

קיים x כך $x^2 \equiv a \pmod{p}$ - נ-א $\left(\frac{a}{p}\right) = \begin{cases} 1 \\ -1 \end{cases}$ כאשר $a \in \mathbb{Z}_p$, ראשוני $p \geq 3$ סימן של a יחסית ל- p

משפט הקדמות הריבועיות (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 משפט הקדמות הריבועיות - דפי Kim 2004

נשתמש ב-
 - משפט וילסון: $(p-1)! \equiv -1 \pmod{p}$
 - קריטריון אוילר - $a \in \mathbb{Z}_p$ אם $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$

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

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

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

$$\left(\frac{-1}{p}\right) - (-1)^{\frac{p-1}{2}} \in \{0, \pm 2\}, \quad p \neq 2$$

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

- משפט השאריות הסיני - אם m_1, m_2 זרים, $b_1, b_2 \in \mathbb{Z}$
 אז יש $x \in \mathbb{Z}$ כך ש-
 $x \equiv b_1 \pmod{m_1}$
 $x \equiv b_2 \pmod{m_2}$
 ומתקיים $x \equiv a \pmod{m_1 m_2}$ - ה- a יחיד

הוכחה II

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

$$A = \prod_{a \in F} a \pmod{p}$$

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

$$S = \{a \in \{1, \dots, \frac{p-1}{2}\} \mid \gcd(a, p) = 1\}$$

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

$$S = T \cup F$$

אז S מכיל את F ואת T .
 נניח $p \equiv 1 \pmod{4}$, אז $\frac{p-1}{2}$ זוגי.
 אז T מכיל את F ואת T .
 אז S מכיל את F ואת T .

$$\prod_{a \in S} a \pmod{p}$$

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

$$\frac{p-1}{2} = \frac{p-1}{2} p + \frac{p-1}{2}$$

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

המשק הוכחת העזרה:

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

$$\Downarrow$$

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

עזרה II - התנאים הבאים מקלים:

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

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

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

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

הוכחה: א' $\Leftarrow$ ב'

A פתר שתי משוואות.
מהימדות במשפט השני, י"ש רק מספר אחד טפולר
אז שתי המשוואות (מוצאים) (pq) .
מספר זה הוא המספר המופיע ב-א', שהוא ± 1
ב' $\Leftarrow$ א'

$$\left\{ \frac{pq-1}{2}, \dots, \frac{pq-1}{2} \right\} \quad - ב' \quad A \quad \text{של} \quad B \quad \text{נציג} \quad \text{של} \quad A \quad - ב'$$

אז $B = \pm 1$
אם מסתכלים מוצאים p אז $B \equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \pmod{p}$
נסתכל על ההפרש ומקבלים מספר טפולר $\delta - 0$ מוצאים p ,
וקיב בקבוצה $\{2, \pm 2, \dots, \pm 2\}$, עכן מספר זה הוא אפס.

$$B \equiv (-1)^{\frac{p-1}{2}} \left(\frac{q}{p}\right) \quad \text{עכן} \quad B = (-1)^{\frac{q-1}{2}} \left(\frac{p}{q}\right) \quad \text{ואז באופן דומה}$$

ב' $\Leftrightarrow$ ג'

$$m = pq \quad \text{נסמן}$$

נסתכל על $x^2 \equiv 1 \pmod{m}$
עמנואל זו יש 2 פתרונות מוצאים $\pm 1 \pmod{p}$
1-2 פתרונות מוצאים $\pm 1 \pmod{q}$
מקבלים 4 מספרים שונים: $(\pm 1, \pm N)$
 ~~$x^2 \equiv 1 \pmod{pq}$~~
: (חזר חלק מההוכחה)

נקבל ש:
עכ p, q יש 4 פתרונות $\delta - x^2 \equiv 1 \pmod{pq}$
והם מהצורה $\{ \pm 1, \pm N \}$ ($N \neq \pm 1$)

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

נשים לב שכל $a \in F$ ו $a' \in F$ יחיד כך ש- $aa' \equiv \pm 1 \pmod{pq}$
כי עכ $a \in F$ יפך מוצאים q , ועכן אסטר עסטר $ab \equiv 1 \pmod{pq}$
אם $a \in F$ נסמן $a' = b$, אם $a' \neq a$ אז $-b \in F$, ונסמן $a' = b$
ואז $aa' \equiv -1 \pmod{pq}$

$$F_0 = \{a \in F \mid a \neq a^2\}$$

נסמן

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

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

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

והוכחנו את הטענה.

הוכחת המשפט

מהטענות של א' ו-ב' נראה ש-2 טבעי:

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

נעביר על כל המקרים מודול 4. אם $p \equiv q \equiv 1 \pmod{4}$

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{1}{2}(p-1)(q-1)} = 1 = (-1) \quad \text{אם הוכחנו:} \\ \uparrow \quad \text{במקרים במקרה } p \equiv q \equiv 1 \pmod{4}$$

$$\begin{matrix} p \equiv 1, q \not\equiv 1 \\ p \not\equiv 1, q \equiv 1 \\ q \equiv 1, p \not\equiv 1 \end{matrix} \quad \begin{matrix} \text{אז } p \equiv q \equiv 1 \pmod{4} \\ \text{אז } p \equiv q \equiv 1 \pmod{4} \\ \text{אז } p \equiv q \equiv 1 \pmod{4} \end{matrix} \quad \text{אז } p \equiv q \equiv 1 \pmod{4}$$

$$(-1)^{\frac{1}{2}(p-1)(q-1)} = -1 \quad (*) \quad \text{אם } p \equiv q \equiv 1 \pmod{4}$$