שיעור 1
תורת המספרים

1.1 הגדרות בסיסיות

הגדרה 1.1

יהיו a, b מספרים שלמים. אומרים כי b מחלק את a אם קיים מספר שלם q כך ש-

$$a = qb \ .$$

כלומר $\frac{a}{b}$ שווה למספר שלם q.

הסימון $a \mid b$ אומר כי b מחלק את a.

דוגמה 1.1

א) $6 \mid 3$ בגלל שקיים מספר שלם $q = 2$ כך ש- $6 = 3q$.

ב) $42 \mid 7$ בגלל שקיים מספר שלם $q = 6$ כך ש- $42 = 7q$.

ג) $8 \nmid 5$ בגלל שלא קיים מספר שלם q כך ש- $8 = 5q$.

הגדרה 1.2 יחס שקילות בין a ל- b

נניח כי $a, b \in \mathbb{Z}$ מספרים שלמים ו- m מספר שלם חיובי. היחס

$$a \equiv b \mod m$$

אומר כי m מחלק את ההפרש $a - b$, כלומר $m|a - b$.

בנסוח שקול, $a \equiv b \mod m$ אם קיים שלם q כך ש- $a = qm + b$.

לעתים אומרים כי "a שקול ל- b מודולו m".

דוגמה 1.2

הוכיחו כי

א $5 \equiv 2 \mod 3$

ב $43 \equiv 23 \mod 10$

ג $7 \not\equiv 2 \mod 4$

פתרון:

א)

$$5-2=3=1\cdot 3 \quad\Rightarrow\quad 3\,|\,5-2 \quad\Rightarrow\quad 5\equiv 2 \mod 3\ .$$

ב)

$$43-23=20=2\cdot 10 \quad\Rightarrow\quad 10\,|\,43-23 \quad\Rightarrow\quad 43\equiv 23 \mod 10\ .$$

ג) $7-2=5$.

לא קיים שלם q כך ש- $7-2=4q$ לכן $4\nmid 7-2$ לכן

$$7\not\equiv 2 \mod 4\ .$$

■

הגדרה 1.3 השארית

נתונים מספרים שלמים $a,b\in\mathbb{Z}$, היחס

$$a\ \texttt{\%}\ b$$

מציין את השארית בחלוקת a ב- b.

דוגמה 1.3

$$43\ \texttt{\%}\ 10=3\ .$$
$$13\ \texttt{\%}\ 4=1\ .$$
$$8\ \texttt{\%}\ 2=0\ .$$

$$-10\ \texttt{\%}\ 3=-1\ .$$

משפט 1.1 משפט החילוק של אוקלידס

יהיו a,b מספרים שלמים $b\neq 0$. קיימים מספרים שלמים q,r יחידים כך ש-

$$a=qb+r$$

כאשר $0\leq r<|b|$.

- b נקרא ה**מודולו**,
- q נקראת ה**מנה**
- ואילו r נקרא ה**שארית**.
- $r=a\ \texttt{\%}\ b$.

הוכחה: ההוכחה למטה בדף 18. והיא לא חלק של הקורס. ■

דוגמה 1.4

עבור המספרים $a=46$, $b=8$ מצאו את הפירוק האוקלידי $a=bq+r$.

פתרון:
עבור $b=8$ ו- $a=46$ מתקיים

$$46=8\cdot 5+6 \qquad \Rightarrow \qquad q=5\ ,r=6\ .$$

■

דוגמה 1.5

עבור $b=8$ ו- $a=-46$ מתקיים

$$-46=8\cdot(-6)+2 \qquad \Rightarrow \qquad q=-6\ ,r=2\ .$$

משפט 1.2 נוסחת השארית

נתונים $a,b>0$ מספר שלמים.

א) $a\ \%\ b=a-b\left\lfloor\frac{a}{b}\right\rfloor$.

ב) $(-a)\ \%\ b=b-(a\ \%\ b)=b\left\lceil\frac{a}{b}\right\rceil-a$.

הוכחה:

א) לפי משפט החילוק של אוקלידס 1.1, קיימים שלמים q,r כך ש-

$$a=qb+r \qquad (*1)$$

כאשר $0\leq r<b$ ו- $r=a\ \%\ b$. נחלק ב- b ונקבל

$$\frac{a}{b}=q+\frac{r}{b} \qquad (*2)$$

נשים לב כי $0<\frac{r}{b}<1$, לכן לפי (*2)

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

נציב זה ב- (*1) ונקבל

$$a=\left\lfloor\frac{a}{b}\right\rfloor b+r \quad \Rightarrow \quad r=a-b\left\lfloor\frac{a}{b}\right\rfloor\ . \qquad (*3)$$

