

למה (עולה): יור, $p \equiv 1 \pmod{8}$, $p-1$ נכנס ל- 8 , k זוגי
 $\rightarrow$ a_j זוגיים, $\delta(p)$ $\in [-\frac{p-1}{2}, \frac{p-1}{2}]$ אז
 $L = \{j \leq \frac{p-1}{2} : a_j < 0\}$ כעת $(\frac{a}{p}) = (-1)^{|L|}$ ש.פ

הוכחה: ראשונים הבה

באמצעות נקודת גורר, $1 \leq a \leq p-1$

כגון: $\frac{p-1}{2} \leq \frac{p-1}{2} = 5$ $a \in [-5, 5]$ $p=11$

$$\left. \begin{array}{l} 3 \cdot 7 \equiv 3 \\ 3 \cdot 2 \equiv -5 \\ 3 \cdot 3 \equiv -2 \\ 3 \cdot 4 \equiv 1 \\ 3 \cdot 5 \equiv 4 \end{array} \right\}$$

$$(mod \ 11) \Rightarrow L=2 \Rightarrow \left(\frac{3}{11}\right) = (-1)^2 = 1$$

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases} = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$$

$$r \in \{-1, 1, -3, 3\}, p = 8k + r$$

הוכחה: נראה כי $p \equiv \pm 1 \pmod{8}$ נכנס ל- 8

$$\frac{p^2-1}{2} = \frac{64k^2 + 64kr + r^2 - 1}{2} = \frac{r^2-1}{2} \pmod{2}$$

$$= \frac{r^2-1}{8} = \begin{cases} 0 & r = \pm 1 \\ 1 & r = \pm 3 \end{cases} \pmod{2}$$

נראה כי $p \equiv \pm 3 \pmod{8}$ אינו נכנס ל- 8

נניח $p \equiv \pm 3 \pmod{8}$, $p-1 \equiv \pm 2 \pmod{8}$, $p-1$ אינו נכנס ל- 8

$$\left[-\frac{p-1}{2}, \frac{p-1}{2}\right]$$

נראה כי $2 \leq 2j \leq 2 \lfloor \frac{p}{4} \rfloor \leq 2 \cdot \frac{p}{4} = \frac{p}{2}$ $j \leq \lfloor \frac{p}{4} \rfloor$ $2j \leq \frac{p-1}{2}$ a_j זוגיים
 $\rightarrow$ a_j זוגיים, $\delta(p)$ $\in [-\frac{p-1}{2}, \frac{p-1}{2}]$ אז $L = \{j \leq \frac{p-1}{2} : a_j < 0\}$ כעת $(\frac{a}{p}) = (-1)^{|L|}$ ש.פ

$$2j \leq \frac{p-1}{2} \Rightarrow 2j \leq \frac{p-1}{2} = \frac{p-1}{2} : \lfloor \frac{p}{4} \rfloor \leq j \leq \frac{p-1}{2}$$

$$2j \leq \frac{p-1}{2} \Rightarrow 2j \leq \frac{p-1}{2} = \frac{p-1}{2} : \lfloor \frac{p}{4} \rfloor \leq j \leq \frac{p-1}{2}$$

$$2j \leq \frac{p-1}{2} \Rightarrow 2j \leq \frac{p-1}{2} = \frac{p-1}{2} : \lfloor \frac{p}{4} \rfloor \leq j \leq \frac{p-1}{2}$$

וכן נראה כי $p \equiv \pm 1 \pmod{8}$

2.3). $r \in \{1, 2, 3, -3\}$ $p = 2 \text{ Mr}$

וְיָמֵי הַיָּדָוָה יִשְׁמְרוּ אֶת הַיָּדָוָה לְעַד וְיִשְׁמְרוּ אֶת הַיָּדָוָה לְעַד

