



n

/

t

100

12

13

14

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

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

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

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

$\beta$

$\beta_2$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$a = 1$$

$$a - 1 = 0$$

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

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

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

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

$$a^2 = 1$$

$$a^2 - 1 = 0$$

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

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

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

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

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

$$x \cdot y \equiv 0 \pmod{15}$$

$$a^2 = 1$$

$$a^2 - 1 = 0$$

$$x \cdot y = 0$$

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

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

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

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

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

$$x \cdot y \equiv 0 \pmod{15}$$

$$a^2 = 1$$

$$x \cdot y = 0$$

$$a^2 - 1 = 0$$

$$x \cdot y \equiv 0 \pmod{15}$$

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

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

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

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

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

$$x \cdot y \equiv 0 \pmod{15}$$

$$a^2 = 1$$

$$a^2 - 1 = 0$$

$$x \cdot y = 0$$

$$5 \cdot 3 \equiv 0 \pmod{15}$$

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

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

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

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

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

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

$$(a^{\frac{n-1}{2}})^2 - 1 \equiv 0 \pmod{n}$$

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

$$x \cdot y \equiv 0 \pmod{15}$$

$$5 \cdot 3 \equiv 0 \pmod{15}$$

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

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

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

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

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

$$(a^{\frac{n-1}{2}})^2 - 1 \not\equiv 0 \pmod{n}$$

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

$$x \cdot y \equiv 0 \pmod{n}$$

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

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

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

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

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

$$(a^{\frac{n-1}{2}})^2 - 1 \not\equiv 0 \pmod{n}$$

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

$$x \cdot y \equiv 0 \pmod{n}$$

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

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

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

95 | 5 · 3

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

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

$$x \cdot y \equiv 0 \pmod{11}$$

$$(a^{\frac{n-1}{2}})^2 - 1 \not\equiv 0 \pmod{n}$$

$$\begin{aligned} 11 | (x \cdot y - 0) \\ c \cdot 11 \equiv x \cdot y \end{aligned} \quad \rightarrow \quad 11 | x \cdot y$$

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

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

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

$$S_n = S_n^+ \cup S_n^- \quad 9S1 S.3$$

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

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

$$(a^{\frac{n-1}{2}})^2 - 1 \equiv 0 \pmod{n}$$

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

$x \cdot y \equiv 0 \pmod{p}$   
 $x \not\equiv 0 \pmod{p}$   
 $x \cdot a \equiv 1 \pmod{p}$   
 $\cancel{(a/x)y} \equiv a \cdot 0 \pmod{p}$   
 1

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

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

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

TS 1.5.3

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

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

$$(a^{\frac{n-1}{2}})^2 - 1 \equiv 0 \pmod{n}$$

$$\begin{cases} x \cdot y = 0 \\ \frac{1}{x} \\ \frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0 \\ y = 0 \end{cases}$$

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

$$\begin{aligned} & x \cdot y \equiv 0 \pmod{p} \\ & x \neq 0 \pmod{p} \\ & x \cdot a \equiv 1 \pmod{p} \\ & (a/x)y \equiv a \cdot 0 \pmod{p} \\ & 1 \end{aligned}$$

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

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

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

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

$\dots \subset$

$x \cdot y \equiv 0 \pmod{p}$

$x \not\equiv 0 \pmod{p}$

$x \cdot a \equiv 1 \pmod{p}$

$(a/x)y \equiv a \cdot 0 \pmod{p}$

1

$$\begin{cases} x \cdot y = 0 \\ x \neq 0 \\ \frac{1}{x} \cdot x \cdot y = \frac{1}{x} \cdot 0 \\ y = 0 \end{cases}$$

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

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

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

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

$\dots \subset$

$X \cdot y \equiv 0 \pmod{p}$

$X \not\equiv 0 \pmod{p}$

$X \cdot a \equiv 1 \pmod{p}$

$(a/X)y \equiv a \cdot 0 \pmod{p}$

$1$

$$\begin{aligned} X \cdot y &= 0 \\ \frac{1}{X} \\ \frac{1}{X} \cdot X \cdot y &= \frac{1}{X} \cdot 0 \\ y &= 0 \end{aligned}$$

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

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

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

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

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

$$x \cdot y \equiv 0 \pmod{p}$$

$$x \not\equiv 0 \pmod{p}$$

$$x \cdot a \equiv 1 \pmod{p}$$

$$(a/x)y \equiv a \cdot 0 \pmod{p}$$

1

$$\begin{aligned} S_n^+ &= \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv 1 \pmod{n}\} \\ S_n^- &= \{a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n}\} \\ n &= S_n^+ \cup S_n^- \end{aligned}$$

$$z_n^* = s_n$$

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

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

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

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

a.  $b^{\frac{n-1}{3}}$  is 1 mod n

$x \cdot y \equiv 0 \pmod{p}$

$x \not\equiv 0 \pmod{p}$

$x \cdot a \equiv 1 \pmod{p}$

~~$a(x)y \equiv a \cdot 0 \pmod{p}$~~

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

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

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

$$x \cdot y \equiv 0 \pmod{p}$$

$$x \not\equiv 0 \pmod{p}$$

$$x \cdot a \equiv 1 \pmod{p}$$

~~(a)~~  $x \cdot y \equiv a \cdot 0 \pmod{p}$

1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

\$x \cdot y \equiv 0 \pmod{p}\$

$x \not\equiv 0 \pmod{p}$

$x \cdot a \equiv 1 \pmod{p}$

$\cancel{(a \cdot x)}y \equiv a \cdot 0 \pmod{p}$

1

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

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

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

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

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

$$P(x) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

$x \cdot y \equiv 0 \pmod{p}$

$x \not\equiv 0 \pmod{p}$

$x \cdot a \equiv 1 \pmod{p}$

$\cancel{(a/x)}y \equiv x \cdot 0 \pmod{p}$

1

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

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

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

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

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

$n = 4k+3$   
 $\frac{n-1}{2} = \boxed{2k+1}$

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

$$|S_n^-| \leq$$

$$\begin{aligned} & X \cdot y \equiv 0 \pmod{p} \\ & X \not\equiv 0 \pmod{p} \\ & X \cdot a \equiv 1 \pmod{p} \\ \hookrightarrow & (a \cancel{\cdot} X) y \equiv a \cdot 0 \pmod{p} \\ & \downarrow 1 \end{aligned}$$

