod n_1$, $n = a^b$

(2) $c \equiv 1 \mod n_2$,

$4^2 \leq n \leq 8^2$

n.

α^{-17}

n es primo

if $neg = 0$ then return COMP

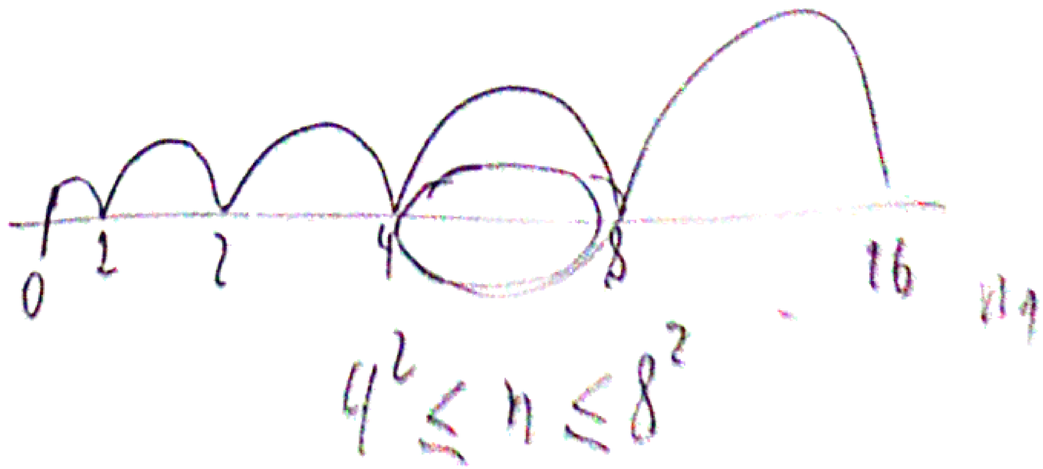
$b_1, \dots, b_k$

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$



$q^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

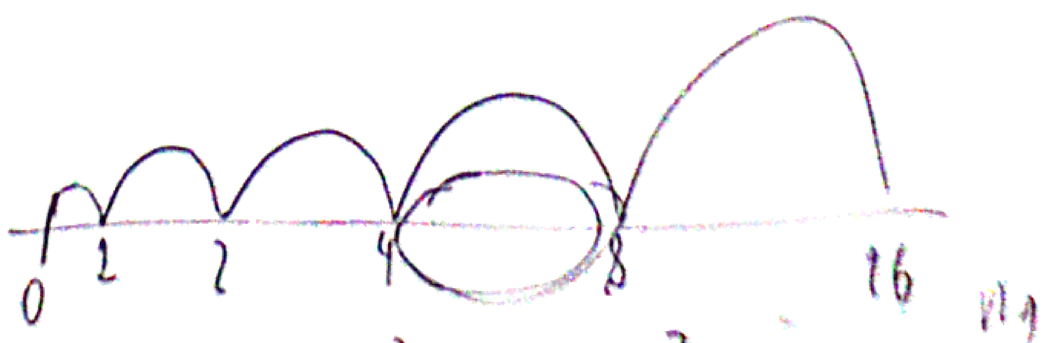
b_1 —, b_k

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

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

(1) $c \equiv a \bmod n_1$, $n = a^b$

(2) $c \equiv 1 \bmod n_2$,



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$

$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1 \ldots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

