

קונגרואנציות ריבועיות

$$x^2 \equiv a \pmod{n}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{אם } a \text{ הוא ריבוע מרובות} \\ -1 & \text{אם } a \text{ אינו ריבוע מרובות} \end{cases}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

$$x \equiv m \pmod{a} \iff \frac{x}{a} \equiv \frac{m}{a} \pmod{1}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

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

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

$$\begin{aligned} x^2 &\equiv 1 \pmod{p} \Rightarrow p \mid x^2 - 1 \\ &\Rightarrow p \mid (x-1)(x+1) \Rightarrow x \equiv \pm 1 \pmod{p} \end{aligned}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

$$a^{\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$$

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הקבוצה $\{a \in \mathbb{Z} : a \equiv 1 \pmod{4}\}$ היא קבוצת ריבועים מרובות

הסקנה: יחידות a, b זרים p ראשוני

הוכחה: מקראו א' לר: $\left(\frac{a}{p}\right) \left(\frac{b}{p}\right) \equiv \left(\frac{ab}{p}\right) \pmod{p}$

הסקנה: יחידות $p \geq 3$ זר, $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$

הוכחה: מקראו א' לר: $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$

$\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$ נקרא כי:

עליון דאמיון יחידות p ראשוני $p \geq 3$ זר, $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$

הסקנה: $\left(\frac{32}{7}\right) = \left(\frac{-1}{7}\right) = -1$

$7 \equiv 3 \pmod{4}$ כי

יחידות: נכתב מקראו א' לר: $ax^2 + bx + c \equiv 0 \pmod{h}$

$ax^2 + bx + c \equiv 0 \pmod{h}$
 $a \neq 0, a \not\equiv 0 \pmod{h}$

נחלק בקוטר a נכחל a - $4a$

$ax^2 + bx + c \equiv 0 \pmod{h}$



$4a(ax^2 + bx + c) \equiv 0 \pmod{4ah}$

$4a^2x^2 + 4abx + 4ac \equiv 0 \pmod{4ah}$

$(2ax + b)^2 = b^2 + 4ac \pmod{4ah}$

$2ax + b = y \quad \text{לכן } (2ax + b)^2 = b^2 - 4ac \pmod{4ah}$

$y^2 \equiv b^2 - 4ac \pmod{4ah}$

יחידות y זר h זר a זר h

$2ax + b \equiv y \pmod{4ah}$

$ax^2 + bx + c \equiv 0 \pmod{h}$

לכן



$2ax + b \equiv y \pmod{4ah}$

$y^2 \equiv b^2 - 4ac \pmod{4ah}$

$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$

היתכונות, יחידות

$$n = p_1^{j_1} \cdots p_k^{j_k}$$

p_{r_i}

שנים אלו בתחנות.

זכמות וזכות, כחמט.

$$p-1 \nmid a_{-j_1, 1, p, 1}, \quad x^2 \equiv a \pmod{p^j}$$

שני המסמכים פורמליים, כיוון ש'א' שולח ת'מ"ל' ת/ת"ו/11 פ"ק ת"ס כחוב

$$a_{p^j-1}(p^j) = \frac{\phi(p^j)}{p^{j-1}(p-1)}$$

$$= a^{\frac{p-1}{2}} \equiv 1 \pmod{p^j}$$

$$\frac{\psi(6)}{2}$$

$-\lambda_0$ מס' הן x_0 מס' הן $\gcd(z, \phi(e')) = 2$ e', λ_0 $e' \in K$

[illegible]

'd/s' k a, 57,7, p² ≡ α(mod 5) 1.2, 3, 7, 11, N,

$$a \equiv 1 \pmod{2} : j=1$$

$\alpha \equiv 3 \quad /k \quad \alpha \equiv 7 \quad /k \quad \therefore j=2$

$$1, 3 \equiv \pm 7 \pmod{4} \text{ and } 1, 1, 1, 1, 2, 1^2 \equiv 7 \pmod{4}$$

$$x^2 \equiv a \pmod{2^j} \quad \text{for } j \geq 3, \text{ then } a \equiv 1 \pmod{8} \quad \text{for } j \geq 3.$$

e' m n o k p̄ p̄ a ≡ r (mod g) s k l e' i g' i q' .