ב) לפי משפט החילוק של אוקלידס 1.1, קיימים שלמים $q',0\leq r'<b$ כך ש-

$$-a=q'b+r'$$

כאשר $r'=(-a)\ \%\ b$. מכאן

$$a=-q'b-r'=-q'b-b+b-r'=-(q'+1)b+(b-r')\ . \qquad (*4)$$

נשים לב כי $b-r'\geq 0$. אבל לפי (*1) $a=qb+r$ כאשר $r=a\ \%\ b$ ו- r יחיד. לכן

$$r=b-r' \quad \Rightarrow \quad r'=b-r \stackrel{\text{משוואה (*3)}}{=} b-a+b\left\lfloor\frac{a}{b}\right\rfloor=b-\left(a-b\left\lfloor\frac{a}{b}\right\rfloor\right)=b-(a\ \%\ b)\ . \qquad (*5)$$

לכן $r' = (-a) \% b = b - (a \% b)$.

הזהות השני מנובע מ- (*5):

$$r = b - r' \quad \Rightarrow \quad r' = b - r \overset{\text{(*3) משוואה}}{=} b - a + b\left\lfloor \frac{a}{b} \right\rfloor - a + \left\lceil \frac{a}{b} \right\rceil \ .$$

לכן $r' = (-a) \% b = -a + \left\lceil \frac{a}{b} \right\rceil$.

■

דוגמה 1.6

מצאו את $101 \% 7$.

פתרון:

$a = 101$, $b = 7$,

$$101 \% 7 = 101 - 7\left\lfloor \frac{101}{7} \right\rfloor = 101 - 7(14) = 3 \ .$$

■

דוגמה 1.7

מצאו את $-101 \% 7$.

פתרון:

$-a = -101$, $b = 7$. נשתמש בנוסחה $(-a) \% b = b - (a \% m)$. מדוגמה הקודמת: $(101 \% 7) = 3$ לפיכך

$$(-101) \% 7 = 7 - (101 \% 7) = 7 - 3 = 4 \ .$$

■

הגדרה 1.4 המחלק המשותף הגדול ביותר gcd

נתונים שני מספרים שלמים $a, b > 0$.
המחלק המשותף הגדול ביותר של a ו- b מסומן $\gcd(a, b)$ (greatest common dividor) ומוגדר להיות המספר שלם הגדול ביותר שמחלק גם a וגם b.

דוגמה 1.8

$$\gcd(2, 6) = 2 \ ,$$

$$\gcd(3, 6) = 3 \ ,$$

$$\gcd(24, 5) = 1 \ ,$$

$$\gcd(20, 10) = 10 \ ,$$

$$\gcd(14, 12) = 2 \ ,$$

$$\gcd(8, 12) = 4 \ .$$

הגדרה 1.5 כפולה משותפת קטנה ביותר

נתונים שני מספרים שלמים $a, b > 0$.
הכפולה המשותפת הקטנה ביותר מסומן $\mathrm{lcm}(a, b)$ (lowest common multiple) ומוגדר להיות המספר השלם החיובי הקטן ביותר ש a ו- b מחלקים אותו.

דוגמה 1.9

$$\mathrm{lcm}(6, 21) = 42 \ ,$$
$$\mathrm{lcm}(3, 6) = 6 \ ,$$
$$\mathrm{lcm}(24, 5) = 120 \ ,$$
$$\mathrm{lcm}(20, 10) = 20 \ ,$$
$$\mathrm{lcm}(14, 12) = 84 \ ,$$
$$\mathrm{lcm}(8, 12) = 24 \ .$$

הגדרה 1.6 מספרים זרים

נניח כי $a \geq 1$ ו- $b \geq 2$ מספרים שלמים. אומרים כי a ו- b **מספרים זרים** אם

$$\gcd(a, b) = 1 \ .$$

במילים פשוטות, שני מספרים שלמים נקראים **מספרים זרים** אם המחלק המשותף המקסימלי שלהם הוא 1, כלומר, אין אף מספר גדול מאחת שמחלק את שניהם.

משפט 1.3 משפט הפירוק לראשוניים

המשפט היסודי של האריתמטיקה או **משפט הפירוק לראשוניים** קובע כי כל מספר טבעי ניתן לרשום כמכפלה יחידה של מספרים ראשוניים.
ז"א, יהי $a \in \mathbb{N}$ כל מספר טבעי. אז

$$a = p_1^{e_1} \times p_2^{e_2} \times \cdots \times p_n^{e_n} \ .$$

כאשר $p_1, \ldots, p_n$ מספרים ראשוניים ו- $e_1 \ldots e_n \in \mathbb{N}$, והפירוק הזה יחיד.