[illegible]

$$L = \frac{p-1}{2} \left[\frac{p}{q} \right] + yk + \frac{r-1}{2} \left[2k + \frac{r}{q} \right] =$$

$$= 2K + \frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor \equiv \frac{r-1}{2} - \left\lfloor \frac{r}{4} \right\rfloor = \begin{cases} 0 & r \equiv \pm 1 \\ 1 & r \equiv \pm 3 \end{cases} \pmod{2}$$

$$\begin{pmatrix} -2 \\ p \end{pmatrix} = \begin{pmatrix} 12 \\ p \end{pmatrix} \begin{pmatrix} -1 \\ p \end{pmatrix} = \begin{cases} 1, & p \equiv 1,3 \pmod{8} \\ -1, & p \equiv 5,7 \pmod{8} \end{cases}$$

הערתו כי יכליות סמל טעם וצדק

2012.12.25 a sk. '11.12.18 = 444 121 '11.12.18 9713 '11.12.18

ר' מ' צ' מ' 13/1

סגירת ק"ק - $\text{ord}_p(2) = p-1$ - p איננו מתחלק ב-2

$$2^7 \# 7 \pmod{P} \cdot x \cdot \{7, 2, 7, 8, 2, 4, 9\} = 1 \text{ for } x=1$$

$$2^4 = 16 \equiv 1 \pmod{17}$$

$$75 \equiv 0 \pmod{p}$$

$$p \mid n5 \Rightarrow p \in \{3, 5\}$$

$p = 49172 - e$ מסת' ו' ו' ק

$$74.3 + 7 = 73$$

$$2^{\frac{2^q-1}{2}} \equiv \binom{2}{p} \pmod{p} \text{ p.k. } 2^{\frac{2^q-1}{2}} \pmod{p} \quad \text{p.k. } 2^{\frac{2^q-1}{2}} \pmod{p}$$

שם ירמיהו
א"ל

$$2^{2^2} \equiv (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(49+7)^2-1}{8}} = (-1)^{2^2+9} = (-1)^9 = -1 \pmod{p}$$

$\text{ord}_p(2) = p-1$

כאשר $\binom{q}{p}$ שווה ל-1, נובע / איננו אחר / אומר
 כי $\binom{q}{p} = 1$ כאשר $p=0$ או $p=q$, מכיוון שיש רק דרך אחת
 לבחור 0 איברים או כל האיברים.

נראה כי, להגדל את $\binom{q}{p}$ כך

$$\binom{q}{p} = 1 \cdot \binom{q-1}{p-1}$$

משפט 1.1 (חוקי החצייה) $\binom{q}{p} = \binom{q}{q-p}$

הוכחה: נניח $p \leq q/2$. נראה כי:

$$\binom{q}{p} = \frac{q!}{p!(q-p)!} = \frac{q!}{p!(q-p)!} \cdot \frac{(q-p)!}{(q-p)!} = \frac{q!}{p!(q-p)!} \cdot \frac{(q-p)!}{(q-p)!} = \frac{q!}{p!(q-p)!} = \binom{q}{q-p}$$

$$\binom{3}{1} = \frac{3!}{1!2!} = \frac{3 \cdot 2 \cdot 1}{1 \cdot 2 \cdot 1} = 3$$

$$= \binom{3}{2} = \frac{3!}{2!1!} = \frac{3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 1} = 3$$

$$\binom{3}{0} = 1$$

$$\binom{5}{1} = \frac{5!}{1!4!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{1 \cdot 4 \cdot 3 \cdot 2 \cdot 1} = 5$$

$$\binom{5}{2} = \frac{5!}{2!3!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2 \cdot 1 \cdot 3 \cdot 2 \cdot 1} = 10$$

$$\binom{5}{3} = \frac{5!}{3!2!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{3 \cdot 2 \cdot 1 \cdot 2 \cdot 1} = 10$$

$$\binom{5}{4} = \frac{5!}{4!1!} = \frac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{4 \cdot 3 \cdot 2 \cdot 1 \cdot 1} = 5$$

$$\binom{5}{0} = 1$$

$$\binom{5}{5} = 1$$