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

$x \cdot y \equiv 0 \pmod{p}$

$x \not\equiv 0 \pmod{p}$

$x \cdot a \equiv 1 \pmod{p}$

$\cancel{(a/x)}y \equiv x \cdot 0 \pmod{p}$

1

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

$$p(x) \equiv$$



$x \cdot y \equiv 0 \pmod{p}$   
 $x \not\equiv 0 \pmod{p}$   
 $x \cdot a \equiv 1 \pmod{p}$   
 $(a/x)y \equiv a \cdot 0 \pmod{p}$   
 ↓  
 1

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

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

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

$$x^2 - 3 \equiv 0 \pmod{11}$$

$$+ 5 \quad \textcircled{-5} \rightarrow 6$$

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

$$x^2 - 3 \equiv 0 \pmod{11}$$

$$(x-5)(x-6) \equiv 0 \pmod{11}$$

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 3 \equiv 0 \pmod{11}$$

$$(x-5)(x-6) \equiv 0 \pmod{11}$$

$$x^2 - 2 \equiv 0 \pmod{11}$$

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 3 \equiv 0 \pmod{11}$$

$$(x-5)(x-6) \equiv 0 \pmod{11}$$

$$x^2 - 2 \equiv 0 \pmod{11}$$

$$a^2 \equiv 2 \pmod{11}$$

2

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 3 \equiv 0 \pmod{11}$$

$$(x-5)(x-6) \equiv 0 \pmod{11}$$

$$x^2 - 2 \equiv 0 \pmod{11}$$

$$a^2 \equiv 2 \pmod{11}$$

∴

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

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

$$P(x) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$P(x)$$

$$P(a) = 0$$

$$P(x) = (x-a) \cdot Q(x)$$

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

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

$$P(x) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

$$Q(x) \in X^{\frac{n-1}{2}-1}$$

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

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

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

$$P(x) \quad P(a) = 0$$

$$P(x) = (x-a) \cdot q(x)$$

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

+

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

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

$$P(x) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$P(x) \quad P(a) = 0$$

$$P(x) = (x-a) \cdot Q(x)$$

$$ax^2 + bx + c = (x - \textcolor{blue}{a}) \cdot Q(x)$$

+

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

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

$$P(x) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

$$Q(x) \in X^{\frac{n-1}{2}-1}$$

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

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

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

$$(X-1)(X+1)$$

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

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

$$P(X) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

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

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

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

$$n = 4k+3$$

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

$$p(x) \in X^{n-2} + 1$$

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

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

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$3 \quad 5$$

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$5 \quad 9 \quad x=7$$

$$x=8$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} x=7 \\ x=8 \end{matrix}$$

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$X^2 - 4 \equiv 0 \pmod{15}$$

$$(X-2)(X+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad X=7$$

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

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

$$P(X) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

$$X^2 - 4 \equiv 0 \pmod{15}$$

$$(X-2)(X+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \\ 7 & \\ 8 & \end{matrix} \quad X=7 \\ X=8$$

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

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

$$P(X) \equiv 0 \pmod{n}$$

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

$$P(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

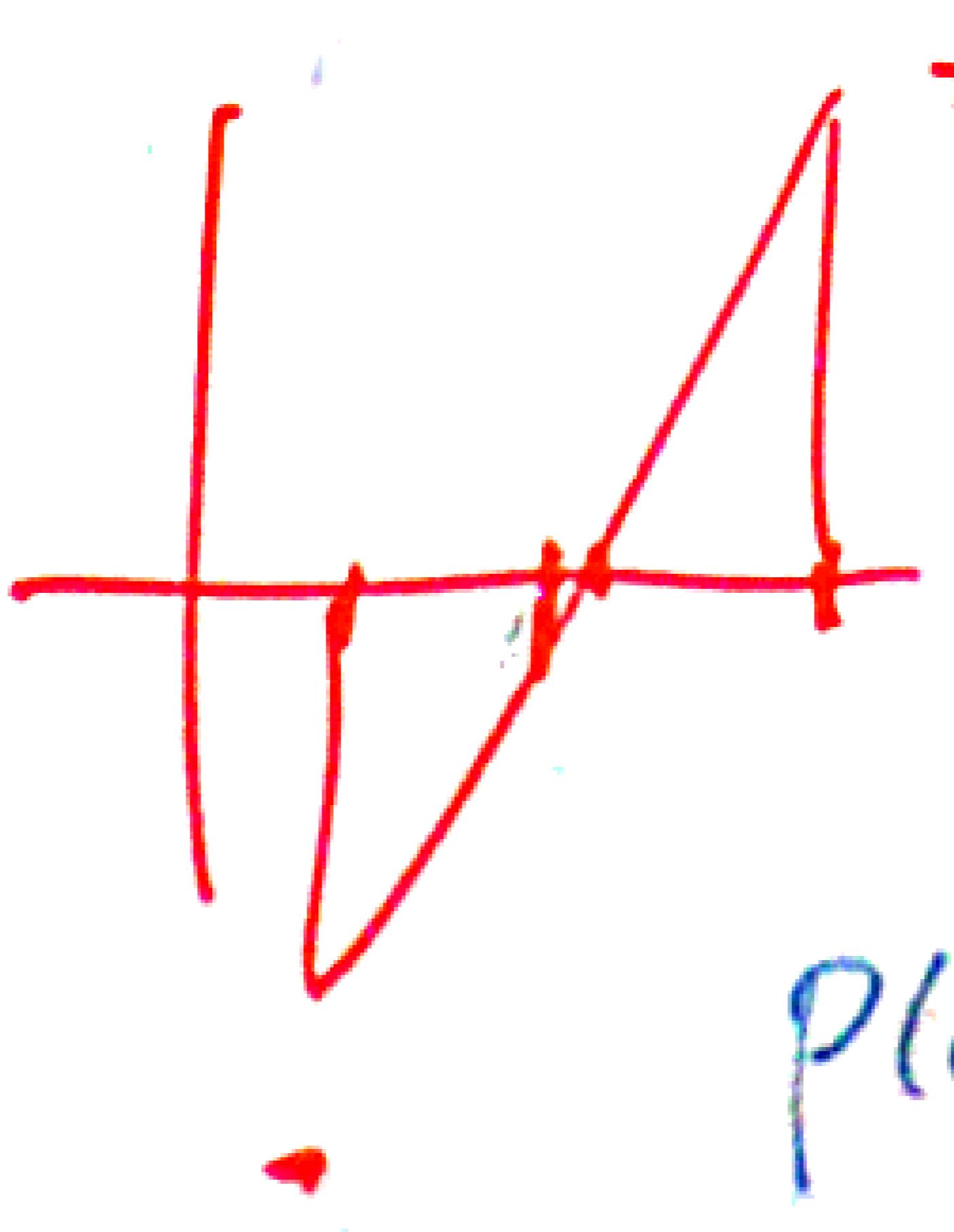
$$S_n^- = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \}$$