כמו כן, אם x כתובו 5 ב 4 הכתובות מ/א/א/ 2^ו הק

$$\cdot \pm x_{j+2}^{j-1}, \pm x_0$$

הנה כח 2: $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \pmod{8}$ לכן, $a \equiv 1 \pmod{8}$

541 י' 4 ב א וונא נח בורק נחיל

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

$$a \equiv 1 \pmod{8} \quad \text{sic} \quad x^2 \equiv a \pmod{8} \quad (\text{too sic})$$

4. $a \in \mathbb{Z}$ (mod) n ו- $b \in \mathbb{Z}$ (mod) n

2) $f(x) = x^2 + 1$

$x \equiv 1 \pmod{8}$, $x \equiv 1 \pmod{8}$

נניח x זוגי, נכתוב $x = 2^j \cdot x_0$, x_0 אי-זוגי, $j \geq 1$
 נניח x אי-זוגי, נכתוב $x = 2^j \cdot x_0$, x_0 זוגי, $j = 0$
 נניח x זוגי, נכתוב $x = 2^j \cdot x_0$, x_0 אי-זוגי, $j \geq 1$

$j+1$ 2 $x \equiv \pm x_0 + k \cdot 2^{j-1} \pmod{2^{j+1}}$, $k \in \mathbb{Z}$, x אי-זוגי, $j \geq 1$

$$x^2 \equiv x_0^2 + 2kx_0 \cdot 2^{j-1} + k^2 \cdot 2^{2j-2} \pmod{2^{j+1}}$$

$$2^{j-2} \geq j+1 \rightarrow x_0^2 + kx_0 \cdot 2^j \equiv x_0^2 + kx_0 \cdot 2^j \pmod{2^{j+1}}$$

 $j \geq 1$

נניח x_0 זוגי, נכתוב $x_0 = 2^j \cdot v$, v אי-זוגי, $j \geq 1$

$x_0^2 \equiv a \pmod{2^j} \Rightarrow x_0^2 = a + r \cdot 2^j$, $r \in \mathbb{Z}$
 נניח v אי-זוגי

$x^2 \equiv a + r \cdot 2^j + k \cdot x_0 \cdot 2^j = a + (r + kx_0) \cdot 2^j \pmod{2^{j+1}}$
 נניח k זוגי

$2^j (r + kx_0) \equiv 0 \pmod{2^{j+1}}$
 $\Leftrightarrow$

$r + kx_0 \equiv 0 \pmod{2}$
 $r + k \equiv 0 \pmod{2}$
 $k \equiv -r \equiv r \pmod{2}$

$j+1$ 2 $x_0^2 = a + r \cdot 2^j$, x_0 אי-זוגי, $j \geq 1$

$k \equiv r \pmod{2}$, $x = \pm x_0 + k \cdot 2^{j-1}$, $j \geq 1$

$x = \pm x_0 + (2m+r) \cdot 2^{j-1}$
 $= \pm x_0 + r \cdot 2^{j-1} + m \cdot 2^j$

$j+1$ 2 $x_0' = x_0 + r \cdot 2^{j-1}$, x_0' אי-זוגי, $j \geq 1$

$-x_0 + r \cdot 2^{j-1} = -x_0' + r \cdot 2^{j-1}$
 $= -(x_0 + r \cdot 2^{j-1}) + r \cdot 2^{j-1}$

אלגוריתם למציאת הנחלקות מודולרית
 קיבלנו $x^2 \equiv 17 \pmod{128}$ מודולרית
 אס סג נחלק -

