

שיעור 1

תורת המספרים

1.1 משפט חילוק של אוקלידס

הגדרה 1.1 מספר שלם שמחולק במספר שלם אחר

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

$$a = qb .$$

כלומר $\frac{a}{b}$ שווה למספר שלם q .

הסימן $a | b$ אומר כי b מחלק את a .

דוגמה 1.1

א) $6 | 3$ בגלל שקיימים מספר שלם $q = 2$ כך ש- $6 = 3q$

ב) $42 | 7$ בgalל שקיימים מספר שלם $q = 6$ כך ש- $42 = 7q$

ג) $8 \nmid 5$ בgalל שלא קיימים מספר שלם q כך ש- $5q = 8$

משפט 1.1 תכונות של חילוק שלמים

יהיו a, b, d שלמים.

(1) אם $d | (a + b)$ ו- $d | b$ אז $d | a$

(2) יהיו x, y שלמים. אם $d | b$ ו- $d | a$ אז $d | (xa + yb)$

(3) אם $a = \pm b$ אז $b | a$ ו- $a | b$

הוכחה:

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow a = a'd \quad \Rightarrow \quad a \pm b = d(a' + b') \quad \Rightarrow \quad d | (a + b) . \quad (1)$$

$$\left. \begin{array}{l} d|a \\ d|b \end{array} \right\} \Rightarrow a = a'd \quad \Rightarrow \quad ax + by = d(a'x + b'y) \quad \Rightarrow \quad d | (ax + by) . \quad (2)$$

$$\left. \begin{array}{l} a|b \\ b|a \end{array} \right\} \Rightarrow b = ca \quad \Rightarrow \quad b = ca = cc'b \quad \Rightarrow \quad cc' = 1 . \quad (3)$$

ונ- c' הם שלמים לכך $cc' = 1$ אם ורק אם $c = c'$ או $c = -1$. לפיכך $b = \pm a$.

הגדרה 1.2 השארית

יהיו $a, b > 0$ שלמים. השארית של a בחלוקת b -השאירה b מסומנת $a \bmod b$ ומוגדרת

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

סימון חלופי לשארית בחלוקת a ב- b : $a \% b$

הערה: השארית מוגדרת באופן חד משמעי עבור שלמים חיוביים בלבד!

דוגמה 1.2

$$43 \bmod 10 = 43 - 10 \cdot \left\lfloor \frac{43}{10} \right\rfloor = 43 - 10(4) = 3 ,$$

$$13 \bmod 4 = 13 - 4 \cdot \left\lfloor \frac{13}{4} \right\rfloor = 13 - 4(3) = 1 ,$$

$$8 \bmod 2 = 8 - 2 \cdot \left\lfloor \frac{8}{2} \right\rfloor = 8 - 2(4) = 0 .$$

משפט 1.2 משפט החלוק של אוקלידס

יהיו a, b מספרים שלמים. אם $b \neq 0$ ו- $a \geq b$ אז קיימים מספרים שלמים q, r ייחודיים כך ש-

$$a = qb + r \quad (1.1)$$

כאשר $|r| \leq b$. השם q נקרא המנה של a בחלוקת b -השאירה r של a בחלוקת b -השאירה a .

ההוכחה עצמה היא לא חלק של הקורס.

דוגמה 1.3

יהיו $a = 46, b = 8$. המנה והשאירה הם $q = 5, r = 6$ והפירוק מנה-שאירה הוא

$$46 = 5(8) + 6 .$$

דוגמה 1.4

יהיו $a = -46, b = 8$. המנה והשאירה הם $q = -6, r = 2$ והפירוק מנה-שאירה הוא

$$-46 = (-6)(8) + 2 .$$

משפט 1.3 שיטה מעשית לחישוב החלוקת מנת-שארית

יהיו a, b שלמים ($a \neq 0$). אין מנתה q והשארית r במשפט החלוק של אוקלידס ניתנים כך:

$$r = a \bmod b \text{ ו } q = \left\lfloor \frac{a}{b} \right\rfloor \text{ אם } a > 0, b > 0 \quad (1)$$

$$r = a \bmod |b| \text{ ו } q = -\left\lfloor \frac{a}{|b|} \right\rfloor \text{ אם } a > 0, b < 0 \quad (2)$$

$$r = b - |a| \bmod b \text{ ו } q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1 \text{ אם } a < 0, b > 0 \quad (3)$$

$$r = |b| - |a| \bmod |b| \text{ ו } q = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1 \text{ אם } a < 0, b < 0 \quad (4)$$

הוכחה: נוכיח בכל אחד מארבעת המקרים.

