

$a \in \mathbb{Z}_p$, ראשוני $p \geq 3$ כאשר $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{אם } x^2 \equiv a \pmod{p} \text{ פתור} \\ -1 & \text{אם לא} \end{cases}$

מטעם הקצוות הרביעיות (גאוס 1796):
 נניח $p, q \geq 3$ ראשוניים. אז:

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}$$

נוכיח שוב את מטעם הקצוות הרביעיות - דפי Kim 2004

שפתאם בתוצאת הקאמי שכבר הוכח:
 - מטעם ויטון - $(p-1)! \equiv -1 \pmod{p}$
 - קריטריון אוילר - $a \in \mathbb{Z}_p$ אם $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

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

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

$$p \mid \left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}}$$

הוכחה: מקריטריון אוילר.

$$\in \{0, \pm 2\}, \quad p \neq 2$$

$$\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} = 0 \quad \text{אם } p \equiv 1 \pmod{4}$$

- מטעם השאלות הישנות - אם m, m_2 זרים, $b_1, b_2 \in \mathbb{Z}$
 אז יש $x \in \mathbb{Z}$ כן ש- $x \equiv b_1 \pmod{m_1}$
 $x \equiv b_2 \pmod{m_2}$
 ומתקיים ש- x הוא יחיד באיבר \mathbb{Z}_{m, m_2}

II הוכחה

$$F = \{a \in \mathbb{Z}_1, \dots, \frac{p-1}{2} \mid \gcd(a, pq) = 1\}$$

$$A = \prod_{a \in F} a \quad \text{כבר "הוכח" - } \sum_{a \in F} a$$

$$A \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}, \quad A \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p} \quad \text{דמה I}$$

$$S = \{a \in \mathbb{Z}_1, \dots, \frac{p-1}{2} \mid \gcd(a, p) = 1\} \quad \text{הוכחה - נסמן}$$

$$T = \{2q, 2q, \dots, \frac{2(p-1)}{2}\}$$

$$S = T \cup F \quad \text{אז יש } S = T \cup F$$

אם $p \equiv 1 \pmod{4}$ אז $\frac{p-1}{2}$ זוגי, אז F מכיל את $1, 2, \dots, \frac{p-1}{2}$
 ואם $p \equiv 3 \pmod{4}$ אז $\frac{p-1}{2}$ אי-זוגי, אז F מכיל את $1, 2, \dots, \frac{p-1}{2}$
 ואם $p \equiv 1 \pmod{4}$ אז $\frac{p-1}{2}$ זוגי, אז F מכיל את $1, 2, \dots, \frac{p-1}{2}$

$$\prod_{a \in S} a \equiv \prod_{a \in T} a \cdot \prod_{a \in F} a \pmod{p}$$

$$\prod_{a \in S} a \equiv \prod_{a \in T} a \cdot \prod_{a \in F} a \pmod{p} = A \cdot q^{\frac{p-1}{2}} \left(\frac{p}{2}\right)! \equiv A \left(\frac{p}{2}\right) \left(\frac{p-1}{2}\right)! \pmod{p}$$

$$\prod_{a \in T} a \equiv \frac{p-1}{2}! \pmod{p}$$

$$\prod_{a \in S} a \equiv ((p-1)!)^{\frac{p-1}{2}} \cdot ((p-1)/2)! \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{2}\right)! \pmod{p}$$

המשק הוכחת העמדה:

$$A \left(\frac{q}{p}\right) \left(\left(\frac{p-1}{2}\right)!\right) \equiv (-1)^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}$$

קימנו ש-

$$A \left(\frac{q}{p}\right) \equiv (-1)^{\frac{q-1}{2}} \pmod{p} \Rightarrow A \equiv \left(\frac{q}{p}\right) (-1)^{\frac{q-1}{2}} \pmod{p}$$

עמדה ± 1 - התנאים הבאים מקובלים:

$$(-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \quad - א$$

$$A \equiv \pm 1 \pmod{pq} \quad - ב$$

$$p \equiv q \equiv 1 \pmod{4} \quad - ג$$

~~$B \equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$~~

הוכחה: א' \Leftarrow ב'

A פותר שתי משוואות.
מהיחידות במשפט השני, יש רק מספר אחד שמתר
אז שתי המשוואות (מוזולו p, q).
מספר זה הוא המספר היחיד ג-א, שהוא ± 1
ב' \neq א'

נסמן ב- B נציג של A ב- ג' $\left\{ \frac{p-1}{2}, \dots, \frac{p-1}{2} \right\}$

אז $B = \pm 1$

אם מסתכלים מוזולו p אז $B \equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$
נסתעם על ההפרש ומקבלים מספר שנקרא δ - מוזולו p,
והוא בקבוצה $\{2, \pm 2, \dots, \pm 2\}$, δ מספר זה הוא אפס.