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} x=7 \\ x=8 \end{matrix}$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

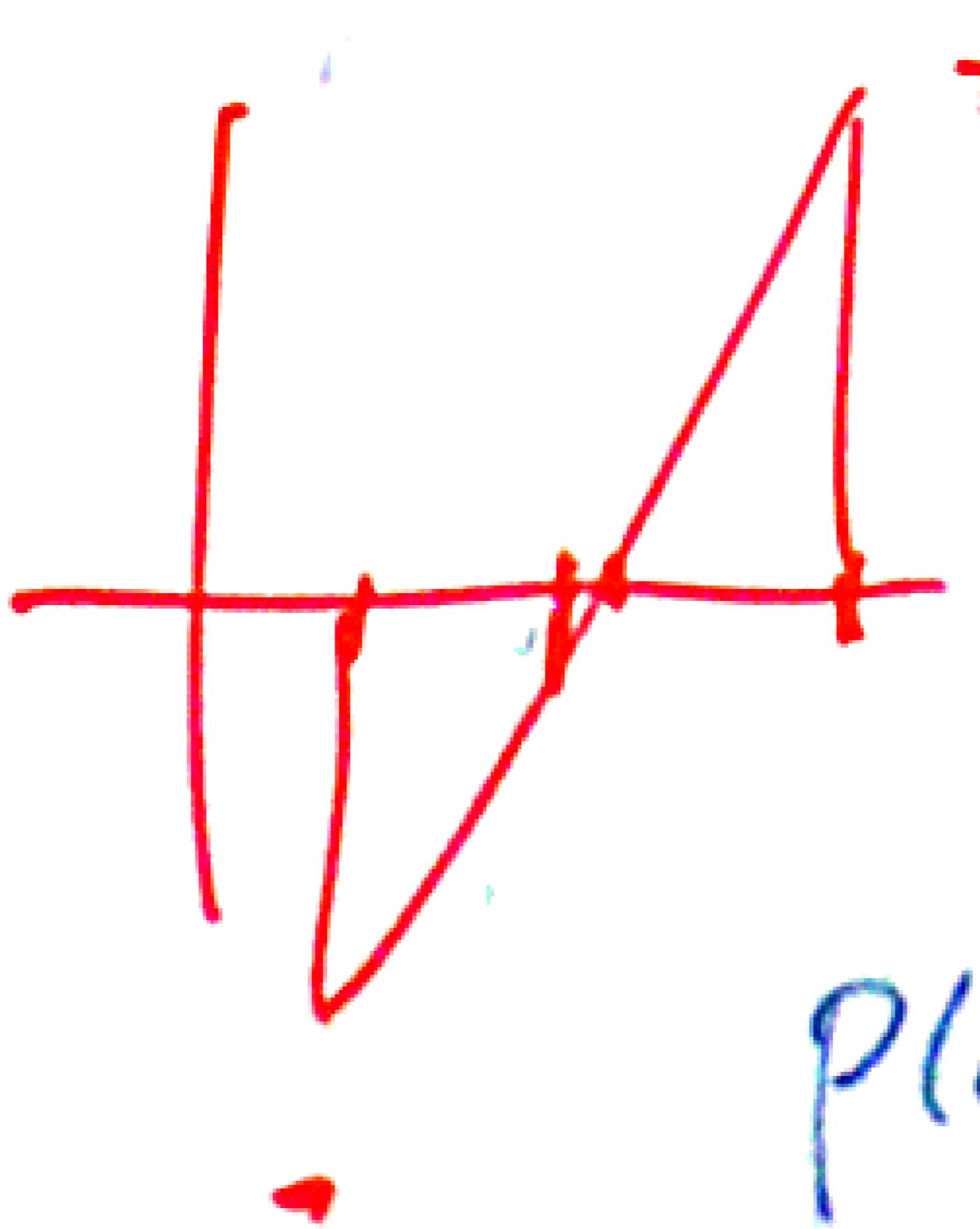
$$S_n^- = \left\{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \right\}$$

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} x=7 \\ x=8 \end{matrix}$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

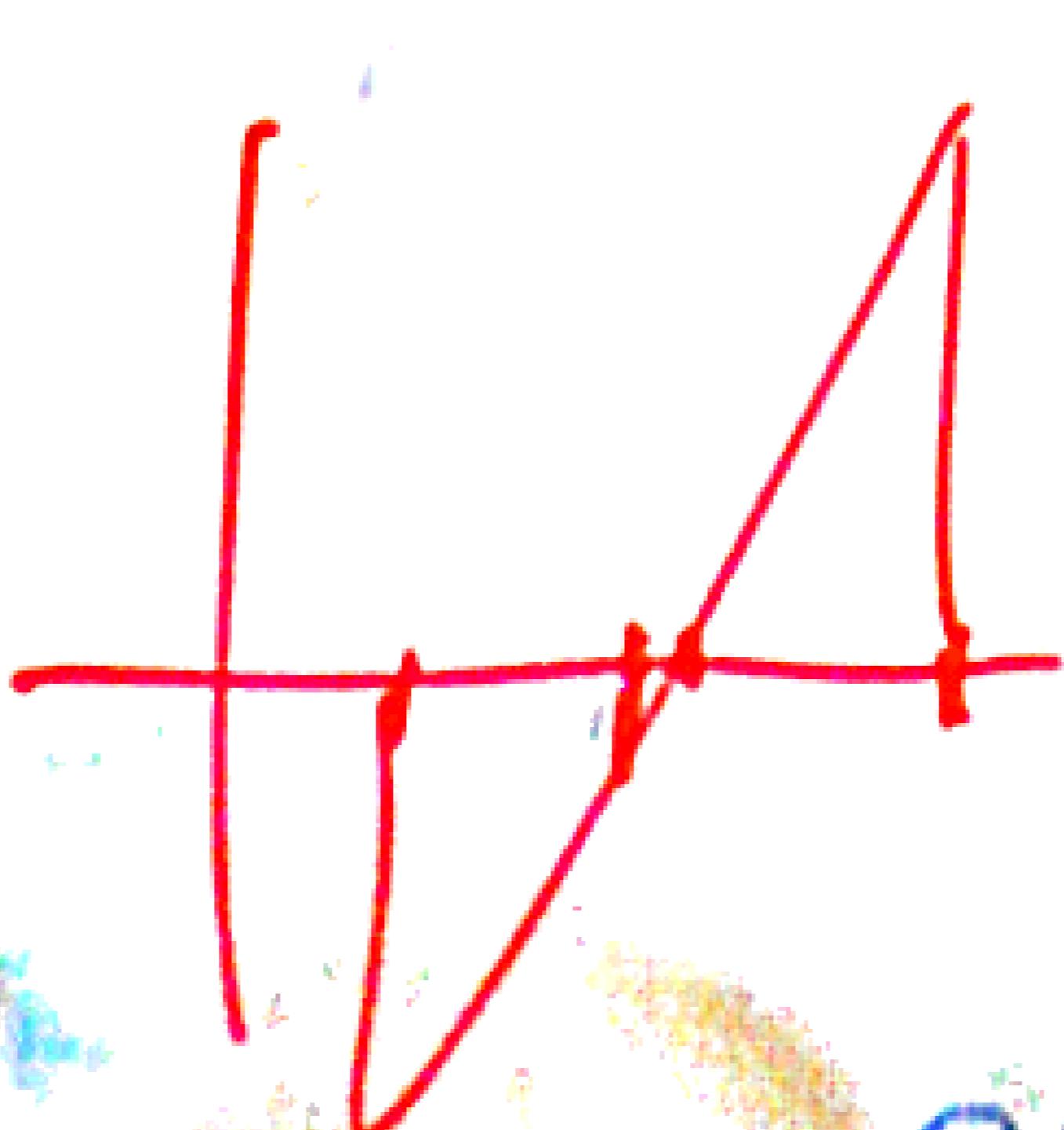
$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix}$$