דוגמה 1.10

$$60 = 2^2 \times 3^2 \times 5 \ ,$$

דוגמה 1.11

$$98 = 2^1 \times 7^2 \ .$$

הגדרה 1.7 פונקציית אוילר

יהי m מספר שלם.
הפונקצית אוילר מסומנת ב- $\phi(m)$ ומוגדרת להיות השלמים שקטנים ממש מ- m וזרים ביחס ל- m.

$$\phi(m) := \left\{ a \in \mathbb{N} \,\middle|\, \gcd(a,m)=1,\ a<m \right\} \ .$$

דוגמה 1.12

מכיוון ש- $26=2\times 13$, הערכים של a עבורם $\gcd(a,26)=1$ הם

$$\{1,3,5,7,9,11,15,17,19,21,23,25\} \ .$$

ז"א יש בדיוק 12 ערכים של a עבורם $\gcd(a,26)=1$.

$$\phi(26)=12 \ .$$

משפט 1.4 הפירוק לראשוניים של פונקציית אוילר

נתון מספר טבעי m. נניח כי הפירוק למספרים ראשוניים שלו הוא

$$m=\prod_{i=1}^n p_i^{e_i} \ ,$$

כאשר p_i מספרים ראשוניים שונים ו- $e_i>0$ מספרים שלמיים ו- $1\leq i\leq n$. אז

$$\phi(m)=\prod_{i=1}^n \left(p_i^{e_i}-p_i^{e_i-1}\right) \ .$$

דוגמה 1.13

מצאו את $\phi(60)$.

פתרון:
$60=2^2\times 3^1\times 5^1$ לכן

$$\phi(60)=\left(2^2-2^1\right)\left(3^1-3^0\right)\left(5^1-5^0\right)=(2)(2)(4)=16 \ .$$

■

משפט 1.5 שיטה לחישוב $\gcd$

נתונים השלמים a,b כך שהפירוק לראשוניים שלהם הם:

$$a=p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k} \ , \qquad b={p_1}^{f_1}{p_2}^{f_2}\ldots {p_n}^{f_n}$$

וללא הגבלה כלליות נניח כי $k\leq n$. אז ה- $\gcd$ נתון על ידי

$$\gcd(a,b)=p_1^{\min(e_1,f_1)}p_2^{\min(e_2,f_2)}\ldots {p_k}^{\min(e_k,f_k)}$$

הוכחה: ■

דוגמה 1.14

מצאו את $\gcd(19200,320)$.

פתרון:

$$19200 = 2^8\,3^1\,5^2\ , \qquad 320 = 2^6\,5^1 = 2^6\,3^0\,5^1\ .$$

$$\gcd(19200,320) = 2^{\min(8,6)}3^{\min(1,0)}5^{\min(2,1)} = 2^6\,3^0\,5^1 = 320\ .$$

■

דוגמה 1.15

מצאו את $\gcd(154,36)$.

פתרון:

$$154 = 2^1\,7^1\,11^1\ , \qquad 36 = 2^2\,3^2\ .$$

ז"א

$$154 = 2^1\,3^0\,7^1\,11^1\ , \qquad 36 = 2^2\,3^2\,7^0\,11^0\ .$$

$$\gcd(154,36) = 2^{\min(1,2)}3^{\min(0,2)}7^{\min(1,0)}11^{\min(1,0)} = 2^1\,3^0\,7^0\,11^0 = 2\ .$$

■

משפט 1.6 שיטה לחישוב lcm

נתונים השלמים a,b כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1}p_2^{e_2}\ldots p_k^{e_k}\ , \qquad b = {p_1}^{f_1}{p_2}^{f_2}\ldots {p_n}^{f_n}$$

וללא הגבלה כלליות נניח כי $k \leq n$. אז ה- lcm נתון על ידי

$$\text{lcm}(a,b) = p_1^{\max(e_1,f_1)}p_2^{\max(e_2,f_2)}\ldots {p_k}^{\max(e_k,f_k)}$$

הוכחה: ■

משפט 1.7

$$\gcd(a,b)\,\text{lcm}(a,b) = ab\ .$$

הוכחה:

$$\min(a,b) + \max(a,b) = a+b\ .$$

■

1.2 האלגוריתם של אוקליד

משפט 1.8 האלגוריתם של אוקליד

יהיו a,b משפרים שלמים חיוביים ($a,b\in\mathbb{Z},a>0,b>0$). קיים אלגוריתם אשר נותן את $d=\gcd(a,b)$.

האלגוריתם הינו מתואר להלן. נגדיר

$$r_0=a\ ,\qquad r_1=b\ .$$

לפי משפט החילוק 1.1 קיימים שלמים q_1 ו- $0\leq r_2<|b|$ עבורם $a=bq_1+r_2$ כלומר

$$r_0=r_1q_1+r_2\ .$$

באותה מידה, לפי משפט החילוק קיימים שלמים q_2 ו- $0\leq r_3<|r_2|$ עבורם

$$r_1=r_2q_2+r_3\ .$$

התהליך ממשיך עד שנקבל $r_{n+1}=0$ בשלב ה- n- ית.

