תרגילים 1: תורת המספרים

שאלה 1 מצאו את הפירוק מנה-שארית של השלמים הבאים:

א) $a = 7503, b = 81$.

ב) $a = -7503, b = 81$.

ג) $a = 81, b = 7503$.

ד) $a = -81, b = 7503$.

שאלה 2 יהיו $a, b, n > 0$ שלמים. הוכיחו כי $a \bmod n = b \bmod n$ אם ורק אם $a \equiv b \pmod{n}$.

שאלה 3 מצאו שלמים s, t, d עבורם $12327s + 2409t = d$.

שאלה 4 הוכיחו כי 7563 ו- 526 מספרים זרים.

שאלה 5 יהיו a, b מספרים שלמים.
הוכיחו שאם קיימים שלמים s, t כך ש- $sa + tb = 1$ אז a ו- b זרים.

שאלה 6 יהיו a, b, n מספרים שלמים. הוכיחו את הטענה הבאה:
אם השלושה תנאים הבאים מתקיימים:

1) a ו- b זרים,
2) $a \mid n$,
3) $b \mid n$,

אז $ab \mid n$.

שאלה 7 הוכיחו את הטענות הבאות:

א) $\gcd(ma, mb) = m \gcd(a, b)$.

ב) אם $m > 0$ ואם $m \mid a$ ו- $m \mid b$ אז $\gcd\left(\frac{a}{m}, \frac{b}{m}\right) = \frac{\gcd(a,b)}{m}$.

ג) המספרים $\frac{a}{\gcd(a,b)}$ ו- $\frac{b}{\gcd(a,b)}$ מספרים זרים.

ד) אם $c \mid ab$ ו- c זר ביחס ל- b אז $c|a$.

ה) אם a, c מספרים זרים ואם b, c מספרים זרים אז c ו- ab מספרים זרים.

ו) $\gcd(a,b) = \gcd(a+cb, b)$.

שאלה 8 יהיו a, m מספרים זרים. הוכיחו כי $ab \equiv ac \pmod{m}$ אם ורק אם $b \equiv c \pmod{m}$.

שאלה 9 יהיו a, m מספרים שלמים (לא בהכרח זרים).
הוכיחו כי $ab \equiv ac \pmod{m}$ אם ורק אם $b \equiv c \bmod \left(\frac{m}{\gcd(a,m)}\right)$.

שאלה 10

א) חשבו את $\gcd(285, 89)$.

ב) מצאו שלמים s, t, d עבורם $285s + 89t = d$.

שאלה 11 הוכיחו: אם $a \mid bc$ וגם a, b זרים אז $a \mid c$.

שאלה 12

א) הוכיחו: אם a, b זרים אז קיים c עבורו $ac \equiv 1 \pmod{b}$.

ב) הוכיחו: אם a, b לא זרים אז לא קיים c עבורו $ac \equiv 1 \pmod{b}$.

שאלה 13

א) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a + c \equiv b + c \pmod{m}$.

ב) הוכיחו: אם $a \equiv b \pmod{m}$ וכן $c \equiv d \pmod{m}$ אז $ac \equiv bd \pmod{m}$.

ג) הוכיחו: אם $a \equiv b \pmod{m}$ אז $a^n \equiv b^n \pmod{m}$.

שאלה 14 יהי $m \geq 2$ שלם. הוכיחו או הפריכו על ידי דוגמה נגדית את הטענות הבאות:

א) m מספר ריבועי אם ורק אם כל אחד מהגורמים הראשוניים שלו מופיע עם חזקה זוגית בפירוק לראשוניים שלו.

ב) אם $\sqrt{m}$ מספר רצונלי אזי m מספר ריבועי.

ג) אם m הוא לא מספר ריבועי אזי $\sqrt{m}$ לא רציונלי.

שאלה 15 הוכיחו או הפריכו:

א) $54 \equiv 3 \pmod{17}$.

ב) $56 \equiv 3 \pmod 2$.

ג) $578 \equiv 9 \pmod 1$.

ד) $-23 \equiv 4 \pmod 9$.

ה) $1001 \equiv 1 \pmod 7$.

ו) $2025 \equiv 5 \pmod{10}$.

ז) $85 \equiv -3 \pmod{11}$.

ח) $2^8 \equiv 1 \pmod 5$.