$x^2 \equiv 17 \pmod{128}$
 נחלק x ב-8, נקבל x_0 כזה ש-
 $x_0^2 \equiv 17 \pmod{8}$
 נחלק x_0 ב-2, נקבל x_1 כזה ש-
 $x_1^2 \equiv 17 \pmod{16}$
 נחלק x_1 ב-4, נקבל x_2 כזה ש-
 $x_2^2 \equiv 17 \pmod{32}$
 נחלק x_2 ב-8, נקבל x_3 כזה ש-
 $x_3^2 \equiv 17 \pmod{64}$
 נחלק x_3 ב-16, נקבל x_4 כזה ש-
 $x_4^2 \equiv 17 \pmod{128}$
 נחלק x_4 ב-32, נקבל x_5 כזה ש-
 $x_5^2 \equiv 17 \pmod{256}$
 נחלק x_5 ב-64, נקבל x_6 כזה ש-
 $x_6^2 \equiv 17 \pmod{512}$
 נחלק x_6 ב-128, נקבל x_7 כזה ש-
 $x_7^2 \equiv 17 \pmod{1024}$
 נחלק x_7 ב-256, נקבל x_8 כזה ש-
 $x_8^2 \equiv 17 \pmod{2048}$
 נחלק x_8 ב-512, נקבל x_9 כזה ש-
 $x_9^2 \equiv 17 \pmod{4096}$
 נחלק x_9 ב-1024, נקבל x_{10} כזה ש-
 $x_{10}^2 \equiv 17 \pmod{8192}$
 נחלק x_{10} ב-2048, נקבל x_{11} כזה ש-
 $x_{11}^2 \equiv 17 \pmod{16384}$
 נחלק x_{11} ב-4096, נקבל x_{12} כזה ש-
 $x_{12}^2 \equiv 17 \pmod{32768}$
 נחלק x_{12} ב-8192, נקבל x_{13} כזה ש-
 $x_{13}^2 \equiv 17 \pmod{65536}$
 נחלק x_{13} ב-16384, נקבל x_{14} כזה ש-
 $x_{14}^2 \equiv 17 \pmod{131072}$
 נחלק x_{14} ב-32768, נקבל x_{15} כזה ש-
 $x_{15}^2 \equiv 17 \pmod{262144}$
 נחלק x_{15} ב-65536, נקבל x_{16} כזה ש-
 $x_{16}^2 \equiv 17 \pmod{524288}$
 נחלק x_{16} ב-131072, נקבל x_{17} כזה ש-
 $x_{17}^2 \equiv 17 \pmod{1048576}$
 נחלק x_{17} ב-262144, נקבל x_{18} כזה ש-
 $x_{18}^2 \equiv 17 \pmod{2097152}$
 נחלק x_{18} ב-524288, נקבל x_{19} כזה ש-
 $x_{19}^2 \equiv 17 \pmod{4194304}$
 נחלק x_{19} ב-1048576, נקבל x_{20} כזה ש-
 $x_{20}^2 \equiv 17 \pmod{8388608}$
 נחלק x_{20} ב-2097152, נקבל x_{21} כזה ש-
 $x_{21}^2 \equiv 17 \pmod{16777216}$
 נחלק x_{21} ב-4194304, נקבל x_{22} כזה ש-
 $x_{22}^2 \equiv 17 \pmod{33554432}$
 נחלק x_{22} ב-8388608, נקבל x_{23} כזה ש-
 $x_{23}^2 \equiv 17 \pmod{67108864}$
 נחלק x_{23} ב-16777216, נקבל x_{24} כזה ש-
 $x_{24}^2 \equiv 17 \pmod{134217728}$
 נחלק x_{24} ב-33554432, נקבל x_{25} כזה ש-
 $x_{25}^2 \equiv 17 \pmod{268435456}$
 נחלק x_{25} ב-67108864, נקבל x_{26} כזה ש-
 $x_{26}^2 \equiv 17 \pmod{536870912}$
 נחלק x_{26} ב-134217728, נקבל x_{27} כזה ש-
 $x_{27}^2 \equiv 17 \pmod{1073741824}$
 נחלק x_{27} ב-268435456, נקבל x_{28} כזה ש-
 $x_{28}^2 \equiv 17 \pmod{2147483648}$
 נחלק x_{28} ב-536870912, נקבל x_{29} כזה ש-
 $x_{29}^2 \equiv 17 \pmod{4294967296}$
 נחלק x_{29} ב-1073741824, נקבל x_{30} כזה ש-
 $x_{30}^2 \equiv 17 \pmod{8589934592}$
 נחלק x_{30} ב-2147483648, נקבל x_{31} כזה ש-
 $x_{31}^2 \equiv 17 \pmod{17179869184}$
 נחלק x_{31} ב-4294967296, נקבל x_{32} כזה ש-
 $x_{32}^2 \equiv 17 \pmod{34359738368}$
 נחלק x_{32} ב-8589934592, נקבל x_{33} כזה ש-
 $x_{33}^2 \equiv 17 \pmod{68719476736}$