שלב $k=1$:	$a=bq_1+r_2$	$0\leq r_2<\|b\|$
שלב $k=2$:	$b=r_2q_2+r_3$	$0\leq r_3<\|r_2\|$
שלב $k=3$:	$r_2=r_3q_3+r_4$	$0\leq r_4<\|r_3\|$
$\vdots$		
שלב $k=n-1$:	$r_{n-2}=r_{n-1}q_{n-1}+r_n$	$0\leq r_n<\|r_{n-1}\|$
שלב $k=n$:	$r_{n-1}=r_nq_n$	$r_{n+1}=0$

התהליך מסתיים בשלב ה-n-ית אם $r_{n+1}=0$. ואז

$$r_n=\gcd(a,b)\ .$$

דוגמה 1.16

מצאו את ה- $\gcd(1071,462)$.

פתרון:

$a=1071,b=462$.

נגדיר $r_0=a=1071$ ו- $r_1=b=462$.

נבצע את האלגוריתם $r_{k-1}=q_kr_k+r_{k+1}$ עד השלב ה-n-ית שבו $r_{n+1}=0$.

שלב		q_k	r_{k+1}
$k=1$:	$1071=2\cdot 462+147\ .$	$q_1=2$	$r_2=147$
$k=2$:	$462=3\cdot 147+21$	$q_2=3$	$r_3=21$
$k=3$:	$147=7\cdot 21+0$	$q_3=7$	$r_4=0$

לפיכך $\gcd(1071, 462) = r_3 = 21$.

■

דוגמה 1.17

מצאו את $\gcd(26, 11)$.

פתרון:

$a = 26, b = 11$.

נגדיר $r_0 = a = 26$ ו- $r_1 = b = 11$.

נבצע את האלגוריתם $r_{k-1} = q_k r_k + r_{k+1}$ עד השלב ה-n-ית שבו $r_{n+1} = 0$.

שלב		q_k	r_{k+1}
$k = 1$:	$26 = 2 \cdot 11 + 4$.	$q_1 = 2$	$r_2 = 4$
$k = 2$:	$11 = 2 \cdot 4 + 3$	$q_2 = 2$	$r_3 = 3$
$k = 3$:	$4 = 1 \cdot 3 + 1$	$q_3 = 1$	$r_4 = 1$
$k = 4$:	$3 = 3 \cdot 1 + 0$	$q_4 = 3$	$r_5 = 0$

לכן $\gcd(26, 11) = r_4 = 1$.

■

משפט 1.9 משפט בזו (Bezout's identity)

יהיו a, b שלמים ויהי $d = \gcd(a, b)$.

קיימים שלמים s, t כך שניתן לרשום ה- $\gcd(a, b)$ כצירוף ליניארי של a ו- b:

$$sa + tb = d \ .$$

משפט 1.10 האלגוריתם של אוקליד המוכלל (שיטה 1)

יהיו a, b שלמים חיוביים. קיים אלגוריתם אשר נותן שלמים s, t עבורם

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$, כמפורט להלן.

מגדירים את הפרמטרים ההתחלתיים:

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

אז מבצעים את השלבים הבאים:

שלב 1:	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	$(0 \leq r_2 < \lvert r_1\rvert)$
שלב 2:	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	$(0 \leq r_3 < \lvert r_2\rvert)$
$\vdots$				
שלב k:	$r_{k+1} = r_{k-1} - q_k r_k$	$s_{k+1} = s_{k-1} - q_k s_k$	$t_{k+1} = t_{k-1} - q_k t_k$	$(0 \leq r_{k+1} < \lvert r_k\rvert)$
$\vdots$				
שלב $n-1$:	$r_n = r_{n-2} - q_{n-1} r_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} t_{n-1}$	$(0 \leq r_n < \lvert r_{n-1}\rvert)$
שלב n:	$r_{n+1} = 0$			

$$d = \gcd(a,b) = r_n \ , \qquad s = s_n \ , \qquad t = t_n \ .$$

דוגמה 1.18 (אלגוריתם איוקליד המוכלל)

מצאו את $d = \gcd(240, 46)$ ומצאו שלמים s, t עבורם $d = 240s + 46t$.