ט) $45 \equiv 5 \pmod 8$.

י) $72 \equiv -1 \pmod 9$.

שאלה 16

חשבו:

א) $12^5 + 2^5 \bmod 11$.

ב) $7^4 + 3^5 \bmod 5$.

ג) $9^6 - 4^7 \bmod 7$.

ד) $5^{2025} \bmod 13$.

ה) $2^{100} + 2^{50} \bmod 3$.

ו) $10^{2025} \bmod 9$.

ז) $14^{12} \bmod 13$.

ח) $8^{17} - 3^{17} \bmod 5$.

ט) $6^{20} + 1 \bmod 7$.

י) $11^{30} \bmod 12$.

שאלה 17

א) אם $x \equiv 3 \pmod 7$ ו־$y \equiv 5 \pmod 7$, חשבו $4x - 3y \pmod 7$.

ב) אם $x \equiv 2 \pmod 9$ ו־$y \equiv 7 \pmod 9$, חשבו $xy^2 \pmod 9$.

ג) אם $a \equiv 11 \pmod{15}$ ו־$b \equiv -4 \pmod{15}$, חשבו $(2a + 5b) \pmod{15}$.

ד) אם $p \equiv 4 \pmod 6$ ו־$q \equiv -1 \pmod 6$, חשבו $p^2q \pmod 6$.

ה) אם $r \equiv 17 \pmod{20}$ ו־$s \equiv 13 \pmod{20}$, חשבו $(r-s)(r+s) \pmod{20}$.

שאלה 18

א) הוכיחו: אם $a \equiv c \pmod n$ וכן $b \equiv d \pmod n$ אז לכל $u, v \in \mathbb{Z}$ מתקיים:

$$ua + vb \equiv uc + vd \pmod n \ .$$

ב) הוכיחו באינדוקציה: אם $a \equiv c \pmod n$ אז לכל $k \in \mathbb{N}$ מתקיים:

$$a^k \equiv c^k \pmod n.$$

ג) הוכיחו: אם $a \equiv c \pmod n$ אז לכל פולינום $P(x)$ עם מקדמים שלמים מתקיים:

$$P(a) \equiv P(c) \pmod n.$$

ד) תנו דוגמה לכך שמ־$ac \equiv bc \pmod n$ לא נובע $a \equiv b \pmod n$.

ה) הוכיחו: אם $\gcd(c, n) = 1$ לכל n וכן $ac \equiv bc \pmod n$ אז $a \equiv b \pmod n$.

ו) תנו דוגמה עם $\gcd(c, n) \neq 1$ שבה $ac \equiv bc \pmod n$ אך $a \not\equiv b \pmod n$.

שאלה 19

אם $x \equiv 5 \pmod{12}$ ו־$y \equiv 8 \pmod{12}$, חשבו:

א) $x + y \bmod 12$

ב) $x - y \bmod 12$

ג) $xy \bmod 12$

ד) $x^3 + 2y \bmod 12$.

פתרונות

שאלה 1

מצב	סימן a	סימן b	מנה q	שארית r
1	$+$	$+$	$\left\lfloor \frac{a}{b} \right\rfloor$	$a \bmod b$
2	$+$	$-$	$-\left\lfloor \frac{a}{\lvert b\rvert} \right\rfloor$	$a \bmod \lvert b\rvert$
3	$-$	$+$	$-\left\lfloor \frac{\lvert a\rvert}{b} \right\rfloor - 1$	$b - \lvert a\rvert \bmod b$
4	$-$	$-$	$\left\lfloor \frac{\lvert a\rvert}{\lvert b\rvert} \right\rfloor + 1$	$\lvert b\rvert - \lvert a\rvert \bmod \lvert b\rvert$

א) נחשב שלמים q, r עבורם $a = qb + r$. השלם $a > 0$ ו- $b > 0$ לכן:

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{7503}{81} \right\rfloor = 92$$

$$r = a \bmod b = a - b\left\lfloor \frac{a}{b} \right\rfloor = 7503 - (81)(92) = 75$$

לכן

$$7503 = (92)(81) + 51 \ .$$

ב) השלם $a < 0$ ו- $b > 0$ לכן:

$$q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1 = -\left\lfloor \frac{7503}{81} \right\rfloor - 1 = -93$$

$$r = b - |a| \bmod b = b - \left(|a| - b\left\lfloor \frac{|a|}{b} \right\rfloor\right) = 81 - (7503 - (81)(92)) = 30 \ .$$