 נחלק x_{33} ב-17179869184, נקבל x_{34} כזה ש-
 $x_{34}^2 \equiv 17 \pmod{137438953472}$
 נחלק x_{34} ב-34359738368, נקבל x_{35} כזה ש-
 $x_{35}^2 \equiv 17 \pmod{274877906944}$
 נחלק x_{35} ב-68719476736, נקבל x_{36} כזה ש-
 $x_{36}^2 \equiv 17 \pmod{549755813888}$
 נחלק x_{36} ב-137438953472, נקבל x_{37} כזה ש-
 $x_{37}^2 \equiv 17 \pmod{1099511627776}$
 נחלק x_{37} ב-274877906944, נקבל x_{38} כזה ש-
 $x_{38}^2 \equiv 17 \pmod{2199023255552}$
 נחלק x_{38} ב-549755813888, נקבל x_{39} כזה ש-
 $x_{39}^2 \equiv 17 \pmod{4398046511104}$
 נחלק x_{39} ב-1099511627776, נקבל x_{40} כזה ש-
 $x_{40}^2 \equiv 17 \pmod{8796093022208}$
 נחלק x_{40} ב-2199023255552, נקבל x_{41} כזה ש-
 $x_{41}^2 \equiv 17 \pmod{17592186044416}$
 נחלק x_{41} ב-4398046511104, נקבל x_{42} כזה ש-
 $x_{42}^2 \equiv 17 \pmod{35184372088832}$
 נחלק x_{42} ב-8796093022208, נקבל x_{43} כזה ש-
 $x_{43}^2 \equiv 17 \pmod{70368744177664}$
 נחלק x_{43} ב-17592186044416, נקבל x_{44} כזה ש-
 $x_{44}^2 \equiv 17 \pmod{140737488355328}$
 נחלק x_{44} ב-35184372088832, נקבל x_{45} כזה ש-
 $x_{45}^2 \equiv 17 \pmod{281474976710656}$
 נחלק x_{45} ב-70368744177664, נקבל x_{46} כזה ש-
 $x_{46}^2 \equiv 17 \pmod{562951913380544}$
 נחלק x_{46} ב-140737488355328, נקבל x_{47} כזה ש-
 $x_{47}^2 \equiv 17 \pmod{1125903826761088}$
 נחלק x_{47} ב-281474976710656, נקבל x_{48} כזה ש-
 $x_{48}^2 \equiv 17 \pmod{2251807653522176}$
 נחלק x_{48} ב-562951913380544, נקבל x_{49} כזה ש-
 $x_{49}^2 \equiv 17 \pmod{4503615307044352}$
 נחלק x_{49} ב-1125903826761088, נקבל x_{50} כזה ש-
 $x_{50}^2 \equiv 17 \pmod{9007230614088704}$
 נחלק x_{50} ב-2251807653522176, נקבל x_{51} כזה ש-
 $x_{51}^2 \equiv 17 \pmod{18036121228177408}$
 נחלק x_{51} ב-4503615307044352, נקבל x_{52} כזה ש-
 $x_{52}^2 \equiv 17 \pmod{36072242456354816}$
 נחלק x_{52} ב-9007230614088704, נקבל x_{53} כזה ש-
 $x_{53}^2 \equiv 17 \pmod{72144484912709632}$
 נחלק x_{53} ב-18036121228177408, נקבל x_{54} כזה ש-
 $x_{54}^2 \equiv 17 \pmod{144288964825419264}$
 נחלק x_{54} ב-36072242456354816, נקבל x_{55} כזה ש-
 $x_{55}^2 \equiv 17 \pmod{288577929650838528}$
 נחלק x_{55} ב-72144484912709632, נקבל x_{56} כזה ש-
 $x_{56}^2 \equiv 17 \pmod{576955858301677056}$
 נחלק x_{56} ב-144288964825419264, נקבל x_{57} כזה ש-
 $x_{57}^2 \equiv 17 \pmod{1153911716603354112}$
 נחלק x_{57} ב-288577929650838528, נקבל x_{58} כזה ש-
 $x_{58}^2 \equiv 17 \pmod{2307823433206708224}$
 נחלק x_{58} ב-576955858301677056, נקבל x_{59} כזה ש-
 $x_{59}^2 \equiv 17 \pmod{4615646866433416448}$
 נחלק x_{59} ב-1153911716603354112, נקבל x_{60} כזה ש-
 $x_{60}^2 \equiv 17 \pmod{9231293732866832896}$
