n impar

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

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

n jumpoz

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

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

n impar

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

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

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

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

$$a = 1$$

$$a - 1 = 0$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$a^2 = 1 \qquad x \cdot y = 0$$
$$a^2 - 1 = 0$$
$$(a-1)(a+1) = 0$$

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$a^2 = 1 \qquad x \cdot y = 0$$

$$x \cdot y \equiv 0 \bmod 15$$

$$a^2 - 1 = 0$$

$$(a-1)(a+1) = 0$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$a^2 = 1 \qquad X \cdot y = 0$$

$$X \cdot y \equiv 0 \bmod 15$$

$$a^2 - 1 = 0$$

$$5 \cdot 3 \equiv 0 \bmod 15$$

$$(a-1)(a+1) = 0$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$a^2 = 1 \qquad x \cdot y = 0$$

$$a^2 - 1 = 0$$

$$(a-1)(a+1) = 0$$

$$x \cdot y \equiv 0 \bmod 15$$

$$5 \cdot 3 \equiv 0 \bmod 15$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$$x \cdot y \equiv 0 \bmod 15$$
$$5 \cdot 3 \equiv 0 \bmod 15$$

$$a^{n-1} \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$$
$$\underbrace{\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right)}_{} \equiv 0 \bmod n$$

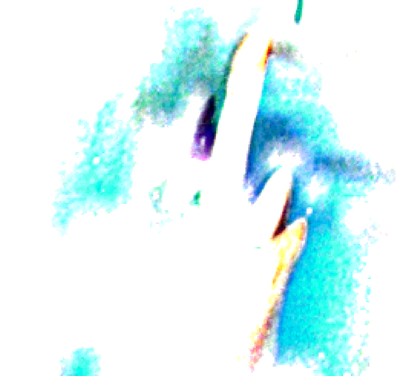
$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$$x \cdot y \equiv 0 \bmod 11$$

$$a^{n-1} \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$$
$$\underbrace{\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right)}_{} \equiv 0 \bmod n$$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$$x \cdot y \equiv 0 \bmod 11$$



$$a^{n-1} \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$$
$$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$$
$$\underbrace{\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right)}_{} \equiv 0 \bmod n$$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$91 \mid 5 \cdot 3$

$x \cdot y \equiv 0 \bmod 11$

$11 \mid (x \cdot y - 0) \Big) \rightarrow 11 \mid x \cdot y$

$c \cdot 11 = x \cdot y$

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

$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$

$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$

$\underbrace{\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right)}_{} \equiv 0 \bmod n$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

9S | S.3

$x \cdot y \equiv 0 \bmod p$

$x \not\equiv 0 \bmod p$

$x \cdot a \equiv 1 \bmod p$

$a \cdot x \cdot y \equiv a \cdot 0 \bmod p$

$1 \cdot y \equiv 0 \bmod p$

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

$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$

$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$

$\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right) \equiv 0 \bmod n$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$91 \mid 5 \cdot 3$

$x \cdot y \equiv 0 \bmod p$

$x \neq 0 \bmod p$

$x \cdot a \equiv 1 \bmod p$

$a \cdot x \cdot y \equiv a \cdot 0 \bmod p$

$1 \cdot y \equiv 0 \bmod p$

$y \equiv 0 \bmod p$

$x \cdot y = 0$

$\frac{1}{x}$

$\frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0$

$y = 0$

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

$\left(a^{\frac{n-1}{2}}\right)^2 \equiv 1 \bmod n$

$\left(a^{\frac{n-1}{2}}\right)^2 - 1 \equiv 0 \bmod n$

$\left(a^{\frac{n-1}{2}} - 1\right)\left(a^{\frac{n-1}{2}} + 1\right) \equiv 0 \bmod n$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$ $\quad \mathbb{Z}_n^* = S_n$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$x \cdot y \equiv 0 \bmod p$

$x \neq 0 \bmod p$

$x \cdot a \equiv 1 \bmod p$

$a \cdot x \cdot y \equiv a \cdot 0 \bmod p$

1

$x \cdot y = 0$

$\frac{1}{x}$

$\frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0$

$y = 0$

2

$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$x \cdot y \equiv 0 \bmod p$