לכן

$$-7503 = (-93)(81) + 30 \ .$$

ג) השלם $a > 0$ ו- $b > 0$ לכן:

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{81}{7503} \right\rfloor = 0 \ .$$

$$r = a \bmod b = \left(a - b\left\lfloor \frac{a}{b} \right\rfloor\right) = 81 - (7503)\left\lfloor \frac{81}{7503} \right\rfloor = 81 \ .$$

לכן

$$81 = (0)(7503) + 81 \ .$$

ד) השלם $a < 0$ ו- $b > 0$ לכן:

$$q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1 = -\left\lfloor \frac{81}{7503} \right\rfloor - 1 = -1$$

$$r = b - |a| \bmod b = b - \left(|a| - b \left\lfloor \frac{|a|}{b} \right\rfloor \right) = 7503 - (81 - (7503)(0)) = 7422 \ .$$

לכן

$$-81 = (-1)(7503) + 7422 \ .$$

<u>שאלה 2</u> נראה את שני הכיוונים:

<u>$\Rightarrow$ כיוון</u>

נניח כי

$$a \bmod n = b \bmod n = r \ .$$

לפי משפט החלוקה של אוקלידס קיימים שלמים q_1, q_2 כך ש:

$$a = q_1 n + r, \qquad b = q_2 n + r.$$

לכן:

$$a - b = (q_1 - q_2)n.$$

כלומר $n \mid (a-b)$, ולכן $a \equiv b \pmod{n}$.

<u>$\Leftarrow$ כיוון</u>

נניח כי

$$a \equiv b \pmod{n},$$

כלומר קיים שלם k כך ש:

$$a = b + kn.$$

הפירוק מנה-שארית של b ו- n הוא:

$$b = qn + r, \qquad 0 \le r < n.$$

כאשר $r = b \bmod n$. אז:

$$a = b + kn = (q+k)n + r.$$

זהו פירוק מנה-שארית של a ו- n, על פי משפט החלוקה של אוקלידס, כאשר המנה השלמה היא $Q = \left\lfloor \frac{a}{n} \right\rfloor = q+k$ והשארית

$$a \bmod n = a - \left\lfloor \frac{a}{n} \right\rfloor n = (q+k)n + r - (q+k)n = r$$

לכן $a \bmod n = r = b \bmod n$.

שאלה 3

קיימים שלמים s, t, d עבורם $12327s + 2409t = d$ כאשר $d = \gcd(12327, 2409)$.
נשתמש באלגוריתם המוכלל של אוקלידס. נסמן $a = 12327, b = 2409$.

$$r_0 = a = 12327 \ , \quad r_1 = b = 2409 \ , \quad s_0 = 1 \ , \quad s_1 = 0 \ , \quad t_0 = 0 \ , \quad t_1 = 1 \ .$$

