הגדרה: יהי $a \in \mathbb{Z}_m^*$, נאמר כי a הוא **שורש פרימיטיבי** מודולו m אם הסדר הכפלי של a הוא $\phi(m)$.

* $a^k \equiv 1 \pmod{m}$ אם"ם $k = ord_m(a)$, $r \mid k$.
* $ord_m(a) \mid \phi(m)$ (משפט אוילר): לכל a, $ord_m(a)$.
* a נקרא **שורש פרימיטיבי מודולו m** אם $ord_m(a) = \phi(m)$.

מתקיים כי: $\mathbb{Z}_m^* = \{1, a, a^2, \ldots, a^{\phi(m)-1}\}$.

הוכחה – **משפט הגזר הפרימיטיבי** – נניח כעת שm מקיים ש"קיים שורש פרימיטיבי מודולו m".

דוגמה – בשלב זה הקורא – כולל, שי"ל כי $1 \neq m$, אז $\phi(m) \equiv 1 \pmod{4}$ – הוא פרימיטיבי עם"כ לכל m יש ש"פ שורש פרימיטיבי מודולו m.

משפט – (ללא הוכחה – מעבר לקורס)

יהי $m = 2$, שורש פרימיטיבי מודולו m אז"ם $m = 4$, או $m = p^k$ או $m = 2p^k$, p פרימי אי-זוגי.

סדרה: יהי $f: \mathbb{Z}_m^* \to \mathbb{Z}_m^*$ לכל $x \mapsto x^r \pmod{m}$. $f(x) = x^r \pmod{m}$.

טענה: (לא הוכחה) שק"ט שורש פרימיטיבי מודולו m. יהי $a \in \mathbb{Z}_m^*$. אז"ם $x \in \mathbb{Z}_m^*$ כך ש$x^r \equiv a \pmod{m}$ אמ"מ $a^{\frac{\phi(m)}{\gcd(\phi(m), r)}} \equiv 1 \pmod{m}$

הוכחה: $\Rightarrow$: יהי x כך ש$x^r \equiv a \pmod{m}$. יהי $g \in \mathbb{Z}_m^*$ כך ש$g^t \equiv x \pmod{m}$, $g^{st} \equiv a \pmod{m}$ פרימיטיבי. צ.ל. st כך ש$d = \gcd(\phi(m), r)$. נסמן $\phi(m) = ed$, $r = r_1 d$, $\gcd(e, r_1) = 1$

$$a^{\phi(m)/\gcd(\phi(m),r)} = a^{\frac{\phi(m)}{d}} = a^e = (*)$$

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

$$rt \equiv s \pmod{\phi(m)} \Leftarrow \phi(m) \mid rt-s$$

$$(*) = (g^s)^e = (g^{rt})^k = g^{rte} = g^{r_1 d te} =$$

$$= (g^{de})^{r_1 t} = (g^{\phi(m)})^{r_1 t} = 1^{r_1 t} = 1 \pmod m$$

$$\Rightarrow g^{\frac{\phi(m)}{d}} \equiv a^e \equiv 1 \pmod m$$

$$\phi(m) \mid se$$

$$at \equiv b \pmod m$$

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

$$x = g^t$$

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

$$sr \equiv 1 \pmod{\phi(m)}$$

$$g(x) = x^s \pmod m$$

$$f(x) = x^r \pmod m$$

$$f \circ g \circ f \circ g = x$$

$$f\circ g(x) = (x^s)^r = x^{sr} = x^{rs} = x^{1+c\phi(m)} = x\cdot(x^{\phi(m)})^c = x \quad (\text{משפט אוילר})$$

כלומר הוכחנו שמתקיים $f = g^{-1}$.

הערה חשובה:

משפט (משפט אוילר): יהיו m שלם חיובי ו-a מספר שלם כך ש-$\gcd(a,m)=1$. אזי $a^{\phi(m)} \equiv 1 \pmod m$.

משפט (משפט פרמה הקטן): יהי p ראשוני ו-a מספר שלם כך ש-$p \nmid a$. אזי $a^{p-1} \equiv 1 \pmod p$.

הוכחה: נובע ישירות ממשפט אוילר, שכן $\phi(p) = p-1$.

משפט (משפט השאריות הסיני): יהיו $m_1, m_2, \ldots, m_k$ מספרים שלמים חיוביים זרים בזוגות, ויהיו $a_1, a_2, \ldots, a_k$ מספרים שלמים כלשהם. אזי קיים פתרון יחיד x למערכת הקונגרואנציות $x \equiv a_i \pmod{m_i}$ לכל i, ופתרון זה הוא יחיד מודולו $m = m_1 m_2 \cdots m_k$.

