

למה $a \in \mathbb{Z}_m^*$ יש $a \in \mathbb{Z}_m^*$ מסת $\phi(m)$
 $a^{\phi(m)} \equiv 1 \pmod{m}$ - ל ϕ נקרא ϕ
 ϕ נקרא ϕ , $k = \text{ord}_m(a)$, $a^k \equiv 1 \pmod{m}$ כל x
 $\text{ord}_m(a) | \phi(m)$, a לכל $(a, m) = 1$ *
 $\text{ord}_m(a) = \phi(m)$ כל m וכל $a \in \mathbb{Z}_m^*$ *
 $\mathbb{Z}_m^* = \{1, a, a^2, \dots, a^{\phi(m)-1}\}$ *
 הוכחה - $\phi(m)$ מסת $\phi(m)$ *
 כל $a \in \mathbb{Z}_m^*$ *

13 נה - $\phi(m)$ מסת $\phi(m)$ *
 $\phi(m) = \phi(p^k) = p^{k-1}(p-1)$ *
 m מסת $\phi(m)$ *
 $(a, m) = 1$ *
 $m=2$ מסת $\phi(m)$ *
 $m=4$ מסת $\phi(m)$ *
 $\phi(m) = p^{k-1}(p-1)$ *

$f(x) = x^{\phi(m)} \pmod{m}$, $f: \mathbb{Z}_m^* \rightarrow \mathbb{Z}_m^*$ *
 $x \mapsto x^{\phi(m)} \pmod{m}$ *
 $a \in \mathbb{Z}_m^*$ *
 $a^{\phi(m)} \equiv 1 \pmod{m}$ *

$a \in \mathbb{Z}_m^*$ *
 $a^{\phi(m)} \equiv 1 \pmod{m}$ *
 $d = \text{gcd}(\phi(m), r)$ *
 $\phi(m) = ed$, $r = r_1 d$, $\text{gcd}(e, r_1) = 1$ *

$$a^{d(m)/\phi(m), r} = a^{\frac{d(m)}{s}} = a^e = \textcircled{*} \quad , r \in \mathbb{Z}$$

\rightarrow not true

$$g^{rt} \equiv x^r \equiv a \equiv g^s \pmod{m} \Rightarrow g^{rt-s} \equiv 1 \pmod{m}$$

$$rt \equiv s \pmod{\phi(m)} \Leftrightarrow \phi(m) | rt - s$$

$$\begin{aligned} \textcircled{*} &= (g^s)^e = (g^{rt})^e = g^{rte} = g^{r \cdot dte} = \\ &= (g^{de})^{rt} = (g^{\phi(m)})^{rt} = 1^{rt} = 1 \pmod{m} \end{aligned}$$

$$g^e \equiv a^e \equiv 1 \pmod{m}$$

$$d | s \quad \text{with } de = \phi(m) | se$$

open to all integers a and r such that $rt \equiv s \pmod{\phi(m)}$, t

$$x = g^t \pmod{m} \quad \text{with } (g^t, m) = 1$$

$$x^r = g^{tr} = g^s = a \pmod{m}$$

$$sr = 1 \pmod{\phi(m)}, \quad \phi(m) - s \text{ is } s, r \text{ at } \frac{1}{s} \pmod{\phi(m)}$$

$$f(x) = x^r \quad \text{and} \quad g(x) = x^s \pmod{m}$$

$$f \circ g \circ f = x \quad \text{and} \quad g \circ f \circ g = x$$

$$f \circ g(x) = (x^S)^r = x^{sr} = x^{rs} = x^{1+\phi(m)} = x \cdot (x^{\phi(m)})^1 = x \cdot 1 = x$$

$$g \circ f = x \quad \text{על המרחב המצוי} \quad \text{הוא הפיכה}$$

הקטור ϕ הפיכה

מקרה הכללי: ϕ הפיכה

הפונקציה f הפיכה

הפונקציה g הפיכה

הפונקציה f הפיכה

הפונקציה g הפיכה

$$b = a^r \pmod{m} \rightarrow \text{הפונקציה}$$

$$b^s = a^{rs} = a \pmod{m}$$

הפונקציה f הפיכה

הפונקציה g הפיכה

הפונקציה f הפיכה

$$b = a^r \pmod{m} \quad m = pq$$

הפונקציה f הפיכה

הפונקציה g הפיכה

$$\phi(m) = (p-1)(q-1)$$

$$pq = m$$

הפונקציה f הפיכה

הפונקציה g הפיכה

$$a^{\frac{\phi(m)}{\gcd(k, \phi(m))}} \equiv 1 \pmod{m} \quad \forall a \in \mathbb{Z}_m^*$$

$$(x \pmod{m_2}) \quad d_1 a_2 = (d_1 x)^2 \pmod{m_2}, \quad m = d_1 m_2, \quad a = d_1 a_2, \quad x = d_1 x_1 \quad \text{כאשר } d_1 \text{ מתחלק על } m_2$$