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{12327}{2409} \right\rfloor = 5$	$r_2 = r_0 - q_1 r_1 = 12327 - (5)(2409) = 282$	$s_2 = s_0 - q_1 s_1 = 1 - (5)(0) = 1$	$t_2 = t_0 - q_1 t_1 = 1 - (5)(1) = -5$
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{2409}{282} \right\rfloor = 8$	$r_3 = r_1 - q_2 r_2 = 2409 - (8)(282) = 153$	$s_3 = s_1 - q_2 s_2 = 0 - (8)(1) = -8$	$t_3 = t_1 - q_2 t_2 = 1 - (8)(-5) = 41$
$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{282}{153} \right\rfloor = 1$	$r_4 = r_2 - q_3 r_3 = 282 - (1)(153) = 129$	$s_4 = s_2 - q_3 s_3 = 1 - (1)(-8) = 9$	$t_4 = t_2 - q_3 t_3 = -5 - (1)(41) = -46$
$q_4 = \left\lfloor \frac{r_3}{r_4} \right\rfloor = \left\lfloor \frac{153}{129} \right\rfloor = 1$	$r_5 = r_3 - q_4 r_4 = 153 - (1)(129) = 24$	$s_5 = s_3 - q_4 s_4 = -8 - (1)(9) = -17$	$t_5 = t_3 - q_4 t_4 = 41 - (1)(-46) = 87$
$q_5 = \left\lfloor \frac{r_4}{r_5} \right\rfloor = \left\lfloor \frac{129}{24} \right\rfloor = 5$	$r_6 = r_4 - q_5 r_5 = 129 - (5)(24) = 9$	$s_6 = s_4 - q_5 s_5 = 9 - (5)(-17) = 94$	$t_6 = t_4 - q_5 t_5 = -46 - (5)(87) = -481$
$q_6 = \left\lfloor \frac{r_5}{r_6} \right\rfloor = \left\lfloor \frac{24}{9} \right\rfloor = 2$	$r_7 = r_5 - q_6 r_6 = 24 - (2)(9) = 6$	$s_7 = s_5 - q_6 s_6 = -17 - (2)(94) = -205$	$t_7 = t_5 - q_6 t_6 = 87 - (2)(-481) = 1049$
$q_7 = \left\lfloor \frac{r_6}{r_7} \right\rfloor = \left\lfloor \frac{9}{6} \right\rfloor = 1$	$r_8 = r_6 - q_7 r_7 = 9 - (1)(6) = 3$	$s_8 = s_6 - q_7 s_7 = 94 - (1)(-205) = 299$	$t_8 = t_6 - q_7 t_7 = -481 - (1)(1049) = -1530$
$q_8 = \left\lfloor \frac{r_7}{r_8} \right\rfloor = \left\lfloor \frac{6}{3} \right\rfloor = 2$	$r_9 = r_7 - q_8 r_8 = 6 - (2)(3) = 0$		

לכן

$$d = r_8 = 3 \ , \qquad s = s_8 = 299 \ , \qquad t = t_8 = -1530 \ .$$

והפירוק אוקלידס הוא

$$12327s + 2409t = 12327(299) + 2409(-1530) = 3 \ ,$$

ו- $\gcd(12327, 2409) = 3$.

שאלה 4

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{7563}{526} \right\rfloor = 14$	$r_2 = r_0 - q_1 r_1 = 7563 - (14)(526) = 199$	$s_2 = s_0 - q_1 s_1 = 1 - (14)(0) = 1$	$t_2 = t_0 - q_1 t_1 = 0 - (14)(1) = -14$
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{526}{199} \right\rfloor = 2$	$r_3 = r_1 - q_2 r_2 = 526 - (2)(199) = 128$	$s_3 = s_1 - q_2 s_2 = 0 - (2)(1) = -2$	$t_3 = t_1 - q_2 t_2 = 1 - (2)(-14) = 29$
$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{199}{128} \right\rfloor = 1$	$r_4 = r_2 - q_3 r_3 = 199 - (1)(128) = 71$	$s_4 = s_2 - q_3 s_3 = 1 - (1)(-2) = 3$	$t_4 = t_2 - q_3 t_3 = -14 - (1)(29) = -43$
$q_4 = \left\lfloor \frac{r_3}{r_4} \right\rfloor = \left\lfloor \frac{128}{71} \right\rfloor = 1$	$r_5 = r_3 - q_4 r_4 = 128 - (1)(71) = 57$	$s_5 = s_3 - q_4 s_4 = -2 - (1)(3) = -5$	$t_5 = t_3 - q_4 t_4 = 29 - (1)(-43) = 72$
$q_5 = \left\lfloor \frac{r_4}{r_5} \right\rfloor = \left\lfloor \frac{71}{57} \right\rfloor = 1$	$r_6 = r_4 - q_5 r_5 = 71 - (1)(57) = 14$	$s_6 = s_4 - q_5 s_5 = 3 - (1)(-5) = 8$	$t_6 = t_4 - q_5 t_5 = -43 - (1)(72) = -115$
$q_6 = \left\lfloor \frac{r_5}{r_6} \right\rfloor = \left\lfloor \frac{57}{14} \right\rfloor = 4$	$r_7 = r_5 - q_6 r_6 = 57 - (4)(14) = 1$	$s_7 = s_5 - q_6 s_6 = -5 - (4)(8) = -37$	$t_7 = t_5 - q_6 t_6 = 72 - (4)(-115) = 532$
$q_7 = \left\lfloor \frac{r_6}{r_7} \right\rfloor = \left\lfloor \frac{14}{1} \right\rfloor = 14$	$r_8 = r_6 - q_7 r_7 = 14 - (14)(1) = 0$		

מכאן $\gcd(526, 7563) = 1$.