פתרון:

<u>פתרון לדוגמה 1.18 עם השיטה במשפט 1.10 של האלגוריתם איוקליד המוכלל</u>

$a = 240, b = 46$.

$$\begin{aligned} r_0 &= a = 240 \ , & r_1 &= b = 46 \ , \\ s_0 &= 1 \ , & s_1 &= 0 \ , \\ t_0 &= 0 \ , & t_1 &= 1 \ . \end{aligned}$$

שלב $k = 1$:	$r_2 = 240 - 5 \cdot 46 = 10$	$s_2 = 1 - 5 \cdot 0 = 1$	$t_2 = 0 - 5 \cdot 1 = -5$	$q_1 = 5$
שלב $k = 2$:	$r_3 = 46 - 4 \cdot 10 = 6$	$s_3 = 0 - 4 \cdot 1 = -4$	$t_3 = 1 - 4 \cdot (-5) = 21$	$q_2 = 4$
שלב $k = 3$:	$r_4 = 10 - 1 \cdot 6 = 4$	$s_4 = 1 - 1 \cdot (-4) = 5$	$t_4 = -5 - 1 \cdot (21) = -26$	$q_3 = 1$
שלב $k = 4$:	$r_5 = 6 - 1 \cdot 4 = 2$	$s_5 = -4 - 1 \cdot 5 = -9$	$t_5 = 21 - 1 \cdot (-26) = 47$	$q_4 = 1$
שלב $k = 5$:	$r_6 = 4 - 2 \cdot 2 = 0$	$s_6 = 5 - 2 \cdot (-9) = 23$	$t_6 = -26 - 2 \cdot (47) = -120$	$q_5 = 2$

$$\gcd(a,b) = r_5 = 2 \ , \qquad s = s_5 = -9 \ , \qquad t = t_5 = 47 \ .$$

$$ta + sb = -9(240) + 47(46) = 2 \ .$$

■

יש שיטה נוספת למציאת המקדמים s, t במשפט בזו. נתאר אותה על ידי הדוגמה הקודמת.

<u>פתרון לדוגמה 1.18 עם השיטה השניה של האלגוריתם איוקליד המוכלל</u>

לשיטה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקליד במשפט 1.8.

(0*) $\boxed{240} = 5 \cdot \boxed{46} + \boxed{10}$

(1*) $\boxed{46} = 4 \cdot \boxed{10} + \boxed{6}$

(2*) $\boxed{10} = 1 \cdot \boxed{6} + \boxed{4}$

(3*) $\boxed{6} = 1 \cdot \boxed{4} + \boxed{2}$

(4*) $\boxed{4} = 2 \cdot \boxed{2} + 0$

לכן $d = \gcd(240, 46) = 2$.

בשלב השני רושמים 2 כצירוף לינארי של 240 ו- 46 באמצעות המשוואות למעלה:

$$\begin{aligned}
\boxed{2} &= \boxed{6} - 1 \cdot \boxed{4} && \text{לפי (3*)}\\
&= \boxed{6} - 1 \cdot \left(\boxed{10} - 1 \cdot \boxed{6}\right) && \text{לפי (2*)}\\
&= 2 \cdot \boxed{6} - 1 \cdot \boxed{10} \\
&= 2 \cdot \left(\boxed{46} - 4 \cdot \boxed{10}\right) - 1 \cdot \boxed{10} && \text{לפי (1*)}\\
&= 2 \cdot \boxed{46} - 9 \cdot \boxed{10} \\
&= 2 \cdot \boxed{46} - 9 \cdot \left(\boxed{240} - 5 \cdot \boxed{46}\right) && \text{לפי (0*)}\\
&= 47 \cdot \boxed{46} - 9 \cdot \boxed{240} \ .
\end{aligned}$$

■

דוגמה 1.19 (אלגוריתם איוקליד המוכלל)

מצאו את $d = \gcd(326, 78)$ ומצאו שלמים s, t עבורם $d = 326s + 78t$.

פתרון:

<u>פתרון לדוגמה 1.19 עם השיטה במשפט 1.10 של האלגוריתם איוקליד המוכלל</u>

$a = 326, b = 78$.

$$\begin{aligned}
r_0 &= a = 326 \ , & r_1 &= b = 78 \ ,\\
s_0 &= 1 \ , & s_1 &= 0 \ ,\\
t_0 &= 0 \ , & t_1 &= 1 \ .
\end{aligned}$$

שלב $k = 1$:	$r_2 = 326 - 4 \cdot 78 = 14$	$s_2 = 1 - 4 \cdot 0 = 1$	$t_2 = 0 - 4 \cdot 1 = -4$	$q_1 = 4$
שלב $k = 2$:	$r_3 = 78 - 5 \cdot 14 = 8$	$s_3 = 0 - 5 \cdot 1 = -5$	$t_3 = 1 - 5 \cdot (-4) = 21$	$q_2 = 5$
שלב $k = 3$:	$r_4 = 14 - 1 \cdot 8 = 6$	$s_4 = 1 - 1 \cdot (-5) = 6$	$t_4 = -4 - 1 \cdot (21) = -25$	$q_3 = 1$
שלב $k = 4$:	$r_5 = 8 - 1 \cdot 6 = 2$	$s_5 = -5 - 1 \cdot 6 = -11$	$t_5 = 21 - 1 \cdot (-25) = 46$	$q_4 = 1$
שלב $k = 5$:	$r_6 = 6 - 3 \cdot 2 = 0$			$q_5 = 3$

$$\gcd(a,b)=r_5=2\ ,\qquad s=s_5=-11\ ,\qquad t=t_5=46\ .$$

$$sa+tb=-11(326)+46(78)=2\ .$$

■

יש שיטה נוספת למציאת המקדמים s,t במשפט בזו. נתאר אותה על ידי הדוגמה הקודמת.