מצב 1 נניח $0 < a$. לפי משפט החלוק של אוקלידס קיימים שלמים r, q כך ש-

$$a = qb + r, \quad 0 \leq r < b. \quad (*)$$

$$\frac{a}{b} = q + \frac{r}{b}.$$

נחלק ב- b :

$$0 \leq \frac{r}{b} < 1, \text{ מתקיים } 0 \leq r < b, \text{ ולכן}$$

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

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

הצבה חוזרת ב-(*) נותנת

מצב 2 נניח $0 < a$. לפי משפט החלוק של אוקלידס עבור השלמים \bar{r}, \bar{q} כך ש:

$$a = \bar{q}|b| + \bar{r}, \quad 0 \leq \bar{r} < |b|.$$

$$|b| = -b. \bar{r} = a \bmod |b| \text{ ו } \bar{q} = \left\lfloor \frac{a}{|b|} \right\rfloor \text{ מהמקרה הראשון:}$$

$$a = \bar{q}(-b) + \bar{r} \Rightarrow a = -\bar{q}b + \bar{r}. \quad (#)$$

מצד שני משפט החלוק עבור השלמים b, a (כלומר b בלי הערך מוחלט) קיימים שלמים r, q כך ש:

$$a = qb + r, \quad 0 \leq r < |b|.$$

השווואה של משווה (#) ל- $a = qb + r$ נותנת

$$q = -\bar{q} = -\left\lfloor \frac{a}{|b|} \right\rfloor, \quad r = \bar{r} = a \bmod |b|.$$

מצב 3 נניח $a < 0, b > 0$. משפט החלוק עבור הלשימים b , \bar{r} קיימים שלמים \bar{q} כך ש:

$$|a| = \bar{q}b + \bar{r}, \quad 0 \leq \bar{r} < b.$$

מהמקרה הראשון:

$$\bar{q} = \left\lfloor \frac{|a|}{b} \right\rfloor, \quad \bar{r} = |a| \bmod b.$$

$$-a = \bar{q}b + \bar{r} \Rightarrow a = -\bar{q}b - \bar{r}. \quad :|a| = -a$$

כעת השארית \bar{r} – שלילית, ואינה עומדת בתנאי $0 \leq r < b$. לכן נוסיף ונחסר מנתה שלמה b :

$$a = -\bar{q}b - \bar{r} = -(\bar{q} + 1)b + (b - \bar{r}). \quad (**)$$

כך קיבלנו את הצורה הנדרשת. מצד שני עבור הלשימים a, b (כלומר a בלי הערך מוחלט) משפט החלוק קיימים שלמים r, q עוברים

$$a = qb + r, \quad 0 \leq r < b.$$

השווואה של זה עם משווה (** נותרת):

$$q = -\left\lfloor \frac{|a|}{b} \right\rfloor - 1, \quad r = b - |a| \bmod b.$$

מצב 4 נניח $a < 0, b < 0$. לפי משפט החלוק עבור $|a|, |b|$ קיימים שלמים \bar{r}, \bar{q} כך ש:

$$|a| = \bar{q}|b| + \bar{r}, \quad 0 \leq \bar{r} < |b|.$$

מ-(1) קיבל

$$\bar{q} = \left\lfloor \frac{|a|}{|b|} \right\rfloor, \quad \bar{r} = |a| \bmod |b|.$$

$$:|a| = -a, |b| = -b$$

$$-a = -\bar{q}|b| + \bar{r} \Rightarrow a = \bar{q}|b| - \bar{r}.$$

כמו קודם נוסיף ונחסר $|b|$ כדי להפוך את השארית לחיבורית:

$$\begin{aligned} a &= \bar{q}|b| - |b| + |b| - \bar{r} \\ \Rightarrow \quad a &= \bar{q}|b| + b + |b| - \bar{r} \\ \Rightarrow \quad a &= (\bar{q} + 1)|b| + |b| - \bar{r}. \end{aligned} \quad (\#)$$