$x \not\equiv 0 \bmod p$

$x \cdot a \equiv 1 \bmod p$

$a \cdot x \cdot y \equiv a \cdot 0 \bmod p$

$1 \cdot y \equiv 0 \bmod p$

$y \equiv 0 \bmod p$

$x \cdot y = 0$

$\frac{1}{x}$

$\frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0$

$1 \cdot y = 0$

$y = 0$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

$$|S_n^+| \leq \frac{n-1}{2}$$

$X \cdot y \equiv 0 \bmod p$

$X \not\equiv 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot (X \cdot y) \equiv a \cdot 0 \bmod p$

1

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$a, b \in S_n^+ \Rightarrow a \cdot b \in S_n^+$

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

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

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

$X \cdot y \equiv 0 \bmod p$

$X \not\equiv 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot X \cdot y \equiv a \cdot 0 \bmod p$

$1 \qquad\qquad 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$a, b \in S_n^+ \Rightarrow a \cdot b \in S_n^+$

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

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

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

$X \cdot y \equiv 0 \bmod p$

$X \not\equiv 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$(a \cdot X)\, y \equiv a \cdot 0 \bmod p$

$1 \qquad 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$a, b \in S_n^+ \Rightarrow a \cdot b \in S_n^+$

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

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

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

$1 \quad 1$

$X \cdot y \equiv 0 \bmod p$

$X \not\equiv 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$(a \cdot X)\, y \equiv a \cdot 0 \bmod p$

$1 \quad 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$X \cdot y \equiv 0 \bmod p$

$X \neq 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot X \cdot y \equiv a \cdot 0 \bmod p$

$1 \qquad 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$ $\quad \frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq$

$X \cdot y \equiv 0 \bmod p$

$X \neq 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot X \cdot y \equiv a \cdot 0 \bmod p$

$1 \quad 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$X \cdot y \equiv 0 \bmod p$

$X \neq 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot X \cdot y \equiv a \cdot 0 \bmod p$

$1 \quad \rightarrow 0$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X \cdot y \equiv 0 \bmod p$

$X \not\equiv 0 \bmod p$

$X \cdot a \equiv 1 \bmod p$

$a \cdot X \cdot y \equiv a \cdot 0 \bmod p$

1

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$p(X) =$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$x^2 - 3 \equiv 0 \bmod 11$

$p(x) \equiv 0 \bmod n$

$p(x) = x^{\frac{n-1}{2}} - 1$

5 $\quad (-5) \rightarrow 6$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(x) = x^{\frac{n-1}{2}} + 1$

$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$x^2 - 3 \equiv 0 \bmod 11$

$(x-5)(x-6) \equiv 0 \bmod 11$

$x^2 - 2 \equiv 0$

$p(x) \equiv 0 \bmod n$

$p(x) = x^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$p(x) = x^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$x^2 - 3 \equiv 0 \bmod 11$

$(x-5)(x-6) \equiv 0 \bmod 11$

$x^2 - 2 \equiv 0 \bmod 11$

$P(x) \equiv 0 \bmod n$

$P(x) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(x) = X^{\frac{n-1}{2}} + 1$

$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$x^2 - 3 \equiv 0 \bmod 11$

$(x-5)(x-6) \equiv 0 \bmod 11$

$x^2 - 2 \equiv 0 \bmod 11$

$a^2 \equiv 2 \bmod 11$

$p(x) \equiv 0 \bmod n$

$p(x) = x^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(x) = x^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$Q(X) = X^{\frac{n-1}{2}} + 1$

$X^2 - 3 \equiv 0 \bmod 11$

$(X-5)(X-6) \equiv 0 \bmod 11$

$X^2 - 2 \equiv 0 \bmod 11$

$a^2 \equiv 2 \bmod 11$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$p(X)$ $\qquad p(a) = 0$