פתרון לדוגמה 1.19 עם השיטה השניה של האלגוריתם איוקליד המוכלל

לשיטה הזאת יש 2 שלבים. בשלב הראשון מבצעים האלגוריתם של אוקליד במשפט 1.8.

$$\boxed{326}=4\cdot\boxed{78}+\boxed{14} \qquad (*0)$$
$$\boxed{78}=5\cdot\boxed{14}+\boxed{8} \qquad (*1)$$
$$\boxed{14}=1\cdot\boxed{8}+\boxed{6} \qquad (*2)$$
$$\boxed{8}=1\cdot\boxed{6}+\boxed{2} \qquad (*3)$$
$$\boxed{4}=3\cdot\boxed{2}+0 \qquad (*4)$$

לכן $d=\gcd(326,78)=2$.

בשלב השני רושמים 2 כצירוף לינארי של 326 ו- 78 באמצעות המשוואות למעלה:

$$\begin{aligned}
\boxed{2}&=\boxed{8}-1\cdot\boxed{6} && \text{לפי } (*3)\\
&=\boxed{8}-1\cdot\left(\boxed{14}-1\cdot\boxed{8}\right) && \text{לפי } (*2)\\
&=2\cdot\boxed{8}-1\cdot\boxed{14}\\
&=2\cdot\left(\boxed{78}-5\cdot\boxed{14}\right)-1\cdot\boxed{14} && \text{לפי } (*1)\\
&=2\cdot\boxed{78}-11\cdot\boxed{14}\\
&=2\cdot\boxed{78}-11\cdot\left(\boxed{326}-4\cdot\boxed{78}\right) && \text{לפי } (*0)\\
&=46\cdot\boxed{78}-11\cdot\boxed{326}\ .
\end{aligned}$$

■

1.3 משפטים של מספרים ראשוניים

משפט 1.11 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח הטענה דרך השלילה.
נניח כי $\{p_1,\ldots,p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.
נגדיר השלם $M=(p_1\cdot p_2\cdot\ldots\cdot p_n)+1$.
לפי משפט הפירוק לראשוניים (ראו משפט 1.3 למעלה או משפט 5.3 למטה) M הוא מספר ראשוני או שווה למכפלה של ראשוניים.

M לא מספר ראשוני בגלל ש- $M > p_i$ לכל $1 \leq i \leq n$.
גם לא קיים מספר ראשוני p_i אשר מחלק את M. הרי

$$M \,\%\, p_i = 1 \quad \Rightarrow \quad p_i \nmid M \ .$$

הגענו לסתירה של המשפט הפירוק לראשוניים, לכן קיימים אינסוף מספרים ראשוניים. ■

משפט 1.12 משפט הפירוק לראשוניים

(ראו משפט 1.3) לכל מספר שלם n קיימים שלמים e_i וראשוניים p_i כך ש-

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

הוכחה: אינדוקציה. ■

משפט 1.13 נוסחה לפונקצית אוילר

(ראו משפט 1.4) לכל מספר שלם n בעל פירוק לראשוניים

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

פונקציית אוילר ניתנת על ידי

$$\phi(n) = \prod_{i=1}^{k} \left(p_i^{e_i} - p_i^{e_i-1}\right) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right) \ldots \left(p_k^{e_k} - p_k^{e_k-1}\right)$$

דוגמה 1.20

חשבו את $\phi(24)$

פתרון:

$$24 = 2^3 3^1 \ .$$

לכן

$$\phi(24) = (2^3 - 2^2)(3^1 - 3^0) = (8-4)(3-1) = 8 \ .$$

■

משפט 1.14

אם p מספר ראשוני אז

$$\phi(p) = p - 1 \ .$$

הוכחה: תרגיל בית. ■

משפט 1.15

אם p מספר ראשוני אז

$$\phi\left(p^n\right) = p^n - p^{n-1} \ .$$

הוכחה: תרגיל בית. ■

משפט 1.16

אם s,t שלמים זרים (כלומר $\gcd(s,t)=1$) אז

$$\phi(s\cdot t)=\phi(s)\cdot\phi(t)\ .$$

הוכחה: תרגיל בית. ■

משפט 1.17

אם p ו- q מספרים ראשוניים שונים אז

$$\phi(p\cdot q)=(p-1)(q-1)\ .$$

הוכחה: תרגיל בית. ■

משפט 1.18 המשפט הקטן של פרמה

אם p מספר ראשוני ו- $a\in\mathbb{Z}_p$. אז התנאים הבאים מתקיימים:

1. $a^p\equiv a \mod p$
2. $a^{p-1}\equiv 1 \mod p$
3. $a^{-1}\equiv a^{p-2} \mod p$

הוכחה:

טענה 1. נוכיח באינדוקציה.