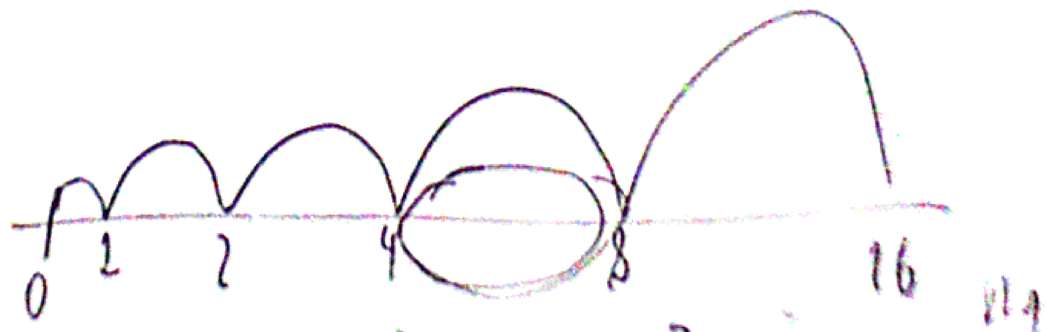
n es compuesto

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

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

(1) $c \equiv a \mod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \mod n_2$,



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

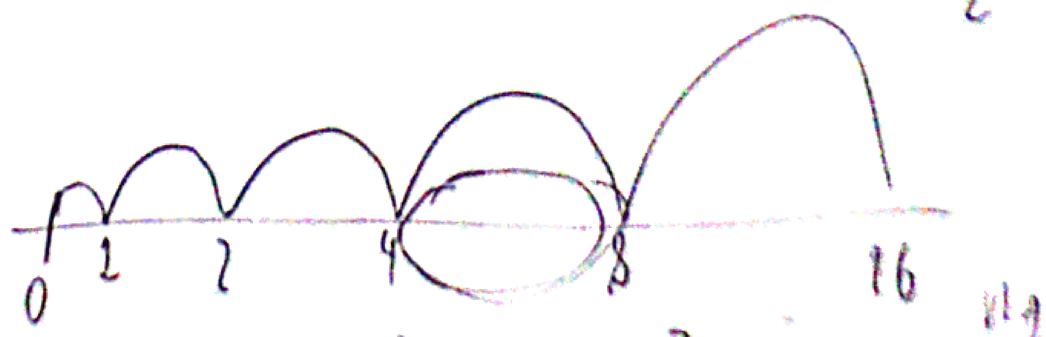
n es compuesto

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1 \ldots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

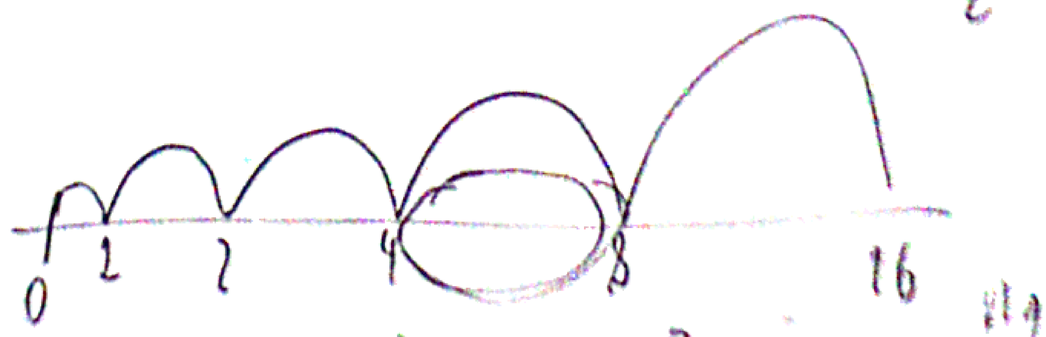
n es compuesto

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1 \ldots b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

