

$a \in \mathbb{Z}_p^*$ נקרא שארית חיבורית מודולו p
אם יש $x \in \mathbb{Z}_p$ כך ש- $x^2 \equiv a \pmod{p}$

סימן עז נדר: אם $p \geq 3$ הנוסח טיב
$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{אם } a \text{ הוא רבוע מרובע} \\ -1 & \text{אחרת} \end{cases}$$

הערה של גאוס: אם $p \geq 3$ ראשוני, $a \in \mathbb{Z}_p^*$ נסמן $j = 1, 2, \dots, \frac{p-1}{2}$
עבור $a_j \equiv j^2 \pmod{p}$, $a_j \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ ו- a_j אינן הופקו זהות
 $a_j \equiv j^2 \pmod{p}$, $a_j \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$

$\mathcal{A} = \{a_j \mid j=1, 2, \dots, \frac{p-1}{2}, a_j \not\equiv 0 \pmod{p}\}$ אינן נסמן

$\left(\frac{a}{p}\right) = (-1)^{|\mathcal{A}|}$ ומתקיים

משפט - חוק ההדדיות הריבועית quadratic reciprocity
נניח $p, q \geq 3$ ראשוניים.

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

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

ניתן לכתוב גם כך:

דוגמה - נחשב את $\left(\frac{15}{71}\right)$

$$\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right) \left(\frac{5}{71}\right) = (-1)^{\frac{3-1}{2} \cdot \frac{71-1}{2}} \cdot \left(\frac{71}{3}\right) \cdot (-1)^{\frac{5-1}{2} \cdot \frac{71-1}{2}} \cdot \left(\frac{71}{5}\right) =$$

$$= -\left(\frac{2}{3}\right) \cdot \left(\frac{1}{5}\right) = -(-1)(1) = 1$$

הערה - וואסר האוס: במאה ה-17 נחשף שהמשפט נכון והשתמש בו, הוא הוכח לכאורה ע"י גאוס ב-1796 (נעדרה בן 19).
במהלך חייו פרסם עוד 3 הוכחות, ו-2 נוספות נמצאו בכתביו לאחר מותו.
עצ- היום ממשיכים לתת הוכחות חדשות, כיום יש 246 הוכחות נ-2020.

הוכחה

נסמן V ו- μ בהתאמה את המספרים של המופעים בעלם של a ו- $a=p$ שניהם עם $a=p$ ו- $a=q$ במקום p .
אז - פעם אחת עם $a=q$ ופעם אחת עם $a=p$.

במילים אחרות, V הוא מספר האיזוקטים $\left\{\frac{p-1}{2}, \dots, 1\right\}$ ו- μ הוא מספר האיזוקטים $\left\{-\frac{p-1}{2}, \dots, -1\right\}$.
שם $a_j \equiv j^2 \pmod{p}$ ו- $a_j \in \left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$ הוא שילוב.

מ' מתקבל מהכיתת תפקודי q ו- p בהצגה של V .

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\mu+V}$$

$$\mu+V = \frac{1}{4}(p-1)(q-1) \pmod{2}$$

יהי $x \in \mathbb{Z}$ הנמצא שם $xq - yp$ כאשר y קטן
הוא מהצורה $[-\frac{p-1}{2}, \frac{p-1}{2}]$ שם y

$$\frac{xq}{p} - \frac{1}{2} < y < \frac{xq}{p} + \frac{1}{2} \iff -\frac{p}{2} < xq - yp < \frac{p}{2}$$

$$\iff y \in (\frac{xq}{p} - \frac{1}{2}, \frac{xq}{p} + \frac{1}{2}) \iff y \in [\frac{xq}{p} - \frac{1}{2}, \frac{xq}{p} + \frac{1}{2}]$$

מאחר ששדה קטן, אם x יט בדיוק y אחד ממקומות את התנאי.

נבדוק אם $x=1, \dots, \frac{p-1}{2}$ $y \geq 0$: א-
שם y : א- (כי הקטע $[\frac{xq}{p} - \frac{1}{2}, \frac{xq}{p} + \frac{1}{2}]$ מאריך או מסתחב)

ב- אם $y=0$, $xq - yp = xq$, x זה לא טרם
מספר v מספר את מספר ה- x יום עבורם $xq - yp < 0$.
אז יותר להשלים ממנו כמסתובב את v .

ג- $y \geq 1$:
 $\frac{1}{2}(q-1) = \frac{1}{2}p \cdot \frac{2}{p} - \frac{1}{2} > \frac{xq}{p} - \frac{1}{2}$
 y הוא השם $y \leq \frac{1}{2}(q-1)$ קטן ביותר שבדול
נ- $\frac{xq}{p} - \frac{1}{2}$, $y \leq \frac{1}{2}(q-1)$ קטן ביותר

$$1 \leq y \leq \frac{q-1}{2}$$

$$S = \left\{ x \in \mathbb{Z} \mid \dots, \frac{p-1}{2} \mid xq - yp < 0 \right\}$$