מכאן נובע כי d_1 חייב להיות חזק של m_2 (במובן של חזק של m_2).

$$d_1 x_1^2 = a_2 \pmod{m_2}$$

כאשר d_1 מתחלק על m_2 , נקרא $d_1 = d_1' m_2$. אז המשוואה הופכת ל:
 $d_1' m_2 x_1^2 = a_2 \pmod{m_2}$
 כלומר $d_1' x_1^2 \equiv a_2 \pmod{m_2}$.
 אם $d_1' \equiv 1 \pmod{m_2}$, אז $x_1^2 \equiv a_2 \pmod{m_2}$.
 אם $d_1' \not\equiv 1 \pmod{m_2}$, אז המשוואה לא תפתור.

$$x_1^2 = \frac{d_1^{-1}}{a_2} a_2 \pmod{m_2}$$

כאשר d_1^{-1} הוא הפיכי של d_1 modulo m_2 .
 נניח $a_2 = d_1' m_2 + r$, אז $x_1^2 \equiv d_1^{-1} r \pmod{m_2}$.
 אם $d_1' \equiv 1 \pmod{m_2}$, אז $x_1^2 \equiv r \pmod{m_2}$.
 אם $d_1' \not\equiv 1 \pmod{m_2}$, אז המשוואה לא תפתור.

נניח $a \in \mathbb{Z}_m^*$, $m = m_1 m_2$, $\gcd(m_1, m_2) = 1$. אז $a \pmod{m}$ מתחלק על m_1 ו- m_2 .

$$x^2 \equiv a \pmod{m} \iff x^2 \equiv a \pmod{m_1} \text{ ו-} x^2 \equiv a \pmod{m_2}$$

כלומר $x^2 \equiv a \pmod{m_1}$ ו- $x^2 \equiv a \pmod{m_2}$ הם תנאים הכרחיים ומוכרחיים.

$$x^2 \equiv a \pmod{m} \iff x^2 \equiv a \pmod{m_1} \text{ ו-} x^2 \equiv a \pmod{m_2}$$

אם $x^2 \equiv a \pmod{m_1}$ ו- $x^2 \equiv a \pmod{m_2}$, אז $x^2 \equiv a \pmod{m}$.

נניח $x \equiv x_1 \pmod{m_1}$ ו- $x \equiv x_2 \pmod{m_2}$. אז $x^2 \equiv x_1^2 \pmod{m_1}$ ו- $x^2 \equiv x_2^2 \pmod{m_2}$.

$$\begin{aligned} m_1 \mid x^2 - a &\iff x^2 \equiv x_1^2 \equiv a \pmod{m_1} \\ m_2 \mid x^2 - a &\iff x^2 \equiv x_2^2 \equiv a \pmod{m_2} \end{aligned}$$

אם $m = m_1 m_2$ ו- $\gcd(m_1, m_2) = 1$, אז $x^2 \equiv a \pmod{m}$ אם ורק אם $x^2 \equiv a \pmod{m_1}$ ו- $x^2 \equiv a \pmod{m_2}$.

אם $m = p_1^{r_1} \dots p_k^{r_k}$, אז $x^2 \equiv a \pmod{m}$ אם ורק אם $x^2 \equiv a \pmod{p_i^{r_i}}$ לכל i .

אם $x^2 \equiv a \pmod{p_i^{r_i}}$, אז $x^2 \equiv a \pmod{p_i}$.
 נניח $x^2 \equiv a \pmod{p}$, אז $x^2 - a = p \cdot k$.
 אם $p \equiv 1 \pmod{4}$, אז $x^2 \equiv a \pmod{p}$ אם ורק אם a הוא חזק של p .
 אם $p \equiv 3 \pmod{4}$, אז $x^2 \equiv a \pmod{p}$ אם ורק אם a הוא חזק של p .

אם $p \equiv 1 \pmod{4}$, אז $x^2 \equiv a \pmod{p}$ אם ורק אם a הוא חזק של p .
 אם $p \equiv 3 \pmod{4}$, אז $x^2 \equiv a \pmod{p}$ אם ורק אם a הוא חזק של p .