דכן $B = (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right)$ ו באופן דומה $B = (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right)$

ב' \Leftrightarrow ג'

נסמן $m = pq$

נסתעם על $x^2 \equiv 1 \pmod{m}$

עמדה זו יש 2 פתרונות מוזולו p - $\pm 1 \pmod{p}$

1-2 פתרונות מוזולו q - $\pm 1 \pmod{q}$

מקבלים 4 מספרים שונים: $(\pm 1, \pm N)$

~~...~~

(חסר חלק מההוכחה):

נקרא ש:

לפני p, q יש 4 פתרונות $x^2 \equiv 1 \pmod{pq}$ -

והם מהצורה $\{ \pm 1, \pm N \}$ ($N \neq \pm 1$)

אם $p \equiv q \equiv 1 \pmod{4}$ אז יש 4 פתרונות גם $x^2 \equiv -1 \pmod{pq}$ -

והם מהצורה $\{ \pm I, \pm IN \}$ ($I \neq \pm 1, \pm N, \pm IN$)

אם לא מתקיים $p \equiv q \equiv 1 \pmod{4}$ אז אין פתרונות $x^2 \equiv -1 \pmod{pq}$ -

נשים לב שכל $a \in F$ ו $a' \in F$ יחיד נק ש- $aa' \equiv \pm 1 \pmod{pq}$

כי לכל $a \in F$ a הפך מוזולו p, q , ולכן אסור עבור $ab \equiv 1 \pmod{pq}$

אם $b \in F$ נסמן $a' = b$ אם $a \neq f$ אז $-b \in F$, ונסמן $a' = -b$

ואז $aa' \equiv -1 \pmod{pq}$

$$F_0 = \{a \in F \mid a' \neq a\}$$

- |N|

$$A = \prod_{a \in F} a = \prod_{a \in F_0} a \cdot \prod_{b \in F_0} b = \pm \prod_{b \in F_0} b \equiv \pm \begin{cases} 1 \cdot 1 \cdot N \cdot 1 \cdot N \\ 1 \cdot N \end{cases} \quad \begin{matrix} p \equiv q \equiv 1 \pmod{4} \\ \text{אחרת} \end{matrix}$$

$$p \equiv q \equiv 1 \pmod{4} \quad \text{כאן מתקיים} \quad \begin{matrix} 1 \cdot N = N \not\equiv \pm 1 \pmod{pq} \\ A \not\equiv \pm 1 \pmod{pq} \end{matrix} \quad \text{אם}$$

$$A \equiv \pm 1^2 \cdot N^2 \equiv \pm 1 \pmod{pq} \quad \text{אם} \quad p \equiv q \equiv 1 \pmod{4} \quad \text{אם}$$

והוכחנו את הטענה.

הוכחת המשפט

מתקיימות של א' ו-ב' בטענה 2 טבע :

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = \begin{cases} (-1)^{\frac{1}{2}(p-1)(q-1)} & p \equiv q \equiv 1 \pmod{4} \\ (-1)^{\frac{1}{2}(p-1)(q-1)+1} & \text{אחרת} \end{cases} \quad (*)$$

נעביר את כל המקרים מודולו 4. אם $p \equiv q \equiv 1 \pmod{4}$ אז

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)(q-1)} = 1 = (-1) \quad \text{אם הוכחנו:}$$

↑
בזרים במקרה $p \equiv q \equiv 1 \pmod{4}$

$p \equiv 1, q \not\equiv 1$	$(\pmod{4})$	באופן דומה עבורים של המקרים
$p \not\equiv 1, q \equiv 1$		
$q \equiv 1, p \not\equiv 1$		

$$(-1)^{\frac{1}{2}(p-1)(q-1)} \quad \text{וככל המקרים חסום ש-} (*) \quad \text{שווה } -1$$