n es compuesto

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$

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

$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

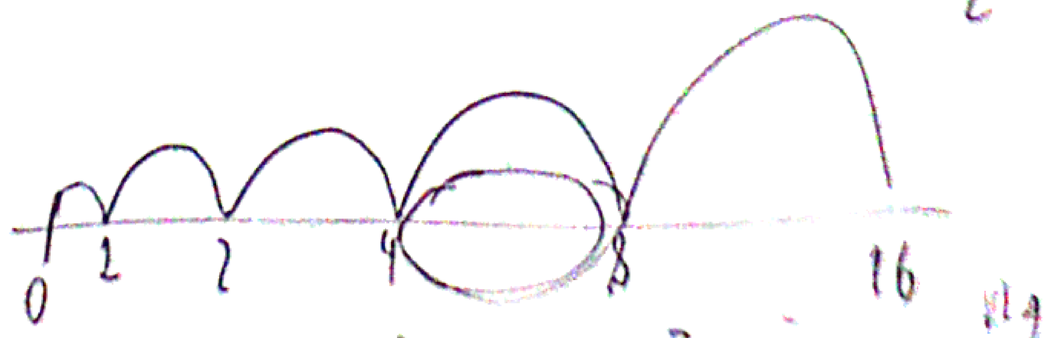
n es compuesto

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1 \ldots b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

$Pr(A \cap B) \leq Pr(A)$

n es compuesto

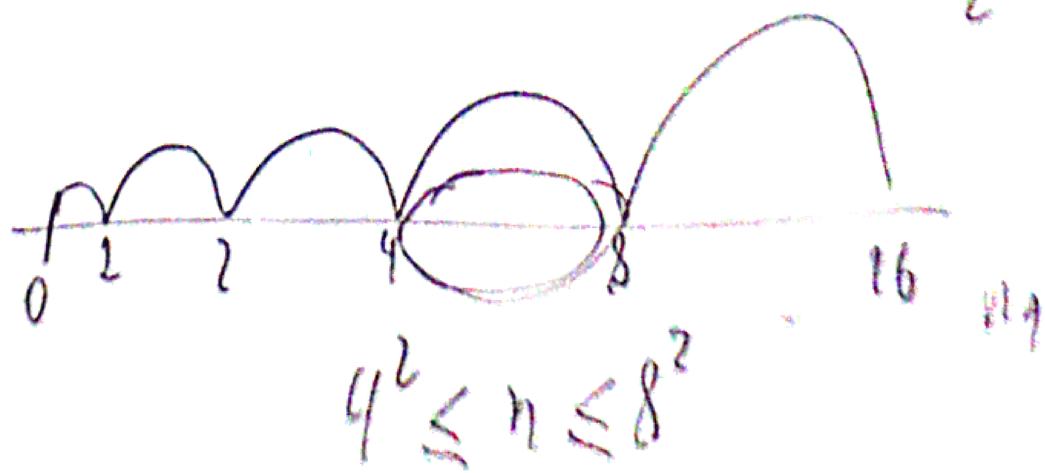
$a \in \mathbb{Z}_n^*$ $\quad a^{\frac{n-1}{2}} \equiv -1 \mod n$

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

(1) $c \equiv a \mod n_1$, $n = a^b$

(2) $c \equiv 1 \mod n_2$

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



$4^2 \leq n \leq 8^2$

n es primo

if neg = 0 then return COMP

$b_1 \dots b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

$Pr(A \cap B) \leq Pr(A)$

$Pr(A_1 \cap A_2)$

$= Pr(A_1) \cdot Pr(A_2)$

n es compuesto

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

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

① $c \equiv a \bmod n_1$ $\quad n = a^b$

② $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$

$4^2 \leq n \leq 8^2$

n es primo

if rng = 0 then return COMP

$b_1, \dots, b_k$

$\hookrightarrow \left(\frac{1}{2}\right)^k$

$Pr(A \cap B) \leq Pr(A)$

$Pr(A_1 \cap A_2)$

---

n es compuesto $= Pr(A_1) \cdot Pr(A_2)$

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$

$Pr(A \cap B) = Pr(A|B) \cdot Pr(B)$

n es primo

if neg = 0 then return COMP

$(b_1, \dots, b_k)$

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

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

(1) $c \equiv a \bmod n_1$

(2) $c \equiv 1 \bmod n_2$

$n = a^b$

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

$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$

$= \underbrace{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{(3)} \cdot Pr(MCD(a_i, n) = 1)$

