

$a \in \mathbb{Z}_p^*$  קטן שאותו חיבור מוצאון  $x^2 \equiv a \pmod{p}$  אם יש  $x \in \mathbb{Z}_p$  כן -  $x^2 \equiv a \pmod{p}$

סימן עש'נדר: אם  $p \geq 3$  הנוסח'ן טול

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

הערה של גאוס: אם  $p \geq 3$  הנוסח'ן טול  $a \in \mathbb{Z}_p^*$  נסמן  $j = 1, 2, \dots, \frac{p-1}{2}$   $a_j \in \mathbb{Z}_p^*$   $a_j \equiv ja \pmod{p}$  את הטבל'ה המקי'ם

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

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

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

ומתקיים

משפט - חוק ההדדיות הריבועית quadratic reciprocity

נתק' אוז'  $p, q \geq 3$  ראשוניים.

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

ניתן לכתוב גם כך:

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

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

$$\left(\frac{15}{71}\right) = \left(\frac{3}{71}\right) \left(\frac{5}{71}\right) = (-1)^{\frac{1}{2}(2 \cdot 70)} \cdot \left(\frac{71}{3}\right) \cdot (-1)^{\frac{1}{2}(4 \cdot 70)} \cdot \left(\frac{71}{5}\right) =$$

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

הצרה - וואסח גאוס: במאה ה-17 נחש' שהמשפט נכון והשתמש בו, הוא הוכח לכאורה ע'י גאוס ב-1796 (נשהר בן 19). במהלך חייו פתסם אזר צ'הנחות, ו-2 נוספות נמצאו בכתביו לכהנך מיטל.

ע'ז - היום ממשיכים לתת הוכחות חדשות, כיום יש 246 הוכחות נ-2022.

הוכחה

נסמן  $V$  - ו-  $\mu$  בהתאמה את המספרים  $\mu$  המופיעים בעמ'ה של גאוס - פסג אחת עם  $a=q$ , ו-  $\mu$  פסג שניה עם  $a=p$ , ו-  $\mu$  בקוק  $p$ .

במילים אחרות,  $V$  הוא מספר האינדקסים  $\{1, 2, \dots, \frac{p-1}{2}\}$  של  $q^j$  מוצאון  $p$  בקטע  $[-\frac{p-1}{2}, \frac{p-1}{2}]$  הוא עש'ים.

$\mu$  מתקבל מהפיכת תבוקיזי  $q-1$  בהצדקה של  $V$ .

עפי' העמ'ה של גאוס:

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

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







למצוא התאמה חד"ע ועל כן  $L = \delta - \alpha$  שמעבירה מקודות שלמות לנקודות שלמות. ההתאמה ניתנת  $\vec{y} = \vec{z} + \vec{a}$  סביב מרכז המלבן  $R$ .

המרכז של  $R$  נתון  $\vec{y} = (\frac{p+1}{4}, \frac{q+1}{2})$ .

הטיקוף הנוט:  $\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x \\ y \end{pmatrix} + 2 \begin{pmatrix} \frac{p+1}{4} - x \\ \frac{q+1}{2} - y \end{pmatrix} = \begin{pmatrix} \frac{p+1}{2} - x \\ \frac{q+1}{2} - y \end{pmatrix}$

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

ההעתקה  $\begin{pmatrix} x \\ y \end{pmatrix} \rightarrow \begin{pmatrix} x' \\ y' \end{pmatrix}$  הפכה ומעבירה שלמים לשלמים.

ברור שההעתקה למעבירה שפה אופקית של  $R$  לטובה אפקית של  $R$  סממורה וכך עבור שפות אלכסוניות. לכן צו לבדוק שמעבירה את האלכסון  $xq - y = \frac{p-1}{2}$  שמעביר את  $\frac{p-1}{2}$  אלכסון  $xq - y = \frac{p-1}{2}$ . אז שים את החשבון והואים טב.

וסיימנו.

**שימוע טסל עמלה של גאוס**

מנפט - ה'  $p \geq 3$  ראשוני. אז  $\left(\frac{p-1}{p}\right) = (-1)^{\frac{p-1}{8}}$

הערה - בין תחילה למשמעות הביטוי  $p = 4k + 1$  ו  $p = 4k + 3$   $k$  שלם. עכיד לטני מקרים:

אם  $p = 4k + 1$  אז:  $\frac{p^2-1}{8} = \frac{(4k+1)^2-1}{8} = \frac{16k^2+8k+1-1}{8} = \frac{16k^2+8k}{8} = 2k^2+k \equiv k \pmod{2}$

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

עס'טים:  $(-1)^{\frac{p-1}{8}} = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases}$

הינחה - נמן  $r = \frac{p-1}{2}$

אמת צרכים להיבון בנצנים של  $p-1 = 2r$   $2, 4, 6, \dots, 2r$  מוצו  $p$  שטיים לקטע  $[r, -r]$  וזהויל כמה מהם שליליים. נכיד למקרים  $p = 4k + 1$  ו  $p = 4k + 3$  שלם.

אם  $p = 4k + 1$   $r = 2k$  הכפולות של 2 בקטע  $[-2k, 2k]$  הן  $2, 4, 6, \dots, 2k$  כפולות חיוביות (מספרן  $k$ )  $-1, -2, -3, \dots, -2k+1, -2k+2, -4k+2 = 2k$  כפולות שליליות, (מספרן  $k$ ) לכן במקרה זה,  $l = k$  עט העמה של גאוס:  $\left(\frac{p}{p}\right) = (-1)^k = (-1)^{\frac{p-1}{8}}$

אם  $p = 4k + 3$   $r = 2k + 1$  הכפולות  $2, 4, \dots, 2k$  הן חיוביות ומספרן  $k$  והכפולות  $-1, -2, -3, \dots, -2k+1, -2k+2, -4k+2 = 2k$  הן שליליות ומספרן  $k+1$ . לכן במקרה זה  $l = k+1$  ועט העמה של גאוס:  $\left(\frac{p}{p}\right) = (-1)^{k+1} = (-1)^{\frac{p-1}{8}}$