<u>בסיס:</u>

עבור $a=0$ הטענה $0^p\equiv 0 \mod p$ מתקיימת.

<u>מעבר:</u>

נניח כי הטענה מתקיימת עבור a.

$$(a+1)^p=a^p+pa^{p-1}+\frac{p(p-1)}{2}a^{p-2}+\cdots+pa+1\equiv a^p+1 \mod p$$

ההנחת האינדוקציה אומרת ש- $a^p\equiv a \mod p$ לכן

$$(a+1)^p \mod p\equiv a^p+1 \mod p\equiv(a+1) \mod p$$

כנדרש.

טענה 2. $\gcd(a,p)=1$ לפיכך קיים איבר הופכי $a^{-1}\in\mathbb{Z}_p$. נכפיל $a^p\equiv 1 \mod p$ ב- a^{-1} אשר הוכחנו בסעיף הקודם:

$$a^{-1}a^p\equiv a^{-1}\cdot a \mod p \qquad\Rightarrow\qquad a^{p-1}\equiv 1 \mod p\ .$$

טענה 3.

$$a^{p-1}\equiv 1 \mod p \qquad\Leftrightarrow\qquad 1\equiv a^{p-1} \mod p \quad\Rightarrow\quad a^{-1}\equiv a^{p-2} \mod p\ .$$

■

משפט 1.19 משפט אוילר

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז
$$a^{\phi(n)} \equiv 1 \mod n \ .$$

משפט 1.20

אם a, n שלמים ו- $\gcd(a, n) = 1$ אז
$$a^{-1} \equiv a^{\phi(n)-1} \mod n \ .$$

דוגמה 1.21

חשבו את האיבר ההופכי ל- 5 ב- $\mathbb{Z}_{11}$.

פתרון:

לפי משפט פרמט 5.9:
$$5^{-1} = 5^{11-2} \mod 11 = 5^9 \mod 11 \ .$$

לפי הנוסחת לשארית 1.2 :
$$5^9 \ \% \ 11 = 5^9 - 11 \left\lfloor \frac{5^9}{11} \right\rfloor = 9$$

לכן $5^{-1} \in \mathbb{Z}_{11} = 9$. ■

1.4 משפט השאריות הסיני

משפט 1.21 משפט השאריות הסיני

יהיו $m_1, m_2, \ldots, m_r$ שלמים אשר זרים בזוגות ויהיו $a_1, a_2, \ldots, a_r$ שלמים. למערכת של יחסים שקילות
$$\begin{aligned} x =& a_1 \mod m_1 \ , \\ x =& a_2 \mod m_2 \ , \\ &\vdots \\ x =& a_r \mod m_r \ , \end{aligned}$$

קיים פתרון יחיד מודולו $M = m_1 m_2 \cdots m_r$ שניתן על ידי
$$x = \sum_{i=1}^{r} a_i M_i y_i \mod M$$

כאשר $M_i = \dfrac{M}{m_i}$ ו- $y_i = M_i^{-1} \mod m_i$ לכל $1 \leq i \leq r$.

דוגמה 1.22

היעזרו במשפט השאריות הסיני כדי לפתור את המערכת
$$\begin{aligned} x =& 22 \mod 101 \ , \\ x =& 104 \mod 113 \ . \end{aligned}$$

פתרון:

$$a_1 = 22 \ , \qquad a_2 = 104 \ , \qquad m_1 = 101 \ , \qquad m_2 = 113 \ .$$

$$M = m_1 m_2 = 11413 \ , \qquad M_1 = \frac{M}{m_1} = 113 \ , \qquad M_2 = \frac{M}{m_2} = 101 \ .$$

בעזרת הקוד-פיתון `modularinverse.py`

$$y_1 = M_1^{-1} \mod m_1 = 113^{-1} \mod 101 = 59$$

$$x = 22 \cdot \left(\frac{101 \cdot 113}{101}\right) \cdot$$

ו-

$$y_2 = M_2^{-1} \mod m_2 = 101^{-1} \mod 113 = 47$$

$$\begin{aligned} x =& a_1 M_1 y_1 + a_2 M_2 y_2 \mod M \\ =& 22 \cdot 113 \cdot 59 + 104 \cdot 111 \cdot 47 \mod 11413 \\ =& 640362 \mod 11413 \\ =& 1234 \ . \end{aligned}$$

■

1.5 הוכחות של משפטים*

משפט 1.22 משפט החילוק של אוקלידס

יהיו a,b מספרים שלמים $b \neq 0$. קיימים מספרים שלמים q,r יחידים כך ש-

$$a = qb + r$$

כאשר $0 \leq r < |b|$.

