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 $12327s + 409t = d$.

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 $ab \equiv ac \mod m$ אם ורק אם $b \equiv c \mod m$.

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

שאלה 10

א) חשבו את $\gcd(285,89)$.

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

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

שאלה 12

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

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

שאלה 13

א) הוכיחו: אם $a \equiv b \mod m$ אז $a+c \equiv b+c \mod m$.

ב) הוכיחו: אם $a \equiv b \mod m$ ו- $c \equiv d \mod m$ אז $ac \equiv bd \mod m$.

ג) הוכיחו: אם $a \equiv b \mod m$ אז $a^n \equiv b^n \mod m$.

שאלה 14 חשבו את האיבר ההופכי של 7 ב- $\mathbb{Z}_{20}$.

שאלה 15

א) חשבו את $\gcd(285,89)$.

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

שאלה 16 הוכיחו: אם $a \mid bc$ ו- a,b זרים אז $a \mid c$.

שאלה 17

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

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

שאלה 18

א) הוכיחו: אם $a \equiv b \mod m$ אז $a + c \equiv b + c \mod m$.

ב) הוכיחו: אם $a \equiv b \mod m$ ו- $c \equiv d \mod m$ אז $ac \equiv bd \mod m$.

ג) הוכיחו: אם $a \equiv b \mod m$ אז $a^n \equiv b^n \mod m$.

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:

$\Rightarrow$ 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 $a \equiv b \pmod{n}$.

$\Leftarrow$ נניח כי

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

כלומר קיים שלם k כך ש:

$$a = b + kn.$$

נחלק את b ב־n:

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

אז:

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

זהו פירוק על פי משפט החלוקה של אוקלידס, ולכן השארית של a בחלוקה ב־n היא r. מכאן:

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

<u>שאלה 3</u>

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

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

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

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 $\gcd(526, 7563) = 1$.

<u>שאלה 5</u> יהי d ה- gcd של a ו- b. אם $sa + tb = 1$ אז בהכרח d מחלק 1. לכן $d = 1$ לכן $\gcd(a, b) = 1$.

<u>שאלה 6</u>

$$a \mid n \ , \quad b \mid n$$

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
$$msa + mtb = md \quad \Rightarrow \quad s(ma) + t(mb) = md \ .$$
לכן $\gcd(ma,mb) = md = m\gcd(a,b)$.

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

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

נחלק (*) ב- m ונקבל

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

נשים לב $m \mid a$ ו- $m \mid b$. לכן $\frac{a}{m}$ שלמ ו- $\frac{b}{m}$ שלם.
לכן $\frac{d}{m}$ בהכרח שלם 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 $d = \gcd(a,b)$.
$\exists$ שלמים s,t עבורם
$$sa + tb = d \ .$$

נחלק ב- d ונקבל
$$s\frac{a}{d} + t\frac{b}{d} = 1 \ .$$

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) a, b שלמים לכן קיימים שלמים s, t, d עבורם

$$sa + tb = d$$

כאשר $d = \gcd(a, b)$.

מכאן

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

נשים לב ש- $d = \gcd(a, b)$ לכן בהכרח $\frac{a}{d}$ ו- $\frac{b}{d}$ שלמים. לכן קיבלנו שלמים s, t עבורם

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

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

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

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 נניח כי $ab \equiv ac \mod m$.

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

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

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

נניח כי $b \equiv c \mod m$. אז

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

שאלה 9 נניח כי $ab \equiv ac \mod m$. אז

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

מכיוון ש- $\frac{m}{\gcd(a,m)}$ ו- $\frac{a}{\gcd(a,m)}$ זרים, אז

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

לכן

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

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

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

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

■

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

(#1) $$bc = qa$$

$\gcd(a,b) = 1$ לכן $\exists$ x, y שלמים עבורם $xa + yb = 1$.

מכאן

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

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

$$sa + tb = 1 \ .$$

נקח את $\bmod b$ של הצד שמאל והצד ימין ונקבל

$$(sa + tb) \mod b = 1 \mod b \quad \Rightarrow \quad sa \mod b = 1 \mod b \quad \Rightarrow \quad sa \equiv 1 \mod b \ .$$

ב) נוכיח את הטענה דרך השלילה. נניח $\exists$ c שלם עבורו $ac \equiv 1 \mod b$.

ז"א $\exists$ q שלם עבורו $ac = qb + 1$.

מכאן

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

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

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

סתירה!

<u>שאלה 13</u>

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

מכאו

$$a + c = qm + b + c \quad \Rightarrow \quad a + c \equiv b + c \mod m \ .$$

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

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

מכאו

$$ac = (mq + b)(q'm + d) = qq'm^2 + bq'm + dqm + bd = (qq'm + bq' + dq)\, m + bd \ .$$

לכן $\exists \bar{q} = qq'm + bq' + dq$ כך ש-

$$ac = \bar{q}m + bd$$

לפיכך $ac \equiv bd \mod m$.

ג) אינדוקציה על n.

שאלה 14

$$\begin{aligned} 1 \cdot 7 = 7 &\equiv 7 \mod 20 \ , \\ 2 \cdot 7 = 14 &\equiv 14 \mod 20 \ , \\ 3 \cdot 7 = 21 &\equiv 1 \mod 20 \ . \end{aligned}$$

לכן $7^{-1} \equiv 3 \mod 20$.

שאלה 15

$a = 285, b = 89$.

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

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

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

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

■

שאלה 16 $a \mid bc$ לכן $\exists$ שלם q עבורו

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

$\gcd(a,b) = 1$ לכן $\exists\ x, y$ שלמים 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 $a \mid c$.

שאלה 17

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

$$sa + tb = 1 \ .$$

נקח את $\bmod b$ של הצד שמאל והצד ימין ונקבל

$$(sa + tb) \mod b = 1 \mod b \quad \Rightarrow \quad sa \mod b = 1 \mod b \quad \Rightarrow \quad sa \equiv 1 \mod b \ .$$

ב) נוכיח את הטענה דרך השלילה. נניח $\exists\ c$ שלם עבורו $ac \equiv 1 \mod b$.

ז"א $\exists\ q$ שלם עבורו $ac = qb + 1$.

מכאן

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

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

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

סתירה!

שאלה 18

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

מכאו

$$a + c = qm + b + c \quad \Rightarrow \quad a + c \equiv b + c \mod m\ .$$

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

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

מכאו

$$ac = (mq + b)\,(q'm + d) = qq'm^2 + bq'm + dqm + bd = (qq'm + bq' + dq)\,m + bd\ .$$

לכן $\exists \bar{q} = qq'm + bq' + dq$ כך ש-

$$ac = \bar{q}m + bd$$

לפיכך $ac \equiv bd \mod m$.

ג) אינדוקציה על n.