

$x^2 \equiv a \pmod{m}$ :  $\exists x \in \mathbb{Z}$  אם  $m$  מודולו  $x$  יס

מחשבו הטאריות היסני טבע שאם  $m = 2^{\alpha} p_1^{r_1} \dots p_k^{r_k}$  אז  $a$  שארית ריבועית מודולו  $m$  אם ורק אם שארית ריבועית מודולו  $2^{\alpha}$  ו- $a$  שארית ריבועית מודולו  $p_i^{r_i}$  ( $p_0=2$ )

(\*) האילו -  $a$  שארית ריבועית מודולו  $2^k$   $\Leftrightarrow$   $\begin{cases} \pmod{2^k}, & 2^k=2,4 \\ \pmod{8}, & 2^k \geq 8 \end{cases}$  (א או - צי)

$\Leftrightarrow$  נראה  $p$  ראשוני או צי, אז  $a$  שארית ריבועית מודולו  $p^k$  אם ורק אם שארית ריבועית מודולו  $p$ .

קונתה - (4):  
 צד להוכיח שאם  $23 \nmid a$  אז  $a$  שארית ריבועית מודולו  $2^k$   $\Leftrightarrow$   $a$  שארית ריבועית מודולו  $2^{k+1}$ .  
 נצי הטצה נובעת מאינדוקציה, כשאם הבסיס  $2, 3, 4, \dots$  בודקים בידיים.

$\Rightarrow$  מיני מההצרות  
 $\Leftarrow$  ציין להוכיח שאם  $a$  שארית ריבועית מודולו  $2^k$  אז  $a$  שארית ריבועית מודולו  $2^{k+1}$ , תחת ההנחה  $23 \nmid a$ .

לפי ההנחה קיים  $x$  כך  $x^2 \equiv a \pmod{2^k}$   
 הטרה - למצוא  $x$  כך  $x^2 \equiv a \pmod{2^{k+1}}$   
 תחילה נבדוק אם  $x^2 \equiv a \pmod{2^{k+1}}$  אם כן,  $x = x_1 + 2^k u$ .

אם לא, נטמן  $x = x_1 + 2^{k-1} u$   
 $x^2 \equiv (x_1 + 2^{k-1} u)^2 \equiv x_1^2 + 2^k x_1 u + 2^{2k-2} u^2 \equiv a + 0 + 0 \equiv a \pmod{2^k}$   
 $\uparrow 2k-2 \geq k$

$y_1 = x_1^2 \equiv a \pmod{2^k} \not\equiv a \pmod{2^{k+1}}$  מה קורה  $\pmod{2^{k+1}}$ ?  
 $y_2 = 2^k x_1 u \equiv 0 \pmod{2^k} \not\equiv 0 \pmod{2^{k+1}}$   
 $y_1 \neq a \pmod{2^{k+1}}$   
 $y_1 \equiv y_1 + y_2 \equiv a \pmod{2^k}$   
 $y_1 \not\equiv y_1 + y_2 \pmod{2^{k+1}}$   
 יש בדיוק 2 מס' שטוים -  $a$  מודולו  $2^k$  בקבוצה  $\mathbb{Z}/2^{k+1}\mathbb{Z}$ .  
 $a$  שונה לבדיוק אחד מהם מודולו  $2^{k+1}$ ,  $a$  לכך  $y_1 + y_2 \equiv a \pmod{2^{k+1}}$  והוכחנו.

שיטת ההתפתחות

הצדקה מעברת היצע, מוכחת את פעולות החיבור והכפל, זל, ולכאוצר  $\mathbb{Z}/m_1\mathbb{Z}$  יש בדיוק  $m_2$  מקלות תחת ההצדקה.  
 $\mathbb{Z}/m_1\mathbb{Z} \rightarrow \mathbb{Z}/m_2\mathbb{Z}$   
 $[a] \rightarrow [a]$   
 אם יש לנו מטואה ואלו זדעים לפתר אותה  $\mathbb{Z}/m_1\mathbb{Z}$  ומצליחים להראות שהמקלות של הפיתרון ניתנות את כל המחלקות האפשריות  $\mathbb{Z}/m_1\mathbb{Z}$  או יש פיתרון  $\mathbb{Z}/m_2\mathbb{Z}$ .

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

$x^2 \equiv 1 \pmod{8}$

$\hookrightarrow 1, 3, 5, 7$

מסתכלים על המשוואה מודולו 8:

נבחר  $x=1$ . קיבא על פתרון מודולו 16.   
 המטרה היא לייצר מימין פיתרון מודולו 18.   
~~נבחר~~ נבחר את  $x=5$  (כמו בהוכחה,  $x+2^{k+1}=1+4$ )

תצבות

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

הוכחנו שספר הטאיות הראשיות  $1, \dots, \frac{p-1}{2}$  הריבועיות מודולו  $p$  הוא  $\frac{p-1}{2}$ .   
 ספר הטאיות השניות  $\frac{p+1}{2}, \dots, p-1$  הוא  $\frac{p-1}{2}$ .

סימן לבנדר:  $a \in \mathbb{Z}_p^*$ ,  $p$  ראשוני:   
 $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{אם } a \text{ ריבועי מודולו } p \\ -1 & \text{אחרת} \end{cases}$

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

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

הערה של גאוס -  $p \geq 3$  ראשוני,  $a \in \mathbb{Z}_p^*$  ו-  $l$    
 $\left(\frac{a}{p}\right) = (-1)^l$    
 כאשר  $l = \left| \left\{ \begin{matrix} \text{הנציבים היחידים של } a \text{ מודולו } p \\ \text{בקיטע } \left[-\frac{p-1}{2}, \frac{p-1}{2}\right] \text{ שונים} \end{matrix} \right\} \right|$

דוגמה - נחשב  $\left(\frac{3}{11}\right)$ . עלינו להסתכל על  $\{j \mid j=1, 2, 3, 4, 5\}$    
 $\rightarrow \{3, 6, 9, 12, 15\} \equiv \{3, -5, -2, 1, 4\}$    
 נציג העתקים מודולו 11 בקטע  $[-5, 5]$

$\left(\frac{3}{11}\right) = (-1)^2 = 1 \leftarrow l=2 \neq$  שני שלילים   
 ואכן  $5^2 = 25 \equiv 3 \pmod{11}$

כל המספרים האלה שונים מודולו  $p$  כי הפך מודולו  $p$    
 זיק אחת. באמצעות קריטריון אוילר:   
 $3^5 \equiv 9 \cdot 9 \cdot 3 \equiv -2 \cdot -2 \cdot 3 \equiv 12 \equiv 1 \pmod{11}$