y השם היחיד בקטע $[\frac{xq}{p} - \frac{1}{2}, \frac{xq}{p} + \frac{1}{2}]$

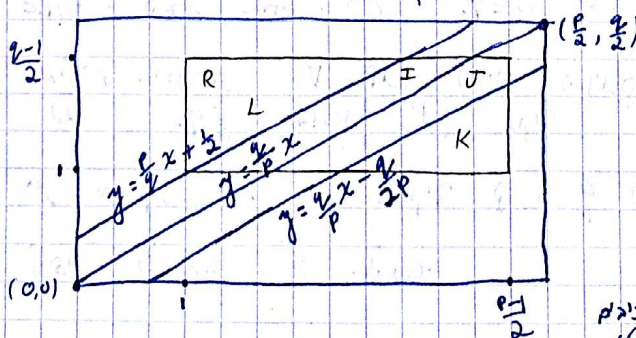
$$I = \left\{ (x, y) \in \mathbb{Z}^2 \mid \begin{array}{l} 1 \leq x \leq \frac{p-1}{2} \\ 1 \leq y \leq \frac{q-1}{2} \\ -\frac{p}{2} < xq - yp < 0 \end{array} \right\}$$

$$|I| = |S| = v$$

מחילתם עקבי p, q , ונקט $\mu = |J|$

$$J = \left\{ (x, y) \in \mathbb{Z}^2 \mid \begin{array}{l} 1 \leq y \leq \frac{1}{2}(q-1) \\ 1 \leq x \leq \frac{1}{2}(p-1) \\ -\frac{1}{2} < xq - yp < 0 \end{array} \right\}$$

אחרון צריכים למצוא את העצמות של $|J| + |I|$
(מכיוון אותן במישור (x, y) שם $0 < xq - yp < \frac{p}{2}$)



$$R = \left\{ (x, y) \in \mathbb{R}^2 \mid \begin{array}{l} 1 \leq x \leq \frac{p-1}{2} \\ 1 \leq y \leq \frac{q-1}{2} \end{array} \right\}$$

$$|\mathbb{Z}^2 \cap R| = \frac{1}{2}(p-1) \cdot \frac{1}{2}(q-1) = \frac{1}{4}(p-1)(q-1)$$

שמן ה- K ו- L את שני הכיוונים
של $(J \cup I) \setminus R$ (כמו בגרף)

די להוכיח ש- $K \cup L$ מספר זוגי של נקודות שלמות!
 $|L \cap \mathbb{Z}^2| = |K \cap \mathbb{Z}^2|$

נמצא התאמה חד"ע ואם בין א-ע L, שמעצורה נקודות שלמות
ענקודות שלמות. התאמה ניתנת ז"י נצ"י שיקוף סביב מרכז המלבן R.

המרחב של R נ"ח $(\frac{p+1}{q}, \frac{q+1}{2})$

$$\begin{pmatrix} x \\ y \end{pmatrix} \mapsto \begin{pmatrix} x \\ y \end{pmatrix} + 2 \begin{pmatrix} \frac{p+1}{4} - x \\ \frac{q+1}{2} - y \end{pmatrix} = \begin{pmatrix} \frac{p+1}{2} - x \\ \frac{q+1}{2} - y \end{pmatrix} : \text{הפוך השני}$$

← נסמן טקורה ב $\begin{pmatrix} x' \\ y' \end{pmatrix}$

ההצגה $\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x' \\ y' \end{pmatrix}$ הפכה למעבירה $\begin{pmatrix} x' \\ y' \end{pmatrix} = M \begin{pmatrix} x \\ y \end{pmatrix}$ כאשר $M = \begin{pmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{pmatrix}$

ברור שההצדקה למעבירה שפה אופקית של R לעברה אופקית של R מתחלפת
וכנ"ל עבור שפות אלכסוניות. לכן צי לבדוק שמעבירה את האלמנט $xq - y = \frac{q}{2}$
שמעביר את a אל אלמנט $xq - y = -\frac{p}{2}$.
עושים את החשבון ונחלים שכן.

UN'01

ישירות נסח סמטה של גאוס

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{8}}$$

מחפץ - ה' $p \geq 3$ ראשון. SL

$$(-1) \frac{p^2 - 1}{8}$$

הערה - לבין תחילה את ממוצות הביטוי

שני מספרים : $p = 4K + 1$, $p = 4K + 3$, K מספר

$$\frac{p^2-1}{8} = \frac{(4k+1)^2-1}{8} = \frac{16k^2+8k+1-1}{8} = 2k^2+k \equiv k \pmod{2} \quad \because \text{sk } p=4k+1 \quad p \equiv 1 \pmod{4}$$

$$\frac{p^2-1}{8} = \frac{(4K+3)^2-1}{8} = \frac{16K^2+24K+9-1}{8} = 2K^2+3K+1 \equiv K+1 \pmod{2}$$

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases} \quad : p \text{ odd}$$

$$r = \frac{p-1}{2} \quad | \text{ נח - נח}$$

P פרמיום 2, 4, 6, ... $2n = p-1$ שלם להיבטון הציבים אמת ציבים
ש"ס כזה n $[r, r]$ ש"ס δ
 p $p = 4K+3$ $p = 4K+1$ נכיר סקרים

אם $p = 4k + 1$, $r = 2k$ הכפולות של 2 בקטע $[-2k, 2k]$
 הן $2, 4, 6, \dots, 2k$ ← כפולות דו-בית (מספרן k)
 $-1, -2k+3, \dots, -2k+1, -(4k+1)+2, 2k+2$ ← כפולות שליליות (מספרן k)
 סך הכול k זוגות של מספרים

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

$$r = 2k + 1 \quad p = 4k + 3 \quad p|c$$

הכ פונקטור $k_2, \dots, k_n$ הן חיוניות ומספרן k

ההנחות $-1, -2k+1, \dots, -2k-1, -(4k+3), \dots, -2k+2$ בן טענות ומספר $k+1$.

$$\left(\frac{2}{p}\right) = (-1)^{k+1} = (-1)^{\frac{p-1}{8}}$$