

תרגילים 1: תורת המספרים

שאלה 1 מצאו את הפירוקמנה-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 n, a, b מספרים שלמים. הוכיחו את הטענה הבאה:

אם השלושה תנאים הבאים מתקיימים:

(1) a ו- b זרים,

, $a \mid n$ (2)

, $b \mid n$ (3)

. $ab \mid n$ (4)

שאלה 7 הוכיחו את הטענות הבאות:

(א) $\gcd(ma, mb) = m \gcd(a, b)$

(ב) אם $m > 0$ ו- a, b זרים, אז $\frac{\gcd(a, b)}{m} \mid \frac{ma}{m}$ ו- $m \mid ab$.

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

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

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

$$\gcd(a, b) = \gcd(a + cb, b) \quad (1)$$

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

שאלה 9 יהיו m, a, b מספרים שלמים (לא בהכרח זרים).

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

הוכיחו כי $ab \equiv ac \pmod{m}$ אם ורק אם $b \equiv c \pmod{\frac{m}{\gcd(a, m)}}$

שאלה 10

(א) חשבו את $\gcd(285, 89)$.

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

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

שאלה 12

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

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

שאלה 13

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

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

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

שאלה 14 יהיו $2 \leq m$ 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 לגורמים.

(ב) אם \sqrt{m} מספר רצונלי אז m מספר ריבועי.

(ג) אם m הוא לא מספר ריבועי אז \sqrt{m} לא רצונלי.

שאלה 15 הוכיחו או הפריכו:

(א) $.54 \equiv 3 \pmod{17}$

- . $56 \equiv 3 \pmod{2}$ (ב)
- . $578 \equiv 9 \pmod{1}$ (ג)
- . $-23 \equiv 4 \pmod{9}$ (ד)
- . $1001 \equiv 1 \pmod{7}$ (ה)
- . $2025 \equiv 5 \pmod{10}$ (ו)
- . $85 \equiv -3 \pmod{11}$ (ז)
- . $2^8 \equiv 1 \pmod{5}$ (ח)
- . $45 \equiv 5 \pmod{8}$ (ט)
- . $72 \equiv -1 \pmod{9}$ (י)

שאלה 16 חשבו:

- . $12^5 + 2^5 \pmod{11}$ (א)
- . $7^4 + 3^5 \pmod{5}$ (ב)
- . $9^6 - 4^7 \pmod{7}$ (ג)
- . $5^{2025} \pmod{13}$ (ד)
- . $2^{100} + 2^{50} \pmod{3}$ (ה)
- . $10^{2025} \pmod{9}$ (ו)
- . $14^{12} \pmod{13}$ (ז)
- . $8^{17} - 3^{17} \pmod{5}$ (ח)
- . $6^{20} + 1 \pmod{7}$ (ט)
- . $11^{30} \pmod{12}$ (י)

שאלה 17

- . $4x - 3y \pmod{7}$, $y \equiv 5 \pmod{7}$ ו- $x \equiv 3 \pmod{7}$ אם (א)
- . $xy^2 \pmod{9}$, $y \equiv 7 \pmod{9}$ ו- $x \equiv 2 \pmod{9}$ אם (ב)
- . $(2a + 5b) \pmod{15}$, $b \equiv -4 \pmod{15}$ ו- $a \equiv 11 \pmod{15}$ אם (ג)

- (ד) אם $p^2q \pmod{6}$ ו- $q \equiv -1 \pmod{6}$, חשבו $p \equiv 4 \pmod{6}$
 . $(r-s)(r+s) \pmod{20}$ ו- $s \equiv 13 \pmod{20}$, חשבו $r \equiv 17 \pmod{20}$

 שאלה 18

(א) הוכיחו: אם $u, v \in \mathbb{Z}$ ו- $b \equiv d \pmod{n}$ אז לכל $a \equiv c \pmod{n}$ מתקאים:
 $ua + vb \equiv uc + vd \pmod{n}$.