$p(X) = (X-a) \cdot q(X)$

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$p(X)$ $\qquad p(a) = 0$

$p(X) = (X-a) \cdot q(X)$

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \iff a \in S_n^+$

$ax^2 + bx + c = (x - r_1) \cdot q(x)$

$|S_n^-| \leq \frac{n-1}{2}$

$q(x) = X^{\frac{n-1}{2}} + 1$

$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$p(X)$ $\qquad p(a) = 0$

$p(X) = (X-a) \cdot q(X)$

$ax^2 + bx + c = (X - \dots) \cdot q(X)$

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$(X-2)(X+2)$

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$R(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$$\mathbb{Z}_n^* = S_n \qquad \frac{n-1}{2}$$

$$|S_n^+| \leq \frac{n-1}{2} \qquad n = 4k+3 \qquad \frac{n-1}{2} = 2k+1$$

$$X^2 - 4 \equiv 0 \bmod 15$$

$$(X-2)(X+2) \equiv 0 \bmod 15$$

$$P(X) \equiv 0 \bmod n$$

$$P(X) = X^{\frac{n-1}{2}} - 1$$

$$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$$

$$|S_n^-| \leq \frac{n-1}{2}$$

$$P(X) = X^{\frac{n-1}{2}} + 1$$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

3 5

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5 9 $\qquad X = 7$

$X = 8$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \iff a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$$\mathbb{Z}_n^* = S_n \qquad \frac{n-1}{2}$$

$$|S_n^+| \leq \frac{n-1}{2} \qquad n = 4k+3 \qquad \frac{n-1}{2} = 2k+1$$

$$X^2 - 4 \equiv 0 \bmod 15$$

$$(X-2)(X+2) \equiv 0 \bmod 15$$

5	9	$X = 7$
6	10	$X = 8$

$$p(X) \equiv 0 \bmod n$$

$$p(X) = X^{\frac{n-1}{2}} - 1$$

$$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$$

$$|S_n^-| \leq \frac{n-1}{2}$$

$$p(X) = X^{\frac{n-1}{2}} + 1$$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = 2k+1$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5	9	$X = 7$
6	10	$X = 8$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$\mathbb{Z}_n^* = S_n$ $\qquad \frac{n-1}{2}$

$|S_n^+| \leq \frac{n-1}{2}$ $\qquad n = 4k+3$

$\frac{n-1}{2} = 2k+1$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5 9 $\quad X = 7$

6 10 $\quad X = 8$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(x) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

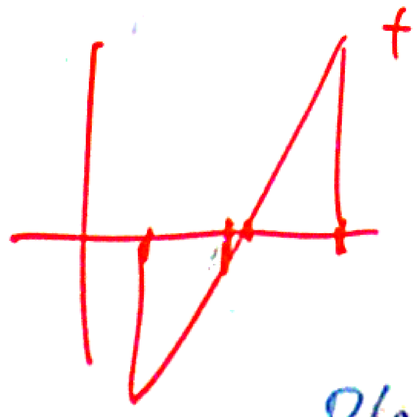
$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5	9	$X = 7$
6	10	$X = 8$



$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

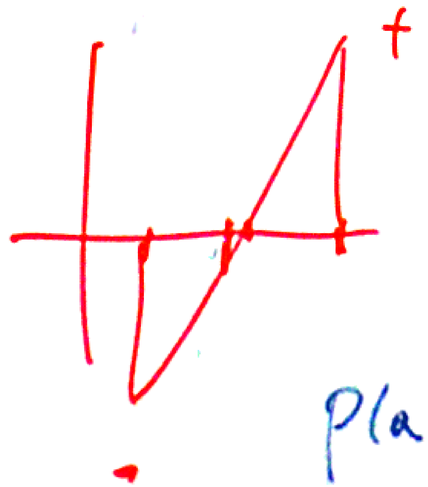
$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5	9	$X = 7$
6	10	$X = 8$



$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$R(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