$$x=7$$

$$x=8$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

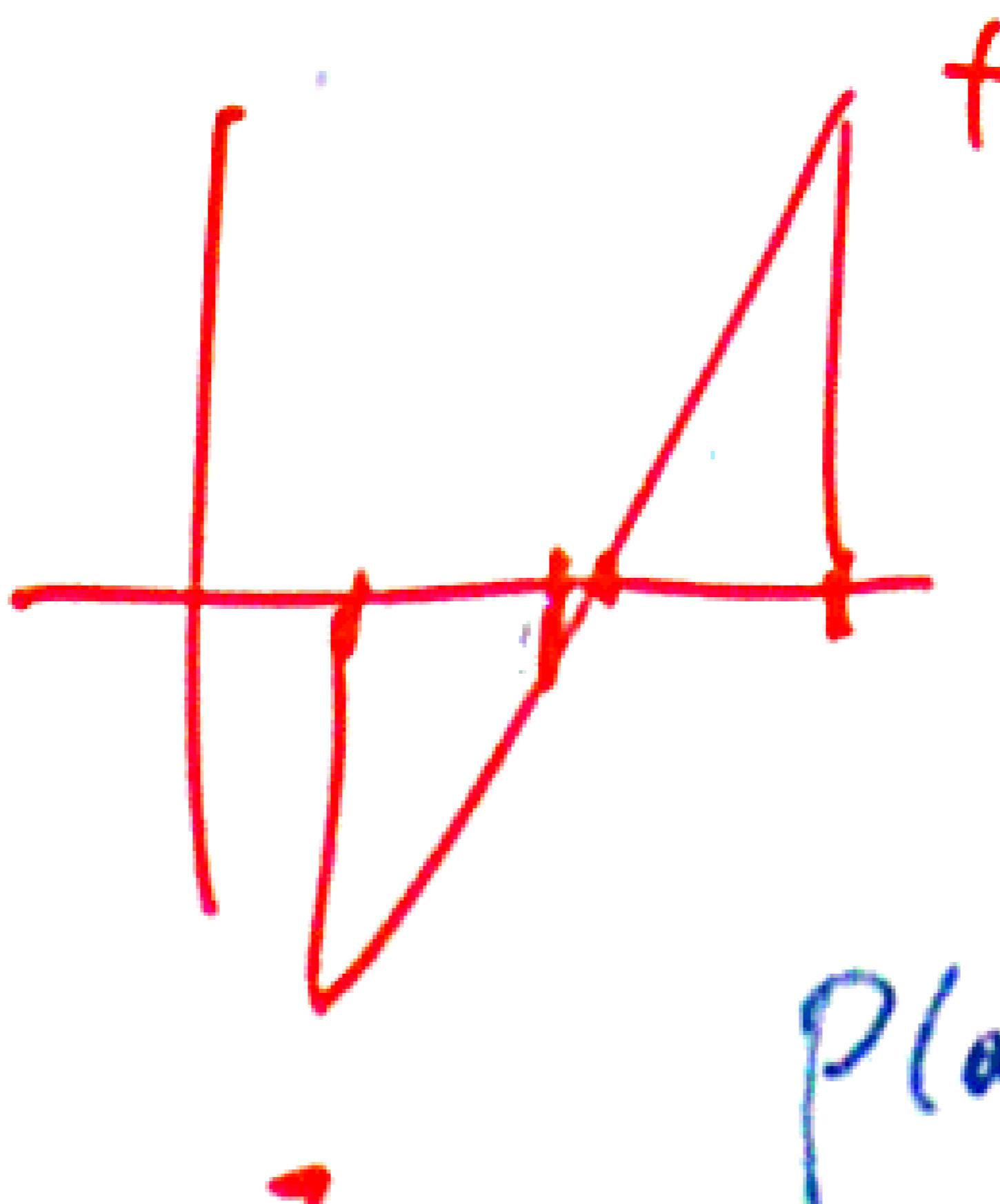
$$S_n^- = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \}$$

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} x=7 \\ x=8 \end{matrix}$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