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

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

- (ד) תנו דוגמה לכך ש- $ac \equiv bc \pmod{n}$ לא נובע $a \equiv b \pmod{n}$.
 (ה) הוכיחו: אם $\gcd(c, n) = 1$ אז $ac \equiv bc \pmod{n}$ ו- $\gcd(c, n) \neq 1$ � $ac \equiv bc \pmod{n}$ שבה $\gcd(c, n) \neq 1$

 שאלה 19

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

$$x + y \pmod{12} \quad (\text{א})$$

$$x - y \pmod{12} \quad (\text{ב})$$

$$xy \pmod{12} \quad (\text{ג})$$

$$x^3 + 2y \pmod{12} \quad (\text{ד})$$

פתרונות **שאלה 1**

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

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

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

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

לכן

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

ב) השלים $b > 0$ ו- $a < 0$ לכך: $b > 0$ ו- $a < 0$.

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

$$r = b - |a| \bmod b = b - \left(|a| - b \left\lfloor \frac{|a|}{b} \right\rfloor \right) = 81 - (7503 - (81)(-93)) = 30 .$$

לכן

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

ג) השלים $b > 0$ ו- $a > 0$ לכך: $b > 0$ ו- $a > 0$.

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

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

לכן

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

(ז) השלים $0 < a < b$ לכך:

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

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

לכן

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

שאלה 2 נראה את שני הכוונים:

כיוון ⇒

נניח כי

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

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

$$a = q_1n + r, \quad b = q_2n + r.$$

לכן:

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

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

כיוון ⇌

נניח כי

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

כלומר קיימים שלם k כך ש:

$$a = b + kn.$$

הפרקמן-שארית של b ו- n הוא:

$$b = qn + r, \quad 0 \leq r < n.$$

כאשר $n \mid r$. א. $r = b \bmod n$.

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

זהו פירוק מנת-שארית של a ו- n , על פי משפט החלוקה של אוקלידס, כאשר המנה השלמה היא $q+k$ 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 המוכל של אוקליידס. נסמן $a = 12327, b = 2409$.

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

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

לכז

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

והפירוק אוקלידס הוא

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

$$\gcd(12327, 2409) = 3 \text{ -}$$

 שאלה 4

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

$$\gcd(526, 7563) = 1 \text{ מכאן}$$

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

נניח כי $sa + tb = 1$. השלים d הוא המחלק המשותף הגדול ביותר של a ו- b . $d | 1$ אז $d | (sa + tb)$ ולכן $d | a$ ו- $d | b$.

לכן $1 = d$ ולכן a ו- b זרים.

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

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

נניח כי $n = ak = bl$. מכאן $b | ak$ ולכן $b | k$. $k = bq$, כלומר $\gcd(a, b) = 1$. לכן $n = abq$.

שאלה 7

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

$$sa + tb = d.$$

מכאן

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

אנחנו קיבלו כי הפירוק אוקליידס של $msa + t(mb) = md$ הוא ma ו- mb ובפרט השלים באגף הימין הוא ה- \gcd של ma ו- mb . לפיכך

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

(ב) ידי $d = \gcd(a, b)$ קיימים שלמים s, t כך ש-

$$sa + tb = d.$$

נחלק (*) ב- m ונקבל

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

נשים לב $a | b$ ו- $m | b$. מכאן $\frac{a}{m}$ שלם ו- $\frac{b}{m}$ שלם. י"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) $d = \gcd(a, b)$
לפי משפט בז'ו 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 בז'ו, השלם בצד ימין הוא ה- \gcd של $\frac{a}{d}$ ו- $\frac{b}{d}$. לכן

$$\begin{aligned} \gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1 &\Rightarrow \gcd\left(\frac{a}{\gcd(a, b)}, \frac{b}{\gcd(a, b)}\right) = 1 \\ &\text{לכן } \frac{b}{\gcd(a, b)} \text{ ו- } \frac{a}{\gcd(a, b)} \text{ זרים.} \end{aligned}$$

(ד)

