

ד"ר יעקובי (Jacobi)

י"י n חסר אי' a-1 ו n-1 (mod n)

$$\left(\frac{1}{n}\right) = 1 \quad \text{כ"י נכנס ל n} \quad \left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right) \quad \begin{matrix} \uparrow & \uparrow \\ \text{חסר אי'} & \text{חסר אי'} \end{matrix}$$

$\left(\frac{a}{n}\right) = 0$ אם a חסר אי' n-1 ו n-1 (mod n) הכונות

1) אם $a \equiv b \pmod{n}$ אז $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$ אם $a \equiv b \pmod{n}$ אז $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$

2) קשר לטבלאות היקפיות: $x^2 \equiv a \pmod{n}$ - חסר אי' n-1 ו n-1 (mod n) הכונות

אם $x^2 \equiv a \pmod{n}$ אז $x^2 \equiv a \pmod{p_i}$ לכל p_i חסר אי' n-1 ו n-1 (mod n) הכונות

3) $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_k}\right)$ אם a חסר אי' n-1 ו n-1 (mod n) הכונות

4) $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2}\right) \dots \left(\frac{a}{p_k}\right)$ אם a חסר אי' n-1 ו n-1 (mod n) הכונות

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

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

$$\left(\frac{-1}{n}\right) = \prod_i \left(\frac{-1}{p_i}\right) = \prod_i (-1)^{\frac{p_i-1}{2}} = (-1)^{\sum \frac{p_i-1}{2}}$$

ונוסחה נוספת: $\sum \frac{p_i-1}{2} = \frac{n-1}{2} \pmod{2}$ אם $n = p_1 \dots p_k$ חסר אי' n-1 ו n-1 (mod n) הכונות

שק, $p_1, \dots, p_k$ ו- m, n נק

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(m-1)(n-1)}$$

$p_1, \dots, p_k$

$q_1, \dots, q_l$

$$h = p_1 p_2 \dots p_k$$

$$m = q_1 q_2 \dots q_l$$

הוכחה

$$\left(\frac{m}{n}\right) \left(\frac{n}{m}\right) = \left(\frac{q_1}{p_1}\right) \left(\frac{p_1}{q_1}\right) \cdot \left(\frac{q_2}{p_2}\right) \left(\frac{p_2}{q_2}\right) \dots = \text{שק}$$

$$= \prod_{i,j} \left(\frac{q_i}{p_j}\right) \left(\frac{p_j}{q_i}\right) = \prod_{i,j} (-1)^{\frac{1}{4}(p_j-1)(q_i-1)} =$$

$$= (-1)^{\sum_{i,j} \frac{1}{4}(p_j-1)(q_i-1)}$$

$$\sum_{i,j} \frac{1}{4}(p_j-1)(q_i-1) = \frac{1}{4}(m-1)(n-1) \quad \text{נח ונראה}$$

$$\left(\sum_i \frac{1}{2}(q_i-1)\right) \cdot \left(\sum_j \frac{1}{2}(p_j-1)\right)$$

$$\left(\frac{1777}{997}\right) \left(\frac{997}{1777}\right) = \text{שק}$$

$$= \left(\frac{2}{997}\right) \cdot \left(\frac{357}{997}\right) = -\left(\frac{357}{997}\right) = -\left(\frac{997}{357}\right) \cdot (-1)^{\frac{1}{4}(996)(356)} =$$

$$= -\left(\frac{997}{357}\right) = -\left(\frac{283}{357}\right) = -\left(\frac{357}{283}\right) \cdot (-1)^{\frac{1}{4}(356)(82)} =$$

$$= -\left(\frac{357}{283}\right) = -\frac{74}{283} = -\left(\frac{2}{283}\right) \cdot \left(\frac{37}{283}\right) = \dots = \left(\frac{2}{13}\right) = -1$$

הוכחה חזק הוויכוח:

$(\frac{p}{q}) = (-1)^u$ שני האיברים באותו:

$(\frac{q}{p}) = (-1)^u$

כאשר u, v מספרים שלמים.

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

$(\frac{q}{p})$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

$V = \{ (x, y) \in \mathbb{Z}^2 \mid 1 \leq x \leq \frac{1}{2}(p-1), 1 \leq y \leq \frac{1}{2}(q-1), \frac{p}{2} < xq - yp < 0 \}$

$\exists b \in \mathbb{Z} \mid [xq - yp] \in [\frac{1}{2}(p-1), \frac{1}{2}(p-1)] \wedge$

$\wedge xq - yp < 0 \}$

$-\frac{p}{2} < xq - yp < \frac{p}{2}$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

$(\frac{p}{q}) = (-1)^u$ שני האיברים באותו:

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

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

$-\frac{p}{2} < xq - yp < 0$

$1 \leq x \leq \frac{1}{2}(p-1)$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

$xq - yp < 0$ כי $y > \frac{p}{2}$ כי $y \leq \frac{1}{2}(q-1)$ כי $y > \frac{p}{2}$ כי $y \leq \frac{1}{2}(q-1)$