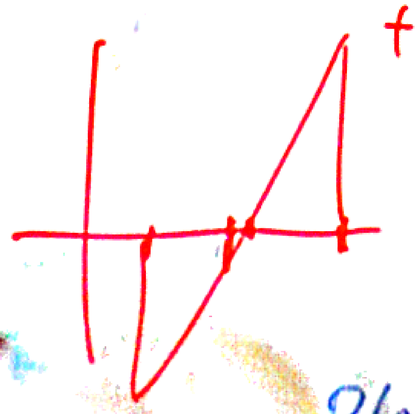
$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5 9

6 10



$X = 7$

$X = 8$

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(x) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

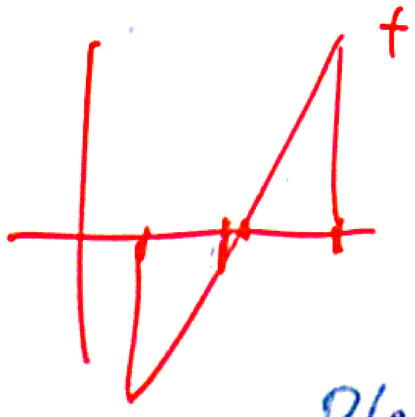
$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5 9 $\quad X = 7$

6 10 $\quad X = 8$



$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5	9	$X = 7$
6	10	$X = 8$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$Q(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

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

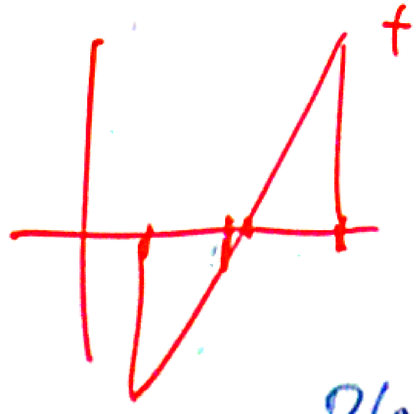
$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$X^2 - 4 \equiv 0 \bmod 15$

$(X-2)(X+2) \equiv 0 \bmod 15$

5	9	$X = 7$
6	10	$X = 8$



$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(x) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$ $\quad \frac{n-1}{2} = 2k+1$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ e \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$ $\quad \frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

$|S_n^+| \leq \frac{n-1}{2}$

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

$n = 4k+3$

$\frac{n-1}{2} = 2k+1$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Rightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$P(X) = X^{\frac{n-1}{2}} + 1$

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$$|S_n^+| \leq \frac{n-1}{2}$$

$$|S_n^-| \leq \frac{n-1}{2}$$

$$|S_n| = |S_n^+| + |S_n^-|$$

$$|\mathbb{Z}_n^*| = n-1$$

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

$$|S_n^+| \leq \frac{n-1}{2}$$

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

$n = 4k+3$

$\frac{n-1}{2} = 2k+1$

$$p(x) \equiv 0 \bmod n$$

$$p(x) = x^{\frac{n-1}{2}} - 1$$

$p(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$$|S_n^-| \leq \frac{n-1}{2}$$

$$p(x) = x^{\frac{n-1}{2}} + 1$$

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

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

$|S_n^+| \leq \frac{n-1}{2}$ $\quad n = 4k+3$

$\frac{n-1}{2} = (2k+1)$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$Q(X) = X^{\frac{n-1}{2}} + 1$

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

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

$|S_n^+| \leq \frac{n-1}{2}$

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

$n = 4k+3$

$\frac{n-1}{2} = 2k+1$

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

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

$p(X) \equiv 0 \bmod n$

$p(X) = X^{\frac{n-1}{2}} - 1$

$p(a) \equiv 0 \bmod n \Leftrightarrow a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$q(X) = X^{\frac{n-1}{2}} + 1$