(4) $Pr(B^2)$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$$Pr\left(MCD(a_i, n) = 1 \wedge \left(b_i \equiv \pm 1 \bmod n \right) \right)$$

$$= \underbrace{Pr\left(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1 \right)} \cdot Pr\left(MCD(a_i, n) = 1 \right)$$

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

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

(3) $\cdot Pr(B^2)$

14

α^{-12}

n es primo

if $neg = 0$ then return COMP

$b_1, \dots, b_k$

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

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

(1) $c \equiv a \bmod n_1$

(2) $c \equiv 1 \bmod n_2$

$n = a^b$

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

$$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$$

$$= \underbrace{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{(3)} \cdot Pr(MCD(a_i, n) = 1)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\quad) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

$(3) \cdot Pr(B^2)$

14

α^{-17}

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$$Pr\left(MCD(a_i, n) = 1 \wedge \left(b_i \equiv \pm 1 \bmod n \right) \right)$$

$$= \underbrace{Pr\left(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1 \right)} \cdot Pr\left(MCD(a_i, n) = 1 \right)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\ ) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

(3) $\cdot Pr(B^2)$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

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

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

① $c \equiv a \bmod n_1$ $\quad n = a^b$

② $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$

$$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$$

$$= \underbrace{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{} \cdot Pr(MCD(a_i, n) = 1) \quad \text{③} \cdot Pr(B^2)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\ ) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

14

α 14

n es primo

if $neg = 0$ then return COMP

$b_1, \dots, b_k$

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

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

(1) $c \equiv a \bmod n_1$

(2) $c \equiv 1 \bmod n_2$

$n = a^b$

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

$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$

$= \underline{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)} \cdot Pr(MCD(a_i, n) = 1)$ (3) $\cdot Pr(B^2)$

$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\quad) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$P_r(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$

$= \underbrace{Pr(b_n \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{} \cdot Pr(MCD(a_i, n) = 1)$

$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\ ) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

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

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

① $c \equiv a \bmod n_1$ $\quad n = a^b$

② $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

③ $\cdot Pr(B^2)$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$$Pr\left(MCD(a_i, n) = 1 \wedge \left(b_i \equiv \pm 1 \bmod n \right) \right)$$

$$= \underbrace{Pr\left(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1 \right)} \cdot Pr\left(MCD(a_i, n) = 1 \right)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\ ) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

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

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

(1) $c \equiv a \bmod n_1$ $\quad n = a^b$

(2) $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2} |\mathbb{Z}_n^*|$

(4) $P(a) \cdot (3) \cdot Pr(B^2)$

19

α^{12}

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

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

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

① $c \equiv a \bmod n_1$ $\quad n = a^b$

② $c \equiv 1 \bmod n_2$ $\quad |S_n| \leq \frac{1}{2}|\mathbb{Z}_n^*|$

$$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$$

$$= \underbrace{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{} \cdot Pr(MCD(a_i, n) = 1) \quad \text{③} \cdot Pr(B^2)$$

$$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\ ) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$$

n es primo

if neg = 0 then return COMP

$b_1, \dots, b_k$

$Pr(MCD(a_i, n) = 1 \wedge (b_i \equiv \pm 1 \bmod n))$

$= \underbrace{Pr(b_i \equiv \pm 1 \bmod n \mid MCD(a_i, n) = 1)}_{\leq \frac{1}{2}} \cdot Pr(MCD(a_i, n) = 1)$

$= \frac{|S_n|}{|\mathbb{Z}_n^*|} \cdot (\quad) \leq \frac{|S_n|}{|\mathbb{Z}_n^*|} \leq \frac{1}{2}$

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

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

(1) $c \equiv a \bmod n_1$

(2) $c \equiv 1 \bmod n_2$

$n = a^b$

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

(1) $P(a)$

(2) $P(a^2)$

(3) $P(B^2)$