- b נקרא ה **מודולו**,
- q נקראת ה**מנה**
- ואילו r נקרא ה**שארית**.
- $r = a$ % b.

הוכחה:
ראשית נוכיח כי לכל a,b קיימים שלמים q,r כך ש- $a = qb + r$, כאשר $0 \leq r < |b|$, ואחר כך נוכיח ש- q,r יחידים.

אנחנו נניח כי $b \neq 0$.

<u>קיום</u>

נגדיר את הקבוצת שלמים אי-שליליים הבאה:

$$S \triangleq \left\{ a - qb \;\middle|\; q \in \mathbb{Z} \;,\; a - qb \geq 0 \right\} \;.$$

נראה כי S קבוצה לא ריקה.

- <u>מקרה $b > 0$</u>:

  אם $b > 0$ אזי קיים שלם $N > 0$ מספיק גדול כך ש- אם $q = -N$ אזי האיבר $a - qb = a + Nb > 0$ ולכן הוא שייך ל-S.

- <u>מקרה $b < 0$</u>:

  אם $b < 0$ אזי קיים שלם $N > 0$ מספיק גדול כך ש- אם $q = N$ אזי האיבר $a - qb = a - Nb > 0$ ולכן הוא שייך ל-S.

לכן $S \neq \emptyset$. לכן על פי העקרון הסדר הטוב (שקובע שלקבוצת שלמים אי-שליליים יש איבר מינימלי) קיים איבר מינימלי של S. ז"א קיים q עבורו

$$r = a - qb = \min \; S \qquad (*)$$

הוא האיבר המינילי של S.
כעת נוכיח כי $0 \leq r < |b|$. לפי ההגדרה של הקבוצה S, $0 \geq r$. נראה כי $|b| < r$. נניח בשלילה כי $|b| \geq r$.
יש שני מקרים:

- <u>אם $b > 0$</u> אז

  $$r - b \overset{(*\text{ משוואה})}{=} a - (q+1)b \geq 0$$

  ולכן $r - b$ שייך ל- S גם כן. אבל, מכיוון ש- $b > 0$ אזי

  $$r - b < r$$

  והרי מצאנו שקיים האיבר $r - b$ של S היותר קטן מ- r, בסתירה לכך ש- r הוא האיבר המינילי של S.

- <u>אם $b < 0$</u> אז $|b| = -b$, אז

  $$r - |b| = r - (-b) = r + b \overset{(*\text{ משוואה})}{=} a - (q-1)b \geq 0$$

  ולכן $r - |b|$ שייך ל- S גם כן. אבל, מכיוון ש- $b < 0$ אזי

  $$r - |b| = r + b < r$$

  והרי מצאנו שקיים האיבר $r - |b|$ של S היותר קטן מ- r, בסתירה לכך ש- r הוא האיבר המינילי של S.

לפיכך בהכרח: $0 \leq r < |b|$.
הוכחנו קיום של q, r עבורם $a = qb + r$. כעת נוכיח שהם יחידים.

<u>יחידות</u>

נניח בשלילה שעבור השלמים a, b כלשהם קיימים שלמים q_1, r_1 עבורם

$$a = q_1 b + r_1 \;,$$

ונניח שקיימים שלמים $q_1 \neq q_2$, $r_1 \neq r_2$ עבורם

$$a = q_2 b + r_2 \;.$$

לכן

$$\left.\begin{aligned} a &= q_1 b + r_1 \\ a &= q_2 b + r_2 \end{aligned}\right\} \Rightarrow \left.\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= a - q_2 b \end{aligned}\right\} \Rightarrow r_2 - r_1 = (q_1 - q_2) b \quad \Rightarrow \quad |r_2 - r_1| = |q_1 - q_2| \cdot |b| \qquad \text{(\#1)}$$

בצד שני מכיוון ש- $0 \leq r_1, r_2 < |b|$ אזי

$$|r_1 - r_2| < |b| \ . \qquad \text{(\#2)}$$

המשוואות (#1) ו- (#2) מהוות סתירה. לכן לא יתכן ש- $q_1 \neq q_2$ או ש- $r_1 \neq r_2$.

לסיכום הוכחנו כי עבור כל a, b קיימים q, r כך ש-

$$a = qb + r$$

ושהם יחידים.

■