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

$$sa + tc = 1 .$$

ו- c זרים או קיימים \bar{s} ו- \bar{t} שלמים עבורם

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

לכן

$$\begin{aligned} (sa + tc)(\bar{s}b + \bar{t}c) &= 1 \\ \Rightarrow s\bar{s}(ab) + (t\bar{s}b + t\bar{t}c + s\bar{t}a)c &= 1 \\ \text{וז"א קיימים שלמים } x, y \text{ עבורם } x(ab) + yc = 1 \text{ וכן } ab \text{ זרים.} \end{aligned}$$

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

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

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

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

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

שאלה 8כיוון \Leftarrow נניח כי $ab \equiv ac \pmod{m}$. אז קיים שלם q עבורו:

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

מכאן $qm | a$.
 m זרים לכך $a | qm$ לכן $a | q$ בהכרח.
 ו"א קיים שלם k שלם עבורו $q = ak$
 לפיכך

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

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

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

שאלה 9כיוון \Leftarrow נניח כי m קיים שלם q כך ש: $ab \equiv ac \pmod{m}$.

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

הביטוי אחרון אומר " $\frac{m}{\gcd(a, m)}$ מחלק את $\frac{a}{\gcd(a, m)}(b - c)$ "

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

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

לכן

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

כיוון \Rightarrow **שאלה 10**

$$a = 285, b = 89$$

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

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

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

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

■

 שאלה 11

$$bc = qa \quad (\#1)$$

$$xa + yb = 1 \quad \text{לכן לפי משפט באז קיימים שלמים } x, y \text{ עבורם } \gcd(a, b) = 1$$

מכאן

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

על די הצבה של (\#2) ב- (\#1) נקבל

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

לכן $a | c$. **שאלה 12**א) לפי משפט באז, מכיוון ש- a, b זרים אז קיימים שלמים s, t עבורם

$$sa + tb = 1 .$$

נעביר אנפחים:

$$sa = -tb + 1$$

מכאן $sa \equiv 1 \pmod{b}$

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

$$ac = qb + 1 \iff \text{קיים שלם } q \text{ עבורו } 1$$

מכאן

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

עכשו b ו- a, b אינם זרים אז קיים מחלק משותף $d > 1$ כך ש-

$$\text{לכן } d \mid 1 \text{ וכן } d \mid (ac + (-q)b)$$

סתירה!

שאלה 13

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

נוסיף c לשני האגפים:

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

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

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

לכן

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

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

$$ac = Qm + bd$$

$$ac \equiv bd \pmod{m}$$

ג) אינדוקציה על n .

שאלה 14

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

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

אז

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

נניח כי בפרק הראשוןיים של m כל מס婢 ראשוני מופיע עם חזקה זוגית. אז

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

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

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

כאשר n הוא השלם

$$n = p_1^{e_1} \cdots p_k^{e_k}$$

(ב)

שאלה 15

- | | |
|----|------|
| א) | אמת |
| ב) | שקר |
| ג) | אמת |
| ד) | אמת |
| ה) | שקר |
| ו) | אמת |
| ז) | אמת |
| ח) | אמת |
| ט) | אמת |
| ו) | שקר. |

שאלה 16

- | | |
|----|---|
| א) | 0 |
| ב) | 4 |
| ג) | 4 |
| ד) | 5 |
| ה) | 2 |
| ו) | 1 |
| ז) | 1 |

- | | |
|---|-----|
| 0 | (ח) |
| 2 | (ט) |
| 1 | (ו) |

 שאלה 17

- | | |
|----|-----|
| 4 | (א) |
| 8 | (ב) |
| 1 | (ג) |
| 22 | (ד) |
| 14 | (ה) |

 שאלה 18

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

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

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

בנוסף זה נתון לנו ש- $b \equiv d \pmod{n}$, שכן באותו אופן אפשר להוכיח ש- $a \equiv c \pmod{n}$. לכן לפי התכונות חיבוריות של יחס מודולריית אנחנו נקבל כי

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

 שאלה 19

- | |
|-----|
| (א) |
| (ב) |
| (ג) |
| (ד) |