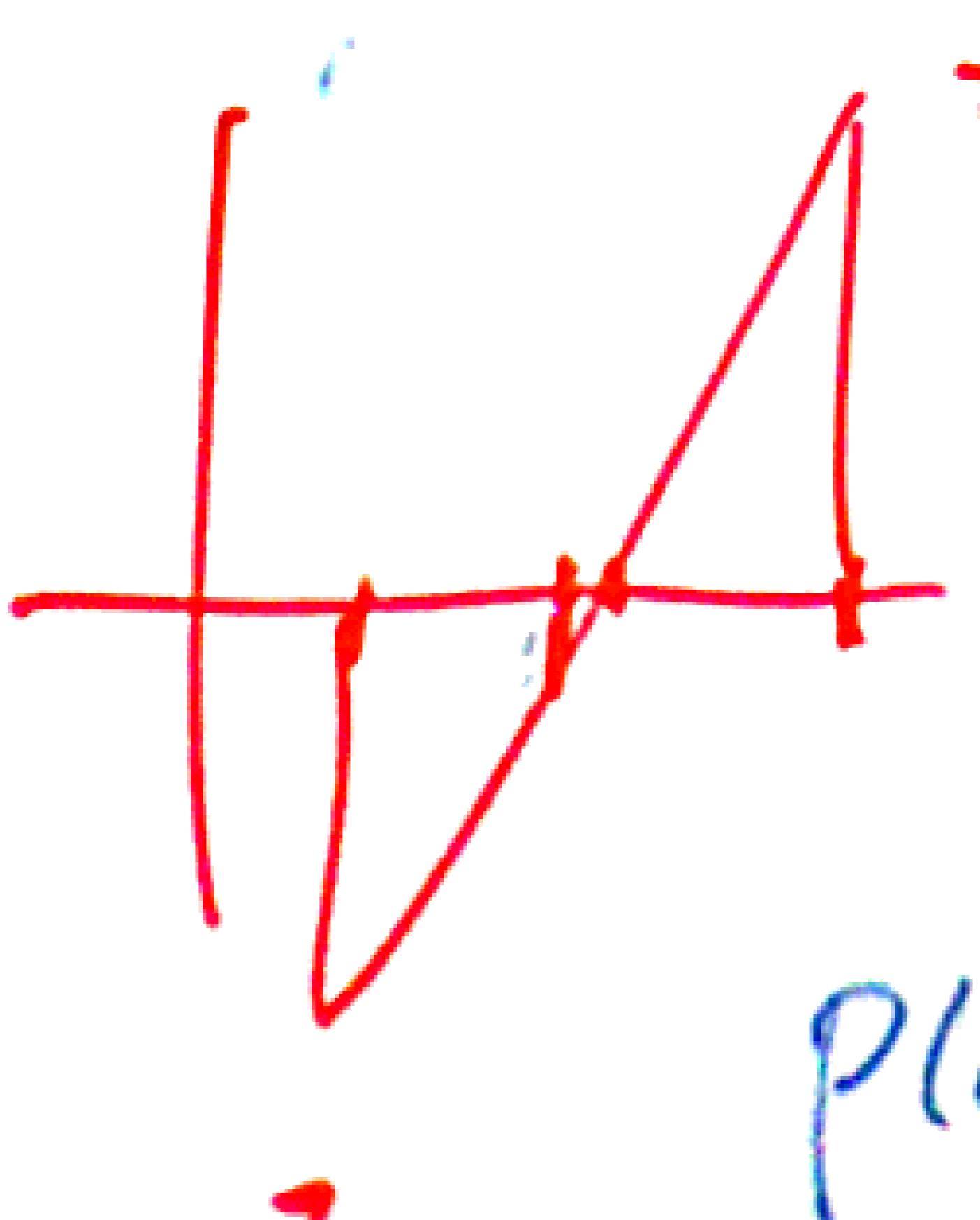
$$S_n^- = \{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \}$$

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

$$x^2 - 4 \equiv 0 \pmod{15}$$

$$(x-2)(x+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} x=7 \\ x=8 \end{matrix}$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

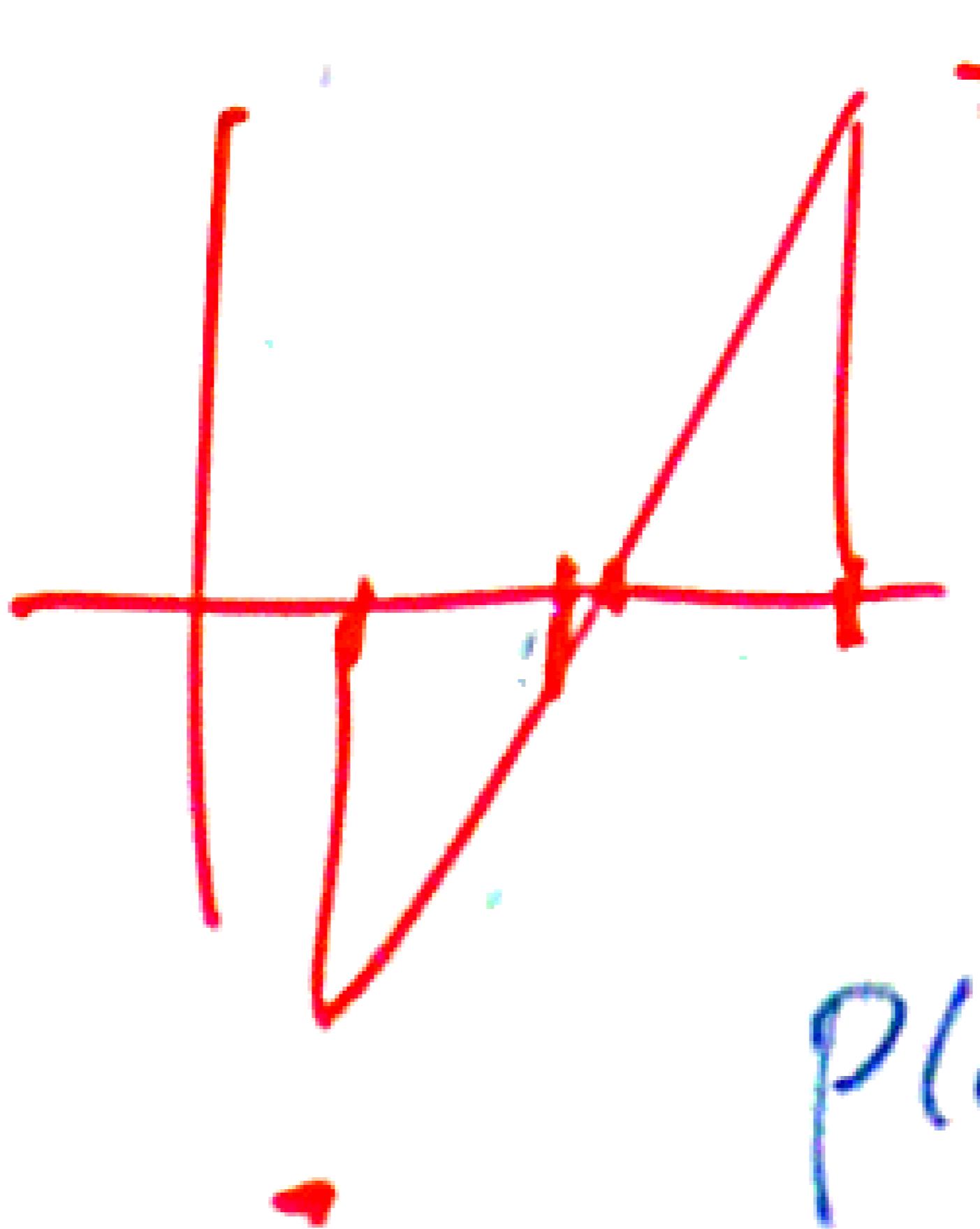
$$S_n^- = \left\{ a \in \mathbb{Z}_n^* \mid a^{\frac{n-1}{2}} \equiv -1 \pmod{n} \right\}$$