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

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

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

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

$|S_n^+| \leq \frac{n-1}{2}$

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

$n = 4k+3$

$\frac{n-1}{2} = 2k+1$

$P(X) \equiv 0 \bmod n$

$P(X) = X^{\frac{n-1}{2}} - 1$

$P(a) \equiv 0 \bmod n \iff a \in S_n^+$

$|S_n^-| \leq \frac{n-1}{2}$

$Q(X) = X^{\frac{n-1}{2}} + 1$

$$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

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

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

$$|S_n^+| \leq \frac{n-1}{2}$$
$$|S_n^-| \leq \frac{n-1}{2}$$

$$|S_n| = |S_n^+| + |S_n^-| .$$

$$|\mathbb{Z}_n^*| = n-1$$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

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

$n = a^b \qquad b \geq 2$

$36 = 6^2$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

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

$n = a^b \qquad b \geq 2$

$n = a^2$

$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

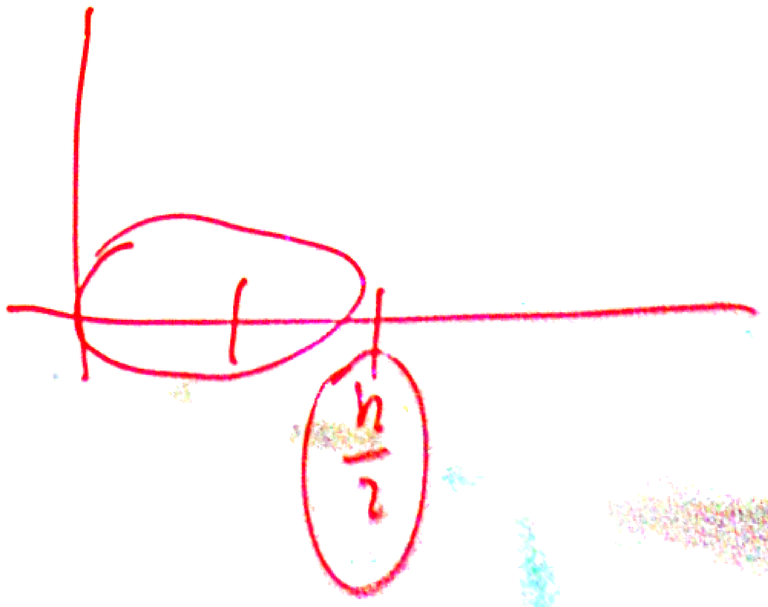
$|\mathbb{Z}_n^*| = n-1$

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

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

$n = a^b \qquad b \geq 2$

$n = a^2$



$S_n^+ = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

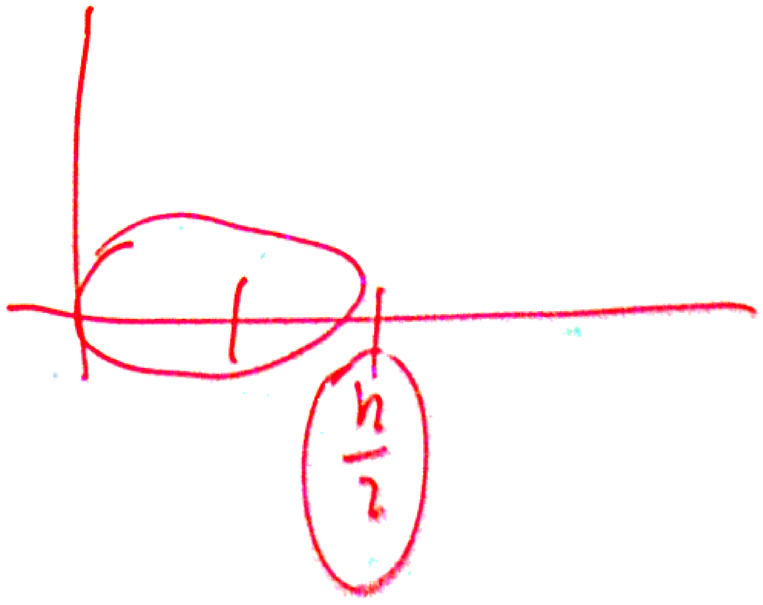
$|\mathbb{Z}_n^*| = n-1$

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