שאלה 5 ראשית נזכיר שאנחנו אומרים כי a ו- b זרים אם $\gcd(a,b)=1$.
נניח כי $\gcd(a,b)=d$. נוכיח כי $d=1$.

נניח כי $sa+tb=1$.
השלם d הוא המחלק המשותף הגדול ביותר של a ו- b.
אז בהכרח $d \mid a$ ו- $d \mid b$ לכן $d \mid (sa+tb)$ אז $d \mid 1$.

לכן $d=1$ ולכן a ו- b זרים.

שאלה 6 נתון לנו כי $a \mid n$ ו- $b \mid n$ לכן קיימים שלמים k ו- l כך ש-

$$n=ak \ , \qquad n=bl \ .$$

ז"א $n=ak=bl$.
מכאן $b \mid ak$.
נתון כי $\gcd(a,b)=1$, לכן $b \mid k$. לכן $k=bq$.
לכן $n=ak=abq$.

שאלה 7

א) יהי $d=\gcd(a,b)$. אז קיימים שלמים s,t עבורם

$$sa+tb=d \ .$$

מכאן

$$msa+mtb=md \quad \Rightarrow \quad s(ma)+t(mb)=md \ .$$

אנחנו קיבלנו כי הפירוק אוקלידס של ma ו- mb הוא $s(ma)+t(mb)=md$ ובפרט השלם באגף הימין הוא ה- gcd של ma ו- mb. לפיכך

$$\gcd(ma,mb)=md=m\gcd(a,b) \ .$$

ב) יהי $d=\gcd(a,b)$.
$\exists$ שלמים s,t כך ש-

$$sa+tb=d \ . \qquad (*)$$

נחלק (*) ב- m ונקבל

$$s\left(\frac{a}{m}\right)+t\left(\frac{b}{m}\right)=\frac{d}{m} \ . \qquad (**)$$

נשים לב $m \mid a$ ו- $m \mid b$. לכן $\frac{a}{m}$ שלם ו- $\frac{b}{m}$ שלם.
ז"א המספר בצד שמאל הוא שלם.
לכן המספר בצד ימין, $\frac{d}{m}$, הוא בהכרח שלם.
לכן ולפי משפט בזו $\frac{d}{m}=\gcd\left(\frac{a}{m},\frac{b}{m}\right)$.
לכן

$$\gcd\left(\frac{a}{m},\frac{b}{m}\right)=\frac{\gcd(a,b)}{m} \ .$$

ג) יהי $d = \gcd(a,b)$.
לפי משפט בזו קיימים שלמים s,t עבורם

$$sa + tb = d \ .$$

נחלק ב- d ונקבל

$$s\left(\frac{a}{d}\right) + t\left(\frac{b}{d}\right) = 1 \ .$$

לפי משפט בזו, השלם בצד ימין הוא ה- gcd של $\frac{a}{d}$ ו- $\frac{b}{d}$. לכן

$$\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 \quad \Rightarrow \quad \gcd\left(\frac{a}{\gcd(a,b)}, \frac{b}{\gcd(a,b)}\right) = 1$$

לכן $\frac{a}{\gcd(a,b)}$ ו- $\frac{b}{\gcd(a,b)}$ זרים.

ד)

ה) a ו- c זרים אז קיימים s ו- t שלמים עבורם

$$sa + tc = 1 \ .$$

b ו- c זרים אז קיימים $\bar{s}$ ו- $\bar{t}$ שלמים עבורם

$$\bar{s}b + \bar{t}c = 1 \ .$$

לכן

$$\begin{aligned} (sa + tc)\left(\bar{s}b + \bar{t}c\right) =& 1 \\ \Rightarrow \quad s\bar{s}(ab) + \left(t\bar{s}b + t\bar{t}c + s\bar{t}a\right)c =& 1 \end{aligned}$$

ז"א קיימים שלמים x,y עבורם $x(ab) + yc = 1$ לכן ab ו- c זרים.