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

$$X^2 - 4 \equiv 0 \pmod{15}$$

$$(X-2)(X+2) \equiv 0 \pmod{15}$$

$$\begin{matrix} 5 & 9 \\ 6 & 10 \end{matrix} \quad \begin{matrix} X=7 \\ X=8 \end{matrix}$$



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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

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

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

$$p(x) \equiv 0 \pmod{n}$$

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

$$p(a) \equiv 0 \pmod{n} \Leftrightarrow a \in S_n^+$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$$36 = 6^2$$

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

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

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

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

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

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

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

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

$$n = a^2$$

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

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

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

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

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

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

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

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

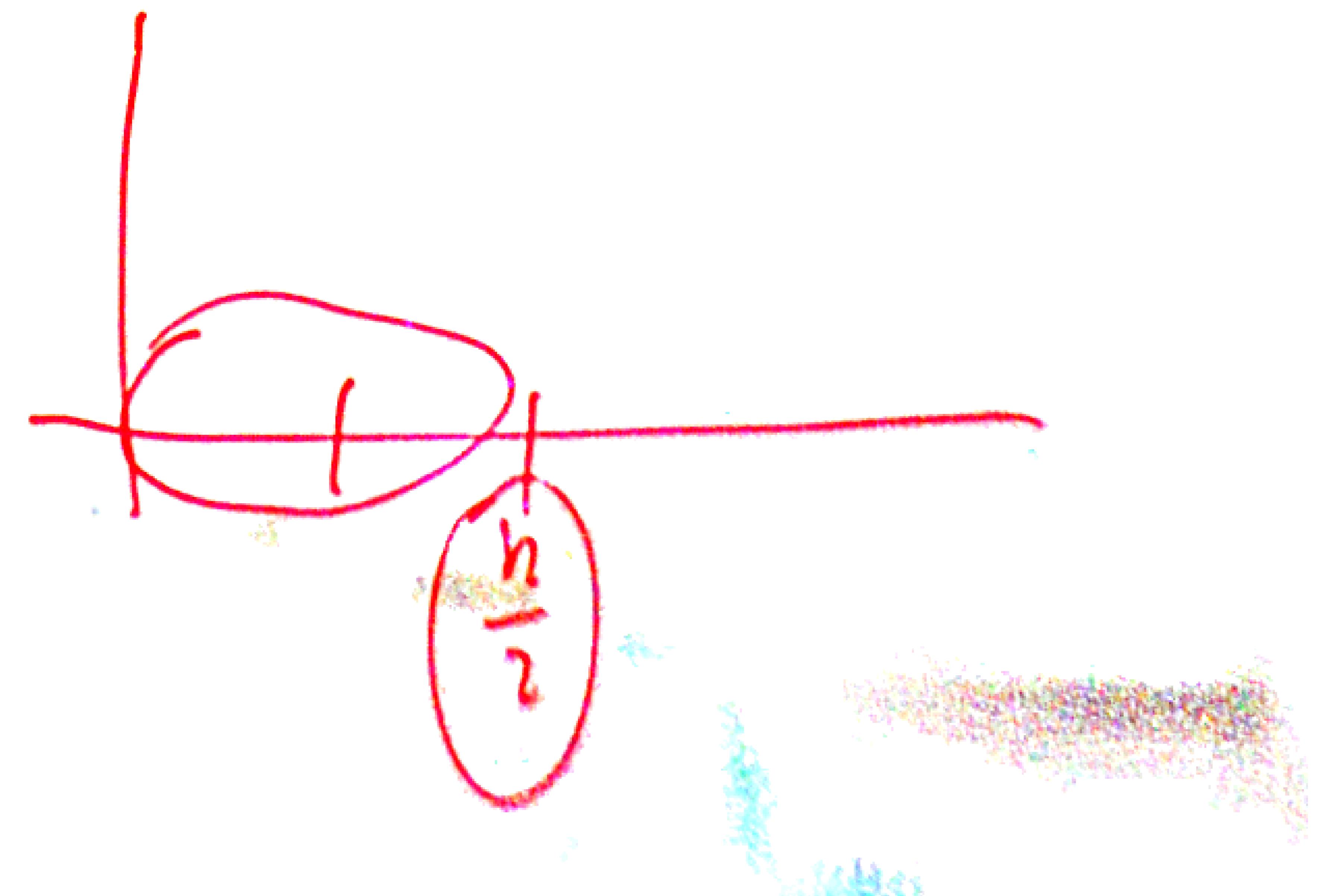
$$|\mathbb{Z}_n^*| = n-1$$

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

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

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

$$n = a^2$$



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

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

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

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

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

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

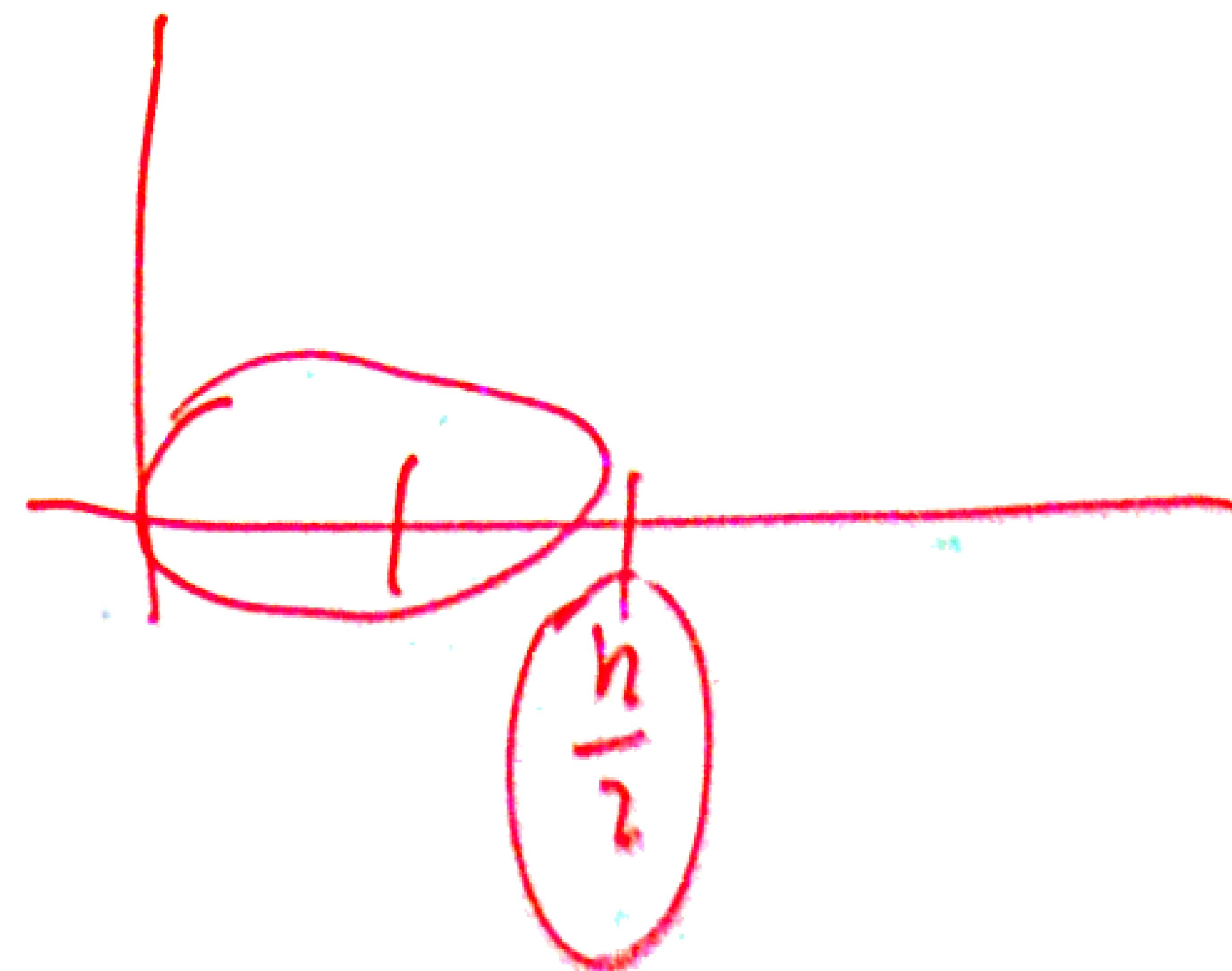
$$|\mathbb{Z}_n^*| = n-1$$

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

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

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

$$n = a^2$$



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

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

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

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

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

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

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

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

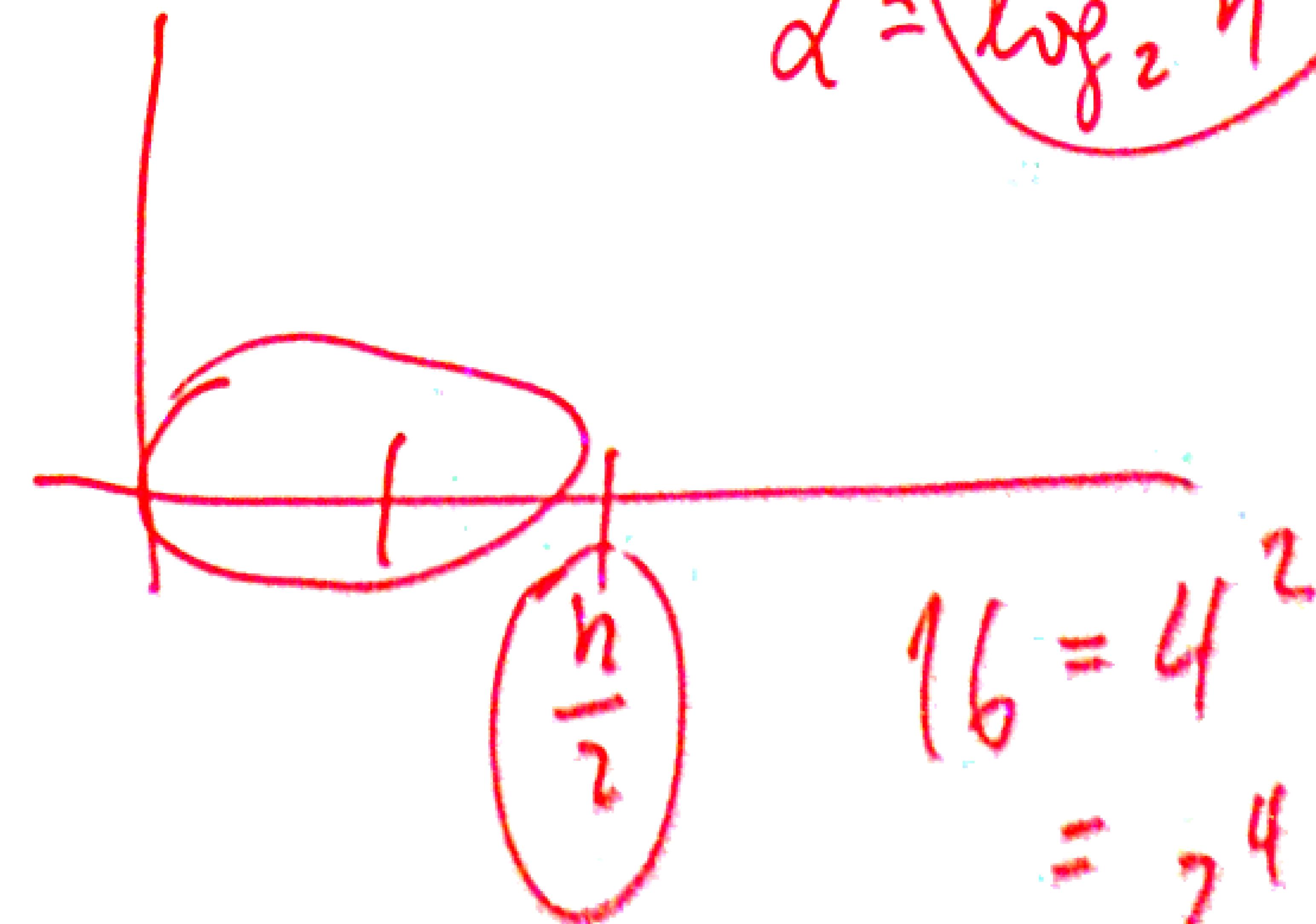
$$a^{\frac{n-1}{2}} \pmod{n}$$

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

$$n = a^2$$

$$n = 2^d$$

$$d = \log_2 n$$



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

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

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

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

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

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

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

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

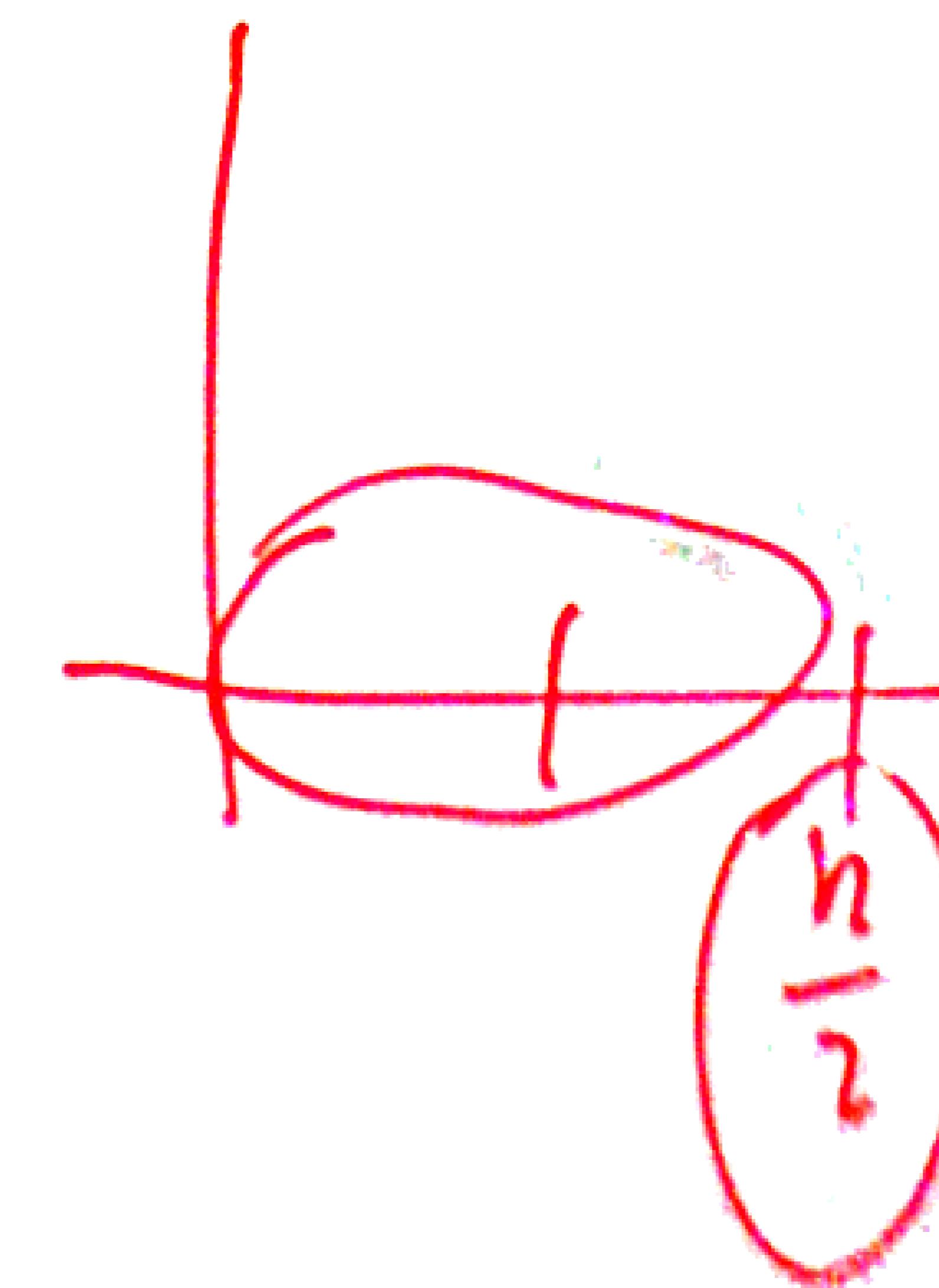
$$a^{\frac{n-1}{2}} \pmod{n}$$

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

$$n = a^2$$

$$n = 2^d$$

$$d = \log_2 n$$



