תזכורת

$a \in \mathbb{Z}_m^*$ נקרא שארית ריבועית מודולו m אם יש $x \in \mathbb{Z}$ כך ש: $x^2 \equiv a \pmod m$.

ממשפט השאריות הסיני נובע שאם $m = 2^{r_0} p_1^{r_1} \cdots p_k^{r_k}$
אז a שארית ריבועית מודולו m $\iff$ a שארית ריבועית מודולו $p_i^{r_i}$ לכל i ($p_0 = 2$).

(*) רצינו - a שארית ריבועית מודולו 2^t $\iff$ $a \equiv \pmod{m, n(2^k, 8)} \equiv$ (a אי-זוגי)
$\equiv \begin{cases} \pmod{2^k}, & 2^k = 2, 4 \\ \pmod 8, & 2^k \geq 8 \end{cases}$

נכונה-ק האשנ אי-זוגי, אז a שארית ריבועית מודולו p^k $\iff$ a שארית ריבועית מודולו p.

הוכחה ל- (*):

צ"ל להוכיח שאם $k \geq 3$, אז a שארית ריבועית מודולו 2^k $\iff$ a שארית ריבועית מודולו 2^{k+1}.
ואז הטענה נובעת מאינדוקציה, כשאת הבסיס $k = 1, 2, 3$ בודקים בידיים.

$\Longrightarrow$ מיידי מההגדרות

$\Longleftarrow$ צריך להוכיח שאם a שארית ריבועית מודולו 2^k אז a שארית ריבועית מודולו 2^{k+1}, תחת ההנחה $k \geq 3$.

לפי ההנחה קיים x_1 כך ש- $x_1^2 \equiv a \pmod{2^k}$

המטרה - למצוא x כך ש $x^2 \equiv a \pmod{2^{k+1}}$

תת"ל נבדוק אם $x_1^2 \equiv a \pmod{2^{k+1}}$. אם כן, $x = x_1$ וסיימנו.

אם לא, נסמן $x = x_1 + 2^{k-1}$

$$x^2 = (x_1 + 2^{k-1})^2 = x_1^2 + 2^k \cdot x_1 + 2^{2k-2} \equiv a + 0 + 0 \equiv a \pmod{2^k}$$
$$2k - 2 \geq k$$

מה קורה $\pmod{2^{k+1}}$?

$y_1 = x_1^2 \equiv a \pmod{2^k} \not\equiv a \pmod{2^{k+1}}$

$y_2 = 2^k x_1 \equiv 0 \pmod{2^k} \not\equiv 0 \pmod{2^{k+1}}$

$y_1 \not\equiv a \pmod{2^{k+1}}$
$y_1 \equiv y_1 + y_2 \equiv a \pmod{2^k}$
$y_1 \not\equiv y_1 + y_2 \pmod{2^{k+1}}$

יש בדיוק 2 מס' שטוחים ל- a מודולו 2^k בקבוצה $\{0, 1, \ldots, 2^{k+1}-1\}$, a שונה מבדיוק אחד מהם מודולו 2^{k+1}, לכן $y_1 + y_2 \equiv a \pmod{2^{k+1}}$, והוכחנו.

שיטת ההעתק הפיתולית

מה כללה: $\mathbb{Z}_{m_1 m_2} \to \mathbb{Z}_{m_1, m_2}$
$\mathbb{Z}[x] \longrightarrow \mathbb{Z}[x]$

הרעיקה מוגדרת היטב, מכבדת את פעולות החיבור והכפל, ולכן הוא הומומורפיזם. ב- $\mathbb{Z}_m$ יש בדיוק 2^m מקורות תחת ההעתקה.

אם יש לנו משוואה ואנו יודעים לפתור אותה ב- $\mathbb{Z}_{m_1}$ ו-$\mathbb{Z}_{m_2}$ ומעוניינים להרצות שהמקורות של הפיתרון נותנות את כל המחלקות האפשריות ב- $\mathbb{Z}_{m_1, m_2}$, אז יש פיתרון ב- $\mathbb{Z}_{m_1, m_2}$

דוגמה - רוצים לפתור $x^2 \equiv 9 \pmod{16}$

מסתכלים על המשוואה מודולו 8: $x^2 \equiv 1 \pmod 8$

↳ 1, 3, 5, 7

נקח $x_1 = 1$. הוכח על פתרון מודולו 16.
המטרה היא לייצר מיתן פתרון מודולו 16.
נקח את $x = 5$ (כמו בהוכחה, $x_{k+1} = x_k + 2^{k-1}$)

תזכורת

נתבונן למקרה $p \geq 3$ כאשר $m = p$. $a \in \mathbb{Z}_p^*$.

הוכחנו שמספר השאריות הריבועיות מודולו p הוא $\frac{p-1}{2}$
ו- ו- - השאריות - ו- - $\frac{p-1}{2}$

סימון לג'נדר: $a \in \mathbb{Z}_p^*$, p ראשוני:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ שארית ריבועית } \pmod p \\ -1 & \text{אחרת} \end{cases}$$

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

קריטריון אוילר - $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$

הטענה של שאלה - $p \geq 3$ ראשוני, $a \in \mathbb{Z}_p^*$. אז $\left(\frac{a}{p}\right) = (-1)^\lambda$

כאשר $\lambda = \left|\left\{ j \mid \text{הנציג היחיד של } aj \text{ מודולו } p \text{ שייך ל } \left[-\frac{p-1}{2}, \frac{p-1}{2}\right] \right\}\right|$

דוגמה - נחשב $\left(\frac{3}{11}\right)$. אפשר להסתכל על $\{3 \cdot j \mid j = 1,2,3,4,5\} =$
$= \{3, 6, 9, 12, 15\} =$
$= \{3, -5, -2, 1, 4\}$

נציגי השאריות $\pmod{11}$ בקטע $[-5, 5]$ ←

יש כאן שני שליליים $\Leftarrow \lambda = 2 \Leftarrow \left(\frac{3}{11}\right) = (-1)^2 = 1$

ואכן $5^2 = 25 \equiv 3 \pmod{11}$

כל המספרים הללו שונים מודולו p כי a הפיך מודולו p

דרך אחרת: באמצעות קריטריון אוילר:
$3^5 \equiv 9 \cdot 9 \cdot 3 \equiv -2 \cdot -2 \cdot 3 \equiv 12 \equiv 1 \pmod{11}$