ו) אם a,b שלמים אז קיימים שלמים s ו- t עבורם $sa + tb = d$ כאשר $d = \gcd(a,b)$. מכאן

$$\begin{aligned} sa + tb =& d \\ s\left(a + cb\right) + tb =& d + scb \\ s\left(a + cb\right) + tb - scb =& d \\ s\left(a + cb\right) + \left(t - sc\right)b =& d \end{aligned}$$

לכן קיימים שלמים $x = s$ ו- $y = t - cb$ עבורם

$$x(a + cb) + yb = d$$

ולכן $\gcd(a + cb, b) = d = \gcd(a,b)$.

שאלה 8

כיוון $\Leftarrow$

נניח כי $ab \equiv ac \pmod m$. אזי קיים שלם q עבורו:

$$ab \equiv ac \pmod m \quad \Rightarrow \quad ab = ac + qm \quad \Rightarrow \quad ab - ac = qm \quad \Rightarrow \quad a(b-c) = qm \ .$$

מכאן $a \mid qm$.
a, m זרים לכן $a \nmid m$ לכן בהכרח $a \mid q$.
ז"א קיים שלם k שלם עבורו $q = ak$.
לפיכך

$$a(b-c) = qm \quad \Rightarrow \quad a(b-c) = akm \quad \Rightarrow \quad b-c = km \quad \Rightarrow \quad b = c+km \quad \Rightarrow \quad b \equiv c \pmod m \ .$$

כיוון $\Rightarrow$

נניח כי $b \equiv c \pmod m$. אז קיים שלם q כך ש:

$$b = qm + c \quad \Rightarrow \quad ab = aqm + ac \quad \Rightarrow \quad ab \equiv ac \pmod m \ .$$

שאלה 9

כיוון $\Leftarrow$

נניח כי $ab \equiv ac \mod m$. אז קיים שלם q כך ש:

$$ab = ac + qm \quad \Rightarrow \quad ab - ac = qm \quad \Rightarrow \quad m \mid a(b-c) \quad \Rightarrow \quad \frac{m}{\gcd(a,m)} \Big| \frac{a}{\gcd(a,m)}(b-c) \ .$$

הביטוי אחרון אומר " $\frac{m}{\gcd(a,m)}$ מחלק את $\frac{m}{\gcd(a,m)}(b-c)$".
מכיוון ש- $\frac{m}{\gcd(a,m)}$ ו- $\frac{a}{\gcd(a,m)}$ זרים, אז בהכרח

$$\frac{m}{\gcd(a,m)} \mid (b-c) \ .$$

לכן

$$b \equiv c \mod \left(\frac{m}{\gcd(a,m)}\right) \ .$$

כיוון $\Rightarrow$

שאלה 10

$a = 285, b = 89$.

$$\begin{aligned} r_0 &= a = 285 \ , & r_1 &= b = 89 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $k=1$:	$t_2 = 0 - 3 \cdot 1 = -3$	$s_2 = 1 - 3 \cdot 0 = 1$	$r_2 = 285 - 3 \cdot 89 = 18$	$q_1 = 3$
שלב $k=2$:	$t_3 = 1 - 4 \cdot (-3) = 13$	$s_3 = 0 - 4 \cdot 1 = -4$	$r_3 = 89 - 4 \cdot 18 = 17$	$q_2 = 4$
שלב $k=3$:	$t_4 = -3 - 1 \cdot (13) = -16$	$s_4 = 1 - 1 \cdot (-4) = 5$	$r_4 = 18 - 1 \cdot 17 = 1$	$q_3 = 1$
שלב $k=4$:	$t_5 = 13 - 17 \cdot (-16) = 285$	$s_5 = -4 - 17 \cdot 5 = -89$	$r_5 = 17 - 17 \cdot 1 = 0$	$q_4 = 17$

$$\gcd(a,b) = r_4 = 1 \ , \qquad s = s_4 = 5 \ , \qquad t = t_4 = -16 \ .$$

$$ta + sb = 5(289) - 16(85) = 1 \ .$$

■

<u>שאלה 11</u> $a \mid bc$ לכן קיים שלם q עבורו

$$bc = qa \tag{\#1}$$

$\gcd(a,b) = 1$ לכן לפי משפט בזו קיימים שלמים x, y עבורם $xa + yb = 1$.