הוכחה: נוכיח תחילה את קיום הפתרון. נסמן $M_i = m/m_i$ לכל i. מכיוון ש-m_i זר ל-M_i, קיים y_i כך ש-$M_i y_i \equiv 1 \pmod{m_i}$. נגדיר $x = \sum_{i=1}^{k} a_i M_i y_i$. לכל j מתקיים $x \equiv a_j M_j y_j \equiv a_j \pmod{m_j}$, שכן $M_i \equiv 0 \pmod{m_j}$ לכל $i \neq j$. נוכיח כעת את יחידות הפתרון. נניח שקיימים שני פתרונות x ו-x'. אזי $x - x' \equiv 0 \pmod{m_i}$ לכל i, ומכיוון שהמספרים m_i זרים בזוגות, נובע ש-$x - x' \equiv 0 \pmod m$, כלומר $x \equiv x' \pmod m$.

דוגמה 13

תרגילים: הוכיחו — יהיו $a \in \mathbb{Z}_m^*$, k טבעי. קבוע כי $x^k \equiv a \pmod m$ יש פתרון x אם"ם $a^{\frac{\phi(m)}{\gcd(k,\phi(m))}} \equiv 1 \pmod m$.

$m = p \geq 3$ – נניח ש- p ראשוני. אז $\phi(m) = p-1$. לכן:

$$\frac{\phi(m)}{\gcd(\phi(m), 2)} = \frac{p-1}{\gcd(p-1, 2)} = \frac{p-1}{2}$$

משפט (אוילר): יהי p ראשוני, אז a שארית ריבועית $\pmod p$ $\iff$ $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

הערה: יהי $a^{p-1} \equiv 1 \pmod p$. נסמן $b = a^{\frac{p-1}{2}}$. אז $b^2 \equiv 1 \pmod p$, לכן $b \equiv \pm 1 \pmod p$.

קולגרוזאנג'ה בית ראשית

השאלה – נתונים m, שאינו אולם, ו- $a \in \mathbb{Z}_m^*$. קיים x כך ש- $x^2 \equiv a \pmod m$?

דוגמאות: האם קיימים $x, y \in \mathbb{Z}$ כך ש- $3x^2 + 2 = y^2$?

עבור y כזה: $y^2 \equiv 2 \pmod 3$. לכן $y \not\equiv 0 \pmod 3$. לפי משפט פרמה הקטן $2^{\frac{3-1}{2}} = 2 \not\equiv 1 \pmod 3$. לכן אין פתרון למשוואה.

אלגוריתם לבדיקת משפט האם קיים x כך ש- $x^2 \equiv a \pmod m$.

מספרים יש לבדוק משפט, נניח שיש x כזה, נוכיח מוכיחים שאכן (או לא) בכך).

נוסף לכך לחלק מהמשוואות פתרון מצורה 2. משוואה $ax^2 + bx + c \equiv 0 \pmod m$. נניח כי אפשר שהשורש $x^2 \equiv a \pmod m$ פתרון כך – שהוכיח.

הערה שימושי: הוכחה $a \in \mathbb{Z}_m^*$:

נניח ש- $1 < \gcd(a, m) = d$. לכן $m = md$, $a = ad$, כך ש- $x^2 \equiv a \pmod m$ פתרון אז יש פתרון. $\gcd(m, a_1) = 1$. נראה שלכן פתרון ש: $x^2 \equiv a_1 d \pmod{md}$ $\Leftarrow$ $d \mid x^2$.

d מספר $\Leftarrow$ $d \mid 4x^2$ $\Leftarrow$ $d \mid x$.

$d_1 a_2 = (d_1 x)^2$ ($\mod m_2$) קיומה, אם נשים $x = d_1 x_1$, $a = d_1 a_2$, $m = d_1 m_2$, אז

$d_1^2 x_1^2$

נוכל לצמצם ב- d_1 ונקבל:

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

אם $m_2 \mid d_1$, אז המשוואה נקבע $d_1 \mid a_2$ והיא תהיה כלשהי

לעומת שלפ. לכן בהכרח ($m_2 \mid d_1 x$, ומשם

d_1 ב- x נוכל לצמצם את m_2 ונקבל:

$$x_1^2 = \underbrace{d_1^{-1} a_2}_{a} \pmod{\underbrace{m_2}_{m}}$$

כך נוכל להקטין את המספרים, עד שיקבל

m, a כאלה - ונשאר רק לענות אלגוריתם לפשוט.

לכן נניח להבא בהמשך שאכן כך.

טענה: נניח ש- $a \in \mathbb{Z}_m^*$, $m = m_1 m_2$, $\gcd(m_1, m_2) = 1$,

$1 < m_1, m_2 < m$. אז פתרון למשוואה $x^2 \equiv a \pmod m$ $\Leftrightarrow$

יש פתרון לכל אחת מהמשוואות $x^2 \equiv a \pmod{m_1}$, $x^2 \equiv a \pmod{m_2}$

הוכחה: $\Rightarrow$: $x^2 \equiv a \pmod m \Rightarrow x^2 \equiv a \pmod{m_1}$

$x^2 \equiv a \pmod{m_2}$

$\Leftarrow$: נניח $x_1^2 \equiv a \pmod{m_1}$, $x_2^2 \equiv a \pmod{m_2}$. צ"ל: משפט

השאריות הסיני, קיים x כך ש- $x \equiv x_1 \pmod{m_1}$, $x \equiv x_2 \pmod{m_2}$.

$$\begin{cases} m_1 \mid x^2 - a \\ m_2 \mid x^2 - a \end{cases} \Leftarrow \begin{cases} x^2 \equiv x_1^2 \equiv a \pmod{m_1} \\ x^2 \equiv x_2^2 \equiv a \pmod{m_2} \end{cases}$$

לפי m_1, m_2 זרים, לכן $m_1 m_2 \mid x^2 - a$, כלומר $m = m_1 m_2 \mid x^2 - a$.