$xq - yp \leq \frac{1}{2}(p-1) - (\frac{1}{2}(q-1) + 1)p = -\frac{q}{2} - \frac{p}{2} < -\frac{p}{2}$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

הוכחה חזקה: נניח u מספר שלם. הוכחנו כי $(\frac{p}{q}) = (-1)^u$

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

$0 < xq - yp < \frac{p}{2}$

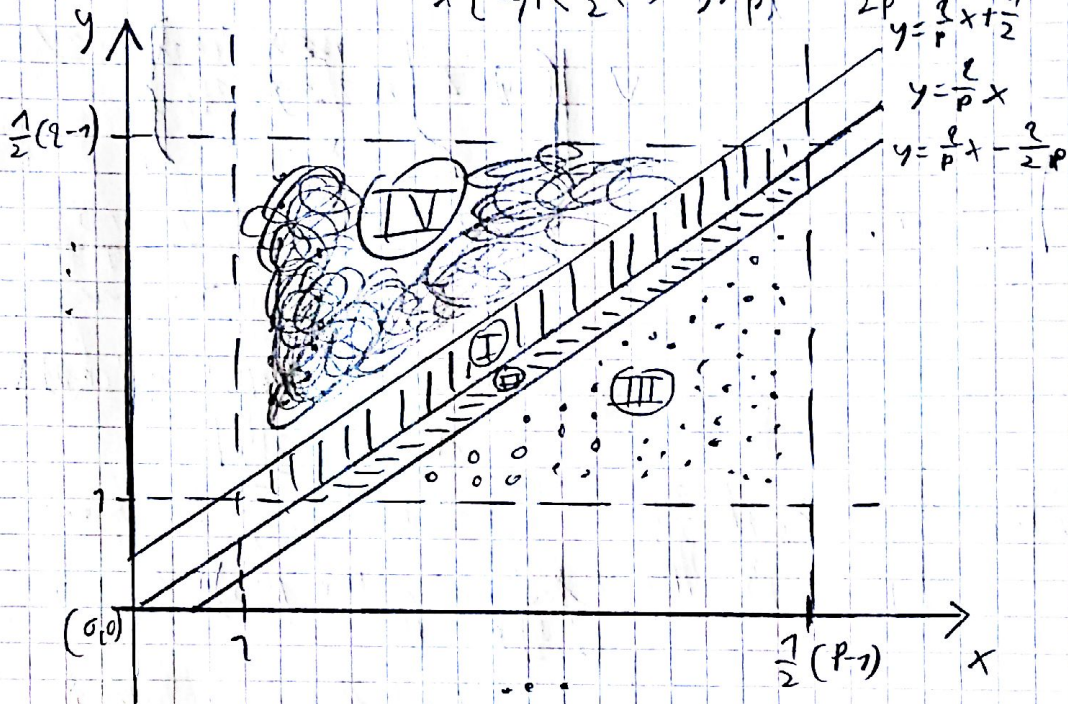
נבדוק את התנאים בהינתן q, p ונראה כי $q \equiv 1 \pmod{2}$.

$$xq - yp < 0 \Leftrightarrow y > \frac{qx}{p}$$

$$xq - yp > 0 \Leftrightarrow y < \frac{qx}{p}$$

$$xq - yp > \frac{p}{2} \Leftrightarrow y < \frac{qx}{p} + \frac{1}{2}$$

$$xq - yp < \frac{q}{2} \Leftrightarrow y > \frac{qx}{p} - \frac{1}{2p}$$



נבדוק את המקרה $q < p$ או $2q > p$.

התוצאה היא שההפרש

$$u + v \equiv \frac{1}{2}(p-1)(q-1) \pmod{2}$$

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

המספר הנק' הוא מספר הנק' (I, II, III, IV) הנמצאים בתוך המלבול, ונראה כי מספר הנק' הנמצאים בתוך המלבול הוא $\frac{1}{2}(p-1)(q-1)$.

$$\lambda = \left| \left\{ (x, y) \in \mathbb{Z}^2 \mid \begin{matrix} 1 \leq x \leq \frac{1}{2}(p-1) \\ 1 \leq y \leq \frac{1}{2}(q-1) \\ xq - yp > \frac{p}{2} \end{matrix} \right\} \right|$$

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

$$x' = \frac{1}{2}(p+1) - x$$

$$y' = \frac{1}{2}(q+1) - y$$

$$1 \leq x' \leq \frac{1}{2}(p-1) \Leftrightarrow 1 \leq x \leq \frac{1}{2}(p-1) \quad \text{ו} \quad 1 \leq y' \leq \frac{1}{2}(q-1) \Leftrightarrow 1 \leq y \leq \frac{1}{2}(q-1)$$

$$x'q - y'p > \frac{q}{2} \iff xq - yp < -\frac{p}{2} \quad \text{p.d.}$$

$$x'q - y'p = \left(\frac{1}{2}(p+\eta) - x\right)q - \left(\frac{1}{2}(q+\eta) - y\right)p = \frac{1}{2}(p+\eta)q - \frac{1}{2}(q+\eta)p - (xq - yp) = \frac{q}{2} - \frac{p}{2} - (xq - yp)$$