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

$n = a^b \qquad b \geq 2$

$n = a^2$



$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

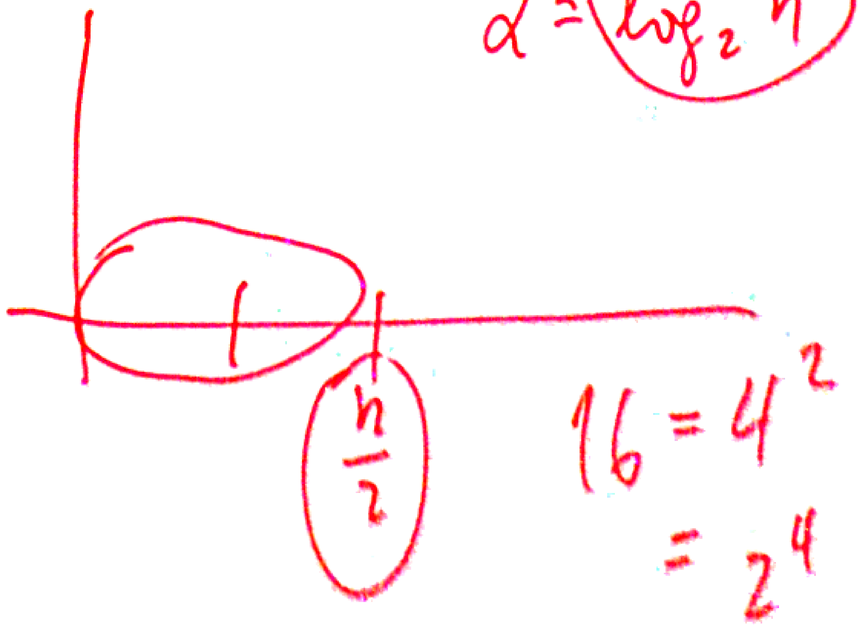
$a^{\frac{n-1}{2}} \bmod n$

$n = a^b \qquad b \geq 2$

$n = a^2$

$n = 2^d$

$d = \log_2 n$



$16 = 4^2$

$= 2^4$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$.

$|\mathbb{Z}_n^*| = n-1$

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

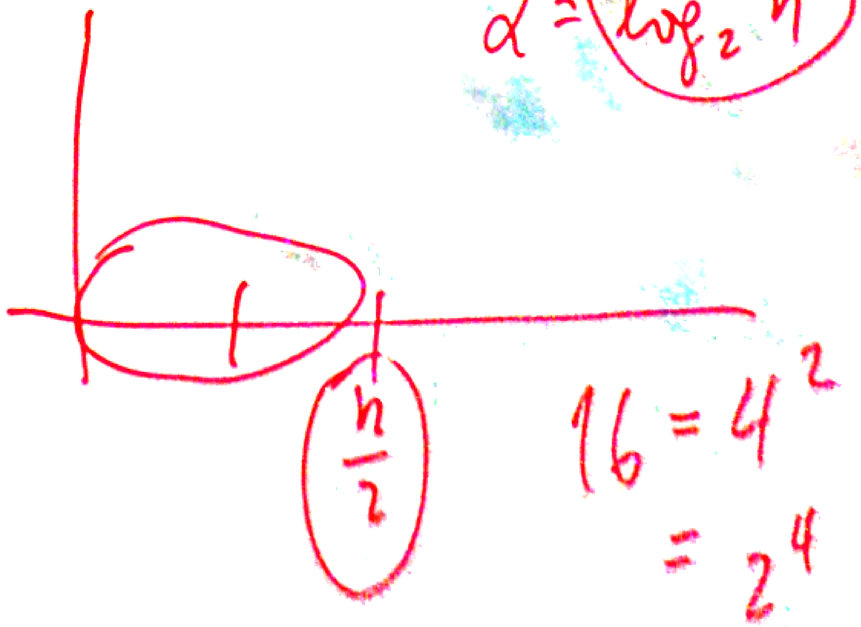
$a^{\frac{n-1}{2}} \bmod n$

$n = a^b \qquad b \geq 2$

$n = a^2$

$n = 2^d$

$d = \log_2 n$



$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

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

$n = a^b \quad b \geq 2$

$n = a^2$

$n = n_1 \cdot n_2 \quad MCD(n_1, n_2) = 1$

$n_1 \geq 3, \; n_2 \geq 3$

$36 = 6^2 = 2^3 \cdot 3^2$

$= 2^4$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

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

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

---

n es compuesto

$- 2^4$

$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$

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

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

$|S_n^+| \leq \frac{n-1}{2}$

$|S_n^-| \leq \frac{n-1}{2}$

$|S_n| = |S_n^+| + |S_n^-|$

$|\mathbb{Z}_n^*| = n-1$

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

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

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2} \qquad |S_n^-| = \frac{n-1}{2}$