מסקנה: מהטענה הזו"מ שכל פתרון $x^2 \equiv a \pmod m$, $m = p_1^{r_1} \cdots p_k^{r_k}$

מספק רצף של $x^2 \equiv a \pmod{p_i^{r_i}}$ לכל i, כאשר p_i, r_i כנ"ל.

הטענה נכונה כי: אם $p=2$ אז: $x^2 \equiv 1 \pmod 2$ יש פתרון יחיד $x=1$.

הגדרה: יהי $p \geq 3$ ראשוני, ו- $a \in \mathbb{Z}_p^*$. נסמן:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{אם } a \text{ שארית ריבועית מודולו } p \\ -1, & \text{אם } a \text{ לא שארית ריבועית מודולו } p \end{cases}$$

סימן זה נקרא **סימן לז'נדר**.

קריטריון אוילר: $a^{\frac{p-1}{2}} \equiv 1 \pmod p \iff x^2 \equiv a \pmod p$ יש פתרון x כך ש-

מסקנה: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.

משפט: יהי $p \geq 3$ ראשוני, ו- $a, b \in \mathbb{Z}_p^*$. אזי:

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$$

הוכחה:

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

הגדרה: a נקרא **שארית ריבועית** מודולו m אם קיים x כך ש- $x^2 \equiv a \pmod m$.

מסקנה: מספר השאריות הריבועיות מודולו p הוא $\frac{p-1}{2}$, כאשר $p \geq 3$.

הוכחה:

$$\{\text{שאריות ריבועיות מודולו } p\} = \left\{x^2 : x \in \mathbb{Z}_p^*\right\} = \left\{x^2 \pmod p : x \in \{1, \ldots, p-1\}\right\}$$

לכל $x \in \mathbb{Z}_p^*$, $x^2 \equiv (-x)^2 \equiv (p-x)^2 \pmod p$.

לכל $x \in \{1 \ldots p-1\}$ מתקיים $p-x \in \{1 \ldots p-1\}$ ו- $p-x \equiv x \pmod p$, כי $x = p-x \Leftarrow p=2x$.

לכן כל שארית ריבועית מודולו p מתקבלת מ- $x \mapsto x^2 \pmod p$ של בדיוק שני איברים שונים, x ו- $p-x$, ולכן מספר השאריות הריבועיות הוא $\frac{p-1}{2}$.

משפט: יהי $p \geq 3$ ראשוני. אז: $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

הוכחה: הפולינום $x^2 - 1$ מעל $\mathbb{Z}_p$ מתפרק לגורמים לינאריים $(x-1)(x+1)$, וכך יש לו בדיוק שני שורשים שונים $1, -1$ (שונים כי $p \geq 3$). לכן לכל $a \neq 0$ יש בדיוק שני פתרונות או אף לא אחד ל-$x^2 \equiv a \pmod{p}$.

בונוס: האם למשוואה $x^2 \equiv 7 \pmod{13}$ יש פתרון?

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

לכן 7 לא שארית ריבועית מודולו 13.

האם 7 שארית ריבועית מודולו 17?

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

לכן 7 לא שארית ריבועית מודולו 17.

עבור כל a שזר, נגדיר: a שארית ריבועית מודולו 2^k, $k \geq 3$:

$k=3$: $a=1$ היא שארית ריבועית היחידה

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

לכן 1 מקיים $x^2=1$ ו-3 לא מקיים $3^2 = 1 \pmod{4}$

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

לכן 1 מקיים $x^2=1 \pmod{8}$ ו-3,5,7 לא מקיימים.

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

הוכחה: a שארית ריבועית מודולו 2^k, $k=2,3$, אמ"מ $a=1$.

משפט: יהי $k=2^m$, $m \geq 3$. a שארית ריבועית מודולו 2^k אמ"מ $a \equiv 1 \pmod{8}$.

הוכחה: מתקיים עבור k (הוכחנו כבר עבור $k=3$) נניח $a \equiv 1 \pmod{8}$ ונוכיח $x^2 \equiv a \pmod{2^k}$ [$k \geq 3$].

עבור $k=3$ נתון $x^2 \equiv a \pmod{2^3}$ - ונוכיח שהוא פתיר.

נניח $a \equiv 1 \pmod{8}$ ולפי ההנחה יש x כך ש-$x^2 \equiv a \pmod{2^{k-1}}$. (מכפל סימון: $x = x_1 + s \cdot 2^{k-2}$, $s \in \{0,1,2,3\}$ כאשר $x_1^2 \equiv a \pmod{2^{k-1}}$.