מצד שני משפט החלוק עבור הלשימים b, a (לא הערכים מוחלטים שלהם) קיימים שלמים r, q עוברים:

$$a = qb + r, \quad 0 \leq r < |b|.$$

השווואה של $a = qb + r$ למשווה (# נותרת):

$$q = \bar{q} + 1 = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1, \quad r = |b| - \bar{r} = |b| - |a| \bmod |b|.$$

שארית r	מנה q	מספר b	סימן a	סימן b	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	



דוגמה 1.5

מצאו את הפירוק מנתה-שארית של השלמים הבאים:

$$a = 46, b = 8 \quad \text{(א)}$$

$$a = -46, b = 8 \quad \text{(ב)}$$

$$a = 101, b = -7 \quad \text{(ג)}$$

$$a = -151, b = -12 \quad \text{(ד)}$$

פתרונות:

(א) במקרה זה $a > 0, b > 0$ אז

$$q = \left\lfloor \frac{a}{b} \right\rfloor = \left\lfloor \frac{46}{8} \right\rfloor = 5, \quad r = a \bmod b = a - b \left\lfloor \frac{a}{b} \right\rfloor = 46 - 8 \left\lfloor \frac{46}{8} \right\rfloor = 6,$$

לכן:

$$46 = (5)(8) + 6.$$

(ב) במקרה זה $a < 0, b > 0$ אז

$$q = - \left\lfloor \frac{|a|}{b} \right\rfloor - 1 = - \left\lfloor \frac{46}{8} \right\rfloor - 1 = -6$$

-1

$$\begin{aligned} r &= b - |a| \bmod b \\ &= b - \left(|a| - b \left\lfloor \frac{|a|}{b} \right\rfloor \right) \\ &= 8 - \left(46 - 8 \left\lfloor \frac{46}{8} \right\rfloor \right) \\ &= 8 - (46 - 8(5)) \\ &= 2. \end{aligned}$$

לכן:

$$-46 = (-6)(8) + 2.$$

ג) במקרה זה $a > 0, b < 0$ אז

$$q = -\left\lfloor \frac{a}{|b|} \right\rfloor = -\left\lfloor \frac{101}{7} \right\rfloor = -14 .$$

-1

$$r = a \bmod |b| = a - |b| \left\lfloor \frac{a}{|b|} \right\rfloor = 101 - 7 \left\lfloor \frac{101}{7} \right\rfloor = 101 - 7(14) = 3 .$$

לכן:

$$101 = (-14)(-7) + 3 .$$

ד) במקרה זה $a < 0, b < 0$ אז

$$q = \left\lfloor \frac{|a|}{|b|} \right\rfloor + 1 = \left\lfloor \frac{151}{12} \right\rfloor + 1 = 12 + 1 = 13 .$$

-1

$$\begin{aligned} r &= |b| - |a| \bmod |b| \\ &= |b| - \left(|a| - |b| \left\lfloor \frac{|a|}{|b|} \right\rfloor \right) \\ &= 12 - \left(151 - 12 \left\lfloor \frac{151}{12} \right\rfloor \right) \\ &= 12 - (151 - 12(12)) \\ &= 12 - 7 \\ &= 5 . \end{aligned}$$

לכן:

$$-151 = (13)(-12) + 5 .$$



1.2 מספרים ראשוניים

הגדרה 1.3 מספר ראשוני

מספר ראשוני הוא מספר שלם וחילובי $2 \geq p$ עבורו המחלקים היחידים שלו הם 1 ו- p בלבד.
ז"א p ראשוני אם התנאי הבא מתקיים:

$$a \mid p \iff a = 1 \vee p .$$

משפט 1.4 משפט הפירוק לזרים

כל מספר טבעי $a \geq 2$ הוא מספר ראשוני או שווה למכפלה של מספרים ראשוניים.
ז"א לכל מספר טבעי $a \geq 2$ קיימים טבעיים e_1, \dots, e_n עבורם

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

כאשר p_1, \dots, p_n מספרים ראשוניים.