$$\begin{aligned} 16 &= 4^2 \\ &= 2^4 \end{aligned}$$

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

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

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

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

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

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

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

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

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

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

$$n = a^2$$

$$n = h_1 \cdot n_2$$

$$\text{MCD}(n_1, n_2) = 1$$

$$h_1 \geq 3, n_2 \geq 3$$

$$\cancel{36 \div 6} = 2^3 \cdot 3^2$$

$$= 2^4$$

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

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

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

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

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

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

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

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

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

*n primo*

$$|S_n| = n-1$$

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

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

*n es compuesto*

$$= 2^4$$

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

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

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

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

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

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

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

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

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

*n primo*

$$|S_n| = n-1$$

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

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

*n es compuesto :*

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

$$\Rightarrow |S_n| < 1 / |\mathbb{Z}_n^*|$$

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

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

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

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

$n$  Primz

$$|S_n| = n-1$$

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

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

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

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

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

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

$n$  es compuesto :

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

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,100}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,100}$$

$n$  primo

$$|S_n| = n-1$$

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

$n$  es compuesto:

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

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

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

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

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

$n$  primo

$$|S_n| = n-1$$

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

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

$$\alpha_1, \dots, \alpha_{100} \in \{1, \dots, n-1\}$$

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

$$b_1, \dots, b_{100}$$

