תרגול 14

המשך משפט ההדדיות הריבועי:

א) $\left(\frac{-1}{p}\right)$ $\quad p=4k+\ell$ $\quad \ell=1 \to 1$, $\ell=3 \to -1$

ב) $\left(\frac{2}{p}\right)$ $\quad p=8k+\ell$ $\quad \ell=3,5 \to -1$; $\ell=1,7 \to 1$

ג) אם $p=4k+1$ או $q=4\ell+1$ אז $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$

אחרת (כלומר $p=4k+3$, $q=4\ell+3$): $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$

⚠ זה התנאי ההכרחי היחיד, כלומר כל הכללה אחרת שגויה. "כל המספרים הטבעיים".

דוגמה:

$$\left(\frac{29}{43}\right) \overset{\downarrow}{=} \left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\left(\frac{7}{29}\right) \overset{\downarrow}{=} -1\cdot\left(\frac{29}{7}\right)=-\frac{1}{7}=-1$$

$29=4\cdot 7+1$ $\qquad$ $29=4\cdot 7+1$ $\qquad$ $29=8\cdot 3+5$

$$\left(\frac{79}{101}\right) \overset{\downarrow}{=} \left(\frac{101}{79}\right)=\left(\frac{22}{79}\right)=\left(\frac{2}{79}\right)\cdot\left(\frac{11}{79}\right) \overset{\uparrow}{=} +1\cdot-\left(\frac{79}{11}\right)=-\left(\frac{2}{11}\right)=1$$

$101=25\cdot 4+1$ $\qquad$ $79=8\cdot 10-1$

וכמובן $33^2\equiv 79 \pmod{101}$

$$5x^2+10x+13\equiv 0 \pmod{71}$$
$$25x^2+50x+65\equiv 0 \pmod{71}$$
$$(5x+5)^2+40\equiv 0 \pmod{71}$$
$$y:=5x+5$$
$$y^2\equiv -40 \pmod{71}$$

$$\left(\frac{-40}{71}\right)=\left(\frac{-10}{71}\right)\cdot\left(\frac{2}{71}\right)^2=\underbrace{\left(-\frac{1}{71}\right)}_{-1}\underbrace{\left(\frac{2}{71}\right)}_{1}\left(\frac{5}{71}\right)$$

$71=4\cdot 18-1$ $\qquad$ $71=8\cdot 9-1$

$$\left(\frac{5}{71}\right)=\left(\frac{71}{5}\right)=\frac{1}{5}=1 \quad\Rightarrow\quad \left(\frac{-40}{71}\right)=-1$$

אין פתרון!

$$p\equiv\pm 1 \pmod{12} \iff \left(\frac{3}{p}\right)=1$$

אמור $p\neq 2$ כלומי! (לכאורה סתם)

$$\left(\frac{3}{p}\right) \overset{\downarrow}{=} \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}=\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}=1$$ אלא

$$p\equiv 1 \pmod{12} \Leftarrow \begin{cases} p\equiv 1 \pmod 3 \\ p\equiv 1 \pmod 4 \end{cases} \Leftarrow \left(\frac{p}{3}\right)=1 \ \wedge\ (-1)^{\frac{p-1}{2}}=1$$

או

$$p\equiv -1 \pmod{12} \Leftarrow \begin{cases} p\equiv 2 \pmod 3 \\ p\equiv 3 \pmod 4 \end{cases} \Leftarrow \left(\frac{p}{3}\right)=-1 \ \wedge\ (-1)^{\frac{p-1}{2}}=-1$$ ▨

$$p\equiv\pm 1 \pmod 5 \iff \left(\frac{5}{p}\right)=1$$

$\left(\frac{5}{p}\right)=\left(\frac{p}{5}\right) \to$ שאריות ריבועיות: $\sqrt{1}, 2, 3, \sqrt{4}$

4. שאלה: איזה מספרים ראשוניים יכולים למנות מספרים מהצורה $x^2-10x+22$?

פתרון: $p \mid x^2-10x+22$ כלומר $x^2-10x+22 \equiv 0 \pmod p$

$(x-5)^2+3 \equiv 0 \pmod p$ ע"י $y=x-5$

$y^2 \equiv 3 \pmod p$

אז $p=2$ $y \neq 0$

או $p=3$ $y=0$

או $\left(\frac{3}{p}\right)=1$

$\Leftarrow$ השארה $p=2,3$ או $p \equiv 1,11 \pmod{12}$

שיעור:

$\gcd(a,b)=1$

הגדרה: יהי $a \in \mathbb{Z}$, b טבעי או שלילי, $b \in \mathbb{Z}_{\neq 0}$ יהי $b=p_1 \cdot p_2 \cdots p_m$ כאשר p_i ראשוניים (לאו דווקא שונים)

אזי $\left(\frac{a}{b}\right) := \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$ $\rightarrow$ כינוי ופקוד:

טענה: ① אם $a_1 \equiv a_2 \pmod b$ אזי $\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$

② $\left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)=\left(\frac{a_1 a_2}{b}\right)$

③ $\left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)=\left(\frac{a}{b_1 b_2}\right)$

משפט - חוק ההדדיות הריבועי טיען ופקוד: יהיו a,b אי זוגיים חיוביים וראשוניים זה לזה

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

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

ג) $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$

דוגמא:

* $\left(\frac{35}{73}\right)=\left(\frac{73}{35}\right)=\left(\frac{3}{35}\right)=-\left(\frac{35}{3}\right)=-\left(\frac{-1}{3}\right)=-(-1)=1$

* $\left(\frac{37603}{48011}\right)=-\left(\frac{48011}{37603}\right)=-\left(\frac{11008}{37603}\right)=-\left(\frac{2^8\cdot 43}{37603}\right)=-\left(\frac{43}{37603}\right)=\left(\frac{37603}{43}\right)=$

$=\left(\frac{21}{43}\right)=\left(\frac{43}{21}\right)=\left(\frac{1}{21}\right)=1$

סכימת הראשונים ומשפט דירכלה:

משפט דירכלה:

אין ידוע שום אינסוף ראשוניים, ובפרט מהצורה 2, $4k+3$, $4k+1$

$8k+1$ $8k+3$, $8k+5$, $8k+7$ $\leftarrow$ יש אינסוף? אי סופה

סדרה חשבונית $a_k=a+km$. $d=\gcd(a,m)$.

משפט: אם $d=1$ אז יש סדרה אינסופית ראשוניים.

תרגול מס' 14

(1) כמה מספרים ראשוניים יש הקטנים מ- $x>0$ כאשר $x\in\mathbb{R}$?

$\pi(x)=\#\{p: p\le x\}$

$\pi(x)=\#\{p: p\text{ ראשוני}, p<x\}$

$a+km$: סדרה חשבונית

$\frac{1}{\varphi(m)}\cdot\pi(x)$

כמה ראשוניים יש?

משפט המספרים הראשוניים:

$\pi(x)\sim x/\log x$:אז מתקיים

↓ הוכחה ע"י Legendre, Gauss ב- 1800.

הוכחה ב- 1896 ע"י Hadamard ו-de la Vallée-Poussin.

x	10	25	50	100	... 5000
$\pi(x)$	4	9	15	25	669
$\frac{\pi(x)}{x}$	0.4	0.36	0.3	0.25	0.139

$\frac{\pi(x)}{x}\xrightarrow{x\to\infty}0$

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1$$