 נחלק x_{60} ב-2307823433206708224, נקבל x_{61} כזה ש-
 $x_{61}^2 \equiv 17 \pmod{18462587465733665792}$
 נחלק x_{61} ב-4615646866433416448, נקבל x_{62} כזה ש-
 $x_{62}^2 \equiv 17 \pmod{36925174931467331584}$
 נחלק x_{62} ב-9231293732866832896, נקבל x_{63} כזה ש-
 $x_{63}^2 \equiv 17 \pmod{73850349862934663168}$
 נחלק x_{63} ב-18462587465733665792, נקבל x_{64} כזה ש-
 $x_{64}^2 \equiv 17 \pmod{147700699725869326336}$
 נחלק x_{64} ב-36925174931467331584, נקבל x_{65} כזה ש-
 $x_{65}^2 \equiv 17 \pmod{295401399451738652672}$
 נחלק x_{65} ב-73850349862934663168, נקבל x_{66} כזה ש-
 $x_{66}^2 \equiv 17 \pmod{590802798903473265344}$
 נחלק x_{66} ב-147700699725869326336, נקבל x_{67} כזה ש-
 $x_{67}^2 \equiv 17 \pmod{1181605597806946530688}$
 נחלק x_{67} ב-295401399451738652672, נקבל x_{68} כזה ש-
 $x_{68}^2 \equiv 17 \pmod{2363211195613893061376}$
 נחלק x_{68} ב-590802798903473265344, נקבל x_{69} כזה ש-
 $x_{69}^2 \equiv 17 \pmod{4726422391227786122752}$
 נחלק x_{69} ב-1181605597806946530688, נקבל x_{70} כזה ש-
 $x_{70}^2 \equiv 17 \pmod{9452844782455572245504}$
 נחלק x_{70} ב-2363211195613893061376, נקבל x_{71} כזה ש-
 $x_{71}^2 \equiv 17 \pmod{18905689564911144491008}$
 נחלק x_{71} ב-4726422391227786122752, נקבל x_{72} כזה ש-
 $x_{72}^2 \equiv 17 \pmod{37811379129822288982016}$
 נחלק x_{72} ב-9452844782455572245504, נקבל x_{73} כזה ש-
 $x_{73}^2 \equiv 17 \pmod{75622758259644574904032}$
 נחלק x_{73} ב-18905689564911144491008, נקבל x_{74} כזה ש-
 $x_{74}^2 \equiv 17 \pmod{151245516519289149808064}$
 נחלק x_{74} ב-37811379129822288982016, נקבל x_{75} כזה ש-
 $x_{75}^2 \equiv 17 \pmod{312491033038578299616128}$
 נחלק x_{75} ב-75622758259644574904032, נקבל x_{76} כזה ש-
 $x_{76}^2 \equiv 17 \pmod{624982066077156599232256}$
 נחלק x_{76} ב-151245516519289149808064, נקבל x_{77} כזה ש-
 $x_{77}^2 \equiv 17 \pmod{1249964132154313198464512}$
 נחלק x_{77} ב-312491033038578299616128, נקבל x_{78} כזה ש-
 $x_{78}^2 \equiv 17 \pmod{2499928264308626396929024}$
 נחלק x_{78} ב-624982066077156599232256, נקבל x_{79} כזה ש-
 $x_{79}^2 \equiv 17 \pmod{4999856528617252793858048}$
 נחלק x_{79} ב-1249964132154313198464512, נקבל x_{80} כזה ש-
 $x_{80}^2 \equiv 17 \pmod{9999713057234505587716096}$
 נחלק x_{80} ב-2499928264308626396929024, נקבל x_{81} כזה ש-
 $x_{81}^2 \equiv 17 \pmod{19999426114469011175432192}$
 נחלק x_{81} ב-4999856528617252793858048, נקבל x_{82} כזה ש-
 $x_{82}^2 \equiv 17 \pmod{39998852228938022350864384}$
 נחלק x_{82} ב-9999713057234505587716096, נקבל x_{83} כזה ש-
 $x_{83}^2 \equiv 17 \pmod{79997704457876044701728768}$
 נחלק x_{83} ב-19999426114469011175432192, נקבל x_{84} כזה ש-