$m = p = 2$: δp \rightarrow δp \rightarrow δp
 $(x=1)$ \rightarrow $x^2=1 \pmod{2} = 1$

$a \in \mathbb{Z}_p^*$, $p \geq 3$: $\left(\frac{a}{p}\right) = \begin{cases} 1, & \exists x \in \mathbb{Z}_p^* \text{ s.t. } x^2 = a \pmod{p} \\ -1, & \nexists x \in \mathbb{Z}_p^* \text{ s.t. } x^2 = a \pmod{p} \end{cases}$

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \Leftrightarrow x^2 = a \pmod{p} \Leftrightarrow \left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \pmod{p}$
 $a, b \in \mathbb{Z}_p^*$: $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$

$\left(\frac{ab}{p}\right) = (ab)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \pmod{p}$

$\frac{p-1}{2}$ \rightarrow p \rightarrow $\frac{p-1}{2}$

$\{x^2 : x \in \mathbb{Z}_p^*\} = \{x^2 \pmod{p} : x \in \{1, \dots, p-1\}\}$
 $x^2 \equiv (-x)^2 \equiv (p-x)^2 \pmod{p}$
 $p-x \in \{1, \dots, p-1\}$
 $x \rightarrow x^2 \pmod{p}$

הוכחה: $p \geq 3$ ראשוני, \dots $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

הוכחה: האפשרות שאין פתרון $x^2 \equiv a \pmod{p}$ עבור $a \neq 0$ היא $\frac{p-1}{2}$ עבור p ראשוני.

שאלה: האם יש פתרון ל- $x^2 \equiv 7 \pmod{13}$?

$$7^6 \equiv (49)^3 \equiv (10)^3 \equiv (-3)^3 \equiv -27 \equiv -1 \pmod{13}$$

לכן 7 הוא שארית הריבועים מוד 13 .

$$7^8 = 49^4 = (-2)^4 = 16 \equiv -1 \pmod{17}$$

לכן 7 הוא שארית הריבועים מוד 17 .

עבור a שארית הריבועים, עבור אינסוף a , שארית הריבועים a היא 2^k עבור $k \geq 0$.

עבור $k=1$: $\mathbb{Z}_4^* = \{1, 3\}$: $k=2$

$$1^2 = 1 = 3^2 \pmod{4}$$

עבור $k=3$: $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$: $k=3$

$$1^2 = 1 = 3^2 = 5^2 = 7^2 \pmod{8}$$

עבור $k=4$: $\mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$: $k=4$

הוכחה: a שארית הריבועים מוד 2^k היא 1 עבור $k \geq 3$.

שאלה: האם יש פתרון ל- $x^2 \equiv a \pmod{2^k}$ עבור $a \equiv 1 \pmod{8}$?

הוכחה: עבור $k \geq 3$, $a \equiv 1 \pmod{8}$ היא שארית הריבועים מוד 2^k .

נניח $a \not\equiv 1 \pmod{8}$ ונניח $x^2 \equiv a \pmod{2^k}$ עבור $k \geq 3$.

אז $x^2 \equiv a \pmod{8}$ וזה בלתי אפשרי.

נניח $a \equiv 1 \pmod{8}$ ונניח $x^2 \equiv a \pmod{2^k}$ עבור $k \geq 3$.

אז $x^2 \equiv a \pmod{2^{k-1}}$ ונניח $x = x_1 + 2^{k-2}y$.

אז $x_1^2 \equiv a \pmod{2^{k-1}}$ עבור $x_1 \in \{0, 1, 3, 5\}$.

הצגה נכונה (הצגה נכונה) → נח וס נסד x_1 נכונה

$x^2 \equiv a \pmod{2^k}$ נכונה נכונה s נכונה

(i) $x^2 = (x_1 + s2^{k-1})^2 = x_1^2 + 2x_1s2^{k-1} + s^22^{2k-2} =$
 $= x_1^2 + x_1s2^{k-1} + s^22^{2k-2} \equiv$
 $\equiv x_1^2 + x_1s2^{k-1} \pmod{2^k}$ $2k-2 \geq k$
 $k \geq 4$

$x^2 \equiv x_1^2 \pmod{2^{k-1}}$ נכונה נכונה

$t \in \{0, 1\}$ (ii) $x^2 \equiv x_1^2 + t2^{k-1} \pmod{2^k}$ נכונה

נכונה (ii) נכונה (i) נכונה

$sx_12^{k-1} = t2^{k-1} \pmod{2^k}$

\updownarrow
 $sx_1 = t \pmod{2}$

נכונה $s = t \pmod{2}$, $s \in \{0, 1\}$ $x_1 \in \{0, 1\}$ נכונה

נכונה $t \in \{0, 1\}$ נכונה $s \in \{0, 1, 2, 3\}$ נכונה

נכונה $x_1^2 = a \pmod{2^{k-1}}$

נכונה $x^2 \pmod{2^k}$ נכונה

$x^2 \equiv a \pmod{2^k}$ נכונה, נכונה, נכונה $a \pmod{2^k}$ נכונה