מכאן

$$b = \frac{1 - xa}{y} \ . \tag{\#2}$$

על די הצבה של (#2) ב- (#1) נקבל

$$\begin{aligned}
\left(\frac{1-xa}{y}\right) c =& qa \\
(1-xa)c =& qay \\
c - xac =& qay \\
c =& qay + xac \\
c =& a\left(xc + qy\right) \ .
\end{aligned}$$

לכן $a \mid c$.

<u>שאלה 12</u>

א) לפי משפט בזו, מכיוון ש- a, b זרים אז קיימים שלמים s, t עבורם

$$sa + tb = 1 \ .$$

נעביר אגפים:

$$sa = -tb + 1$$

מכאן $sa \equiv 1 \pmod{b}$.

ב) נוכיח את הטענה דרך השלילה. נניח כי a, b לא זרים וקיים שלם c עבורו $ac \equiv 1 \pmod{b}$.

$\Leftarrow$ קיים שלם q עבורו $ac = qb + 1$.

מכאן

$$ac - qb = 1 \quad \Rightarrow \quad ac + (-q)b = 1$$

עכשיו a, b אינם זרים אז קיים מחלק משותף $d > 1$ כך ש- $d \mid a$ ו- $d \mid b$.

לכן $d \mid (ac + (-q)b)$ לכן $d \mid 1$.

סתירה!

שאלה 13

א) $a \equiv b \pmod{m}$ אז $\exists\, q$ שלם עבורו $a = qm + b$.

נוסיף c לשני האגפים:

$$a + c = qm + b + c \quad \Rightarrow \quad a + c \equiv b + c \pmod{m} \ .$$

ב) $a \equiv b \pmod{m}$ אז $\exists\, q$ שלם עבורו $a = qm + b$.

$c \equiv d \pmod{m}$ אז $\exists\, q'$ שלם עבורו $c = q'm + d$.

לכן

$$ac = (mq + b)(q'm + d) = (qq'm + bq' + dq)\, m + bd \ .$$

לכן קיים שלם $Q = qq'm + bq' + dq$ כך ש-

$$ac = Qm + bd$$

לפיכך $ac \equiv bd \pmod{m}$.

ג) אינדוקציה על n.

שאלה 14

א) נניח כי m מספר ריבועי. אזי קיים שלם n עבורו $m = n^2$. נניח כי הפירוק לראשוניים של n הוא

$$n = p_1^{e_1} \dots p_k^{e_k} \ .$$

אזי

$$m = n^2 = (p_1^{e_1} \dots p_k^{e_k})^2 = p_1^{2e_1} \dots p_k^{2e_k} \ .$$

נניח כי בפירוק לראשוניים של m כל מספשר ראשוני מופיע עם חזקה זוגית. אזי

$$m = p_1^{f_1} \dots p_k^{f_k}$$

כאשר לכל חזקה f_i קיים שלם e_i כך ש: $f_i = 2e_i$. לכן

$$m = p_1^{2e_1} \dots p_k^{2e_k} = (p_1^{e_1} \dots p_k^{e_k})^2 = n^2$$

כאשר n הוא השלם $n = p_1^{e_1} \dots p_k^{e_k}$.

ב)

שאלה 15

א) אמת

ב) שקר

ג) אמת

ד) אמת

ה) שקר

ו) אמת

ז) אמת

ח) אמת

ט) אמת

י) שקר.

שאלה 16

א) 0

ב) 4

ג) 4

ד) 5

ה) 2

ו) 1

ז) 1

ח) 0

ט) 2

י) 1

שאלה 17

א) 4

ב) 8

ג) 1

ד) 22

ה) 14

שאלה 18

א) $a \equiv c \pmod{n}$ אז קיים q עבורו $a = qn + c$. נכפיל ב- u ונקבל

$$ua = uqn + uc \quad \Rightarrow \quad ua = Qn + uc$$

כאשר $Q = uq$. הוכחנו שקיים Q עבורו $ua = Qn + uc$ ולכן $ua \equiv uc \pmod{n}$.

בנוסף זה נתון לנו ש- $b \equiv d \pmod{n}$, לכן באותו אופן אפשר להוכיח ש- $vb \equiv vd \pmod{n}$. לכן לפי התכונת חיבוריות של יחס מודולרית אנחנו נקבל כי

$$ua + vb \equiv uc + vd \pmod{n} \ .$$

שאלה 19

א)

ב)

ג)

ד)