$n$  es compuesto:

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

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

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

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

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

$n$  primo

$$|S_n| = n-1$$

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  es compuesto:

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

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

$$\alpha_1, \dots, \alpha_{1000} \in \{1, \dots, n-1\}$$

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

$$b_1, \dots, b_{1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

$$\exists \alpha : \alpha^{\frac{n-1}{2}} \equiv -1 \pmod{n}$$

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

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

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

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

$$\alpha_{1,1}, \dots, \alpha_{1,1000} \in \{1, \dots, n-1\}$$

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

$n$  es compuesto:

$$\exists \alpha : \alpha^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$$

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

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

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

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

$n$  primo

$$|S_n| = n-1$$

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

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

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

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

X

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  es compuesto :

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

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

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

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

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

$$\alpha_{1,1}, \dots, \alpha_{1,1000} \in \{1, \dots, n-1\}$$

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

$$\exists \alpha : \alpha^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$$

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

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

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

$$b_1, \dots, b_{1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

$n$  primo

$$|S_n| = n-1$$

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

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

$$\alpha_1, \dots, \alpha_{1000} \in \{1, \dots, n-1\}$$

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

X

$$b_1, \dots, b_{1000}$$

$n$  es compuesto:

$$\exists \alpha : \alpha^{\frac{n-1}{2}} \not\equiv 1 \pmod{n}$$

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

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

$n$  es compuesto:

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

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

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

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

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

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

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

$$b_{1,1}, \dots, b_{1,1000}$$

$n$  primo

$$|S_n| = n-1$$

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

$n$  es compuesto:

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

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