 $x_{84}^2 \equiv 17 \pmod{159995408915752089403457536}$
 נחלק x_{84} ב-39998852228938022350864384, נקבל x_{85} כזה ש-
 $x_{85}^2 \equiv 17 \pmod{319990817831504178806915072}$
 נחלק x_{85} ב-79997704457876044701728768, נקבל x_{86} כזה ש-
 $x_{86}^2 \equiv 17 \pmod{639981635663008357613830144}$
 נחלק x_{86} ב-159995408915752089403457536, נקבל x_{87} כזה ש-
 $x_{87}^2 \equiv 17 \pmod{1279963271326016715227660288}$
 נחלק x_{87} ב-319990817831504178806915072, נקבל x_{88} כזה ש-
 $x_{88}^2 \equiv 17 \pmod{2559926542652033430455320576}$
 נחלק x_{88} ב-639981635663008357613830144, נקבל x_{89} כזה ש-
 $x_{89}^2 \equiv 17 \pmod{5119853085304066860910641152}$
 נחלק x_{89} ב-1279963271326016715227660288, נקבל x_{90} כזה ש-
 $x_{90}^2 \equiv 17 \pmod{10239706170608133721821282304}$
 נחלק x_{90} ב-2559926542652033430455320576, נקבל x_{91} כזה ש-
 $x_{91}^2 \equiv 17 \pmod{20479412341216267443642564608}$
 נחלק x_{91} ב-5119853085304066860910641152, נקבל x_{92} כזה ש-
 $x_{92}^2 \equiv 17 \pmod{40958824682432534887285129216}$
 נחלק x_{92} ב-10239706170608133721821282304, נקבל x_{93} כזה ש-
 $x_{93}^2 \equiv 17 \pmod{81817649364865069774570258432}$
 נחלק x_{93} ב-20479412341216267443642564608, נקבל x_{94} כזה ש-
 $x_{94}^2 \equiv 17 \pmod{163635298729730139549140516864}$
 נחלק x_{94} ב-40958824682432534887285129216, נקבל x_{95} כזה ש-
 $x_{95}^2 \equiv 17 \pmod{327270597459460279098281033728}$
 נחלק x_{95} ב-81817649364865069774570258432, נקבל x_{96} כזה ש-
 $x_{96}^2 \equiv 17 \pmod{654541194918920558196562067456}$
 נחלק x_{96} ב-163635298729730139549140516864, נקבל x_{97} כזה ש-
 $x_{97}^2 \equiv 17 \pmod{1309082389837841116393124134912}$
 נחלק x_{97} ב-327270597459460279098281033728, נקבל x_{98} כזה ש-
 $x_{98}^2 \equiv 17 \pmod{2618164779675682232786248269824}$
 נחלק x_{98} ב-654541194918920558196562067456, נקבל x_{99} כזה ש-
 $x_{99}^2 \equiv 17 \pmod{5236329559351364465572496539648}$
 נחלק x_{99} ב-1309082389837841116393124134912, נקבל x_{100} כזה ש-
 $x_{100}^2 \equiv 17 \pmod{10472659118702728931144993079296}$
 נחלק x_{100} ב-2618164779675682232786248269824, נקבל x_{101} כזה ש-
 $x_{101}^2 \equiv 17 \pmod{20945318237405457862289986158592}$
 נחלק x_{101} ב-5236329559351364465572496539648, נקבל x_{102} כזה ש-
 $x_{102}^2 \equiv 17 \pmod{41890636474810915724579972317184}$
 נחלק x_{102} ב-10472659118702728931144993079296, נקבל x_{103} כזה ש-
 $x_{103}^2 \equiv 17 \pmod{83781272949621831449159944634368}$
 נחלק x_{103} ב-20945318237405457862289986158592, נקבל x_{104} כזה ש-
 $x_{104}^2 \equiv 17 \pmod{167562545899243662898319889268736}$