---

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

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

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

$$|S_n^+| \leq \frac{n-1}{2}$$

$$|S_n^-| \leq \frac{n-1}{2}$$

$$|S_n| = |S_n^+| + |S_n^-|$$

$$|\mathbb{Z}_n^*| = n-1$$

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

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

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto :

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{100} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{100}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$\bar{S}_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

$$S_n = S_n^+ \cup \bar{S}_n$$

$a_1, \dots, a_{100} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{100}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |\bar{S}_n| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{100} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{100}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$\bar{S}_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

$$S_n = S_n^+ \cup \bar{S}_n$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |\bar{S}_n| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

n primo

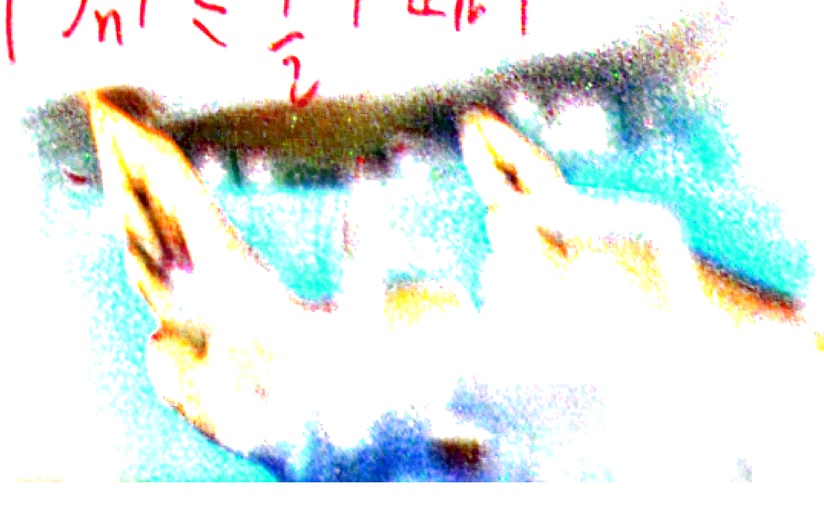
$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2} \qquad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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



$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2} \qquad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

$b_i = a_i^{\frac{n-1}{2}} \bmod n$ X

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $|S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

X

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$\bar{S}_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

$$S_n = S_n^+ \cup \bar{S}_n$$

$a_1, \ldots, a_{1000} \in \{1, \ldots, n-1\}$

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

$b_1, \ldots, b_{1000}$

X

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |\bar{S}_n| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$

$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$

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

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

X

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

X

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

$b_i = a_i^{\frac{n-1}{2}} \bmod n$ X

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $|S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

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

$b_1, \dots, b_{1000}$

X

n primo

$|S_n'| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $\quad |S_n^-| = \frac{n-1}{2}$

n es compuesto:

$\exists a : a^{\frac{n-1}{2}} \not\equiv -1 \bmod n$

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

$$S_n = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

$b_i = a_i^{\frac{n-1}{2}} \bmod n$ X

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $|S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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

$$S_n' = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv 1 \bmod n \}$$
$$S_n^- = \{ a \in \mathbb{Z}_n^* \;/\; a^{\frac{n-1}{2}} \equiv -1 \bmod n \}$$
$$S_n = S_n^+ \cup S_n^-$$

$a_1, \dots, a_{1000} \in \{1, \dots, n-1\}$

$b_i = a_i^{\frac{n-1}{2}} \bmod n$ X

$b_1, \dots, b_{1000}$

n primo

$|S_n| = n-1$

$|S_n^+| = \frac{n-1}{2}$ $|S_n^-| = \frac{n-1}{2}$

n es compuesto:

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

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