 נחלק x_{104} ב-41890636474810915724579972317184, נקבל x_{105} כזה ש-
 $x_{105}^2 \equiv 17 \pmod{335125091798487325796639778537472}$
 נחלק x_{105} ב-83781272949621831449159944634368, נקבל x_{106} כזה ש-
 $x_{106}^2 \equiv 17 \pmod{670250183596974651593279557074944}$
 נחלק x_{106} ב-167562545899243662898319889268736, נקבל x_{107} כזה ש-
 $x_{107}^2 \equiv 17 \pmod{1340500367193949303186559114149888}$
 נחלק x_{107} ב-335125091798487325796639778537472, נקבל x_{108} כזה ש-
 $x_{108}^2 \equiv 17 \pmod{2681000734387898606373118228299776}$
 נחלק x_{108} ב-670250183596974651593279557074944, נקבל x_{109} כזה ש-
 $x_{109}^2 \equiv 17 \pmod{5362001468775797212746236456599552}$
 נחלק x_{109} ב-1340500367193949303186559114149888, נקבל x_{110} כזה ש-
 $x_{110}^2 \equiv 17 \pmod{10724002937551594425492472913199104}$
 נחלק x_{110} ב-2681000734387898606373118228299776, נקבל x_{111} כזה ש-
 $x_{111}^2 \equiv 17 \pmod{21448005875103188850984945826398208}$
 נחלק x_{111} ב-5362001468775797212746236456599552, נקבל x_{112} כזה ש-
 $x_{112}^2 \equiv 17 \pmod{42896011750206377701969891652796416}$
 נחלק x_{112} ב-10724002937551594425492472913199104, נקבל x_{113} כזה ש-
 $x_{113}^2 \equiv 17 \pmod{85792023500412755403939783305592832}$
 נחלק x_{113} ב-21448005875103188850984945826398208, נקבל x_{114} כזה ש-
 $x_{114}^2 \equiv 17 \pmod{171584047000825510807879566611185664}$
 נחלק x_{114} ב-42896011750206377701969891652796416, נקבל x_{115} כזה ש-
 $x_{115}^2 \equiv 17 \pmod{343168094001651021615759133222371328}$
 נחלק x_{115} ב-85792023500412755403939783305592832, נקבל x_{116} כזה ש-
 $x_{116}^2 \equiv 17 \pmod{686336188003302043231518266444742656}$
 נחלק x_{116} ב-171584047000825510807879566611185664, נקבל x_{117} כזה ש-
 $x_{117}^2 \equiv 17 \pmod{1372672376006604086463036532889485312}$
 נחלק x_{117} ב-343168094001651021615759133222371328, נקבל x_{118} כזה ש-
 $x_{118}^2 \equiv 17 \pmod{2745344752013208172926073065778970624}$
 נחלק x_{118} ב-686336188003302043231518266444742656, נקבל x_{119} כזה ש-
 $x_{119}^2 \equiv 17 \pmod{5490689504026416345852146131557941248}$
 נחלק x_{119} ב-1372672376006604086463036532889485312, נקבל x_{120} כזה ש-
 $x_{120}^2 \equiv 17 \pmod{10981379008052832691704292263115882496}$
 נחלק x_{120} ב-2745344752013208172926073065778970624, נקבל x_{121} כזה ש-
 $x_{121}^2 \equiv 17 \pmod{21962758016105665383408584526231764992}$
 נחלק x_{121} ב-5490689504026416345852146131557941248, נקבל x_{122} כזה ש-
 $x_{122}^2 \equiv 17 \pmod{43925516032211330766817169052463529984}$
 נחלק x_{122} ב-10981379008052832691704292263115882496, נקבל x_{123} כזה ש-