דוגמה 1.6

הפירוק לראשוניים של 60 הוא:

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

דוגמה 1.7

הפירוק לראשוניים של 98 הוא:

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

הוכחה:

- נניח בשלילה שהטענה לא נכונה. אז קיימים לפחות מספר טבעי אחד שלא ראשוני וגם לא שווה למינימום של ראשוניים.
- יהי $2 \leq m$ הטבעי הקטן ביותר שלא מקיים הטענה זו. (m הוא הדוגמה הנגדית הקטנה ביותר).
- אזי m לא ראשוני וגם לא שווה למינימום של ראשוניים.
- לכן m פריך, ז"א קיימים טבעיים $2 \leq a < m$, $2 \leq b < m$ כך ש:

$$m = ab .$$

- m הוא הטבעי הקטן ביותר מסווג זה שמספריך את הטענה בעוד b , a , הם קטנים ממש מ- m אז a ו- b בהכרח מקיימים את הטענה: ז"א a או b ראשוני או שווה למינימום של ראשוניים, ואוטו דבר עבור b .

- לכן קיימים טבעיים e_1, e_2, \dots, e_n עבורם

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}$$

כאשר p_1, \dots, p_n מספרים ראשוניים וקיימים טבעיים f_1, \dots, f_n עבורם

$$b = q_1^{f_1} q_2^{f_2} \dots q_n^{f_n}$$

כאשר q_1, \dots, q_n מספרים ראשוניים.

- מכאן

$$m = ab = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n} q_1^{f_1} q_2^{f_2} \dots q_n^{f_n} .$$

לכן m שווה למינימום של מספרים ראשוניים, בסתיויה לכך m לא שווה למינימום של ראשוניים!**משפט 1.5 קיימים אינסוף מספרים ראשוניים**

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח את הטענה דרך השלילה.

נניח כי $\{p_1, \dots, p_n\} = P$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי. נגיד הרسلم $1 + p_n + p_1 p_2 \dots p_n = m$.לפי משפט הפירוק לזרים (ראו משפט 1.4) m הוא ראשוני או שווה למינימום של ראשוניים. לפי ההנחה התחולית שלנו, אין מצב ש- m יכול להיות מספר ראשוני בغالל ש- m גדול ממש מכל הראשוניים בקבוצת כל הראשוניים P . כלומר, $m > p_i$ לכל $n \leq i \leq 1$. גם לא קיים מספק ראשוני p_i אשר מחלק את m . הרי

$$m \pmod{p_i} = 1 \Rightarrow p_i \nmid m .$$

הגענו לסתירה להמשפט הפירוק לזרים. לכן קיימים אינסוף מספרים ראשוניים.

1.3 המחלק המשותף הגדול ביותר

הגדירה 1.4 המחלק המשותף הגדול ביותר (gcd).

יהיו a, b שלמים. המחלק המשותף הגדול ביותר של a ו- b מסומן $\text{gcd}(a, b)$ ומוגדר להיות השם החיוויי grootste gemeenschappelijke deler ביטר. a וגם b .

הסימון gcd מנובע מהשם אנגלי "greatest common divisor".

דוגמה 1.8

$$\text{gcd}(2, 6) = 2 ,$$

$$\text{gcd}(3, 6) = 3 ,$$

$$\text{gcd}(24, 5) = 1 ,$$

$$\text{gcd}(20, 10) = 10 ,$$

$$\text{gcd}(14, 12) = 2 ,$$

$$\text{gcd}(8, 12) = 4 .$$

הגדירה 1.5 כפולה המשותפת הקטנה ביותר

יהיו a, b שלמים. הcpfולה המשותפת הקטנה ביותר ביטר מסומנת $\text{lcm}(a, b)$ ומוגדרת להיות השם החיוויי kleinste gemeenschappelijke veelvoud ביטר. a וגם b מחלקים אותו.

הסימון lcm מנובע מהשם אנגלי "lowest common multiple".

דוגמה 1.9

$$\text{lcm}(6, 21) = 42 ,$$

$$\text{lcm}(3, 6) = 6 ,$$

$$\text{lcm}(24, 5) = 120 ,$$

$$\text{lcm}(20, 10) = 20 ,$$

$$\text{lcm}(14, 12) = 84 ,$$

$$\text{lcm}(8, 12) = 24 .$$

הגדרה 1.6 מספרים זרים

יהיו a, b שלמים. אומרים כי a ו- b **מספרים זרים** אם

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

כלומר, אין אף מספר גדול מאחד שמחלק את שניהם.

משפט 1.6 שיטת פירוק לראשונה לחישוב \gcd

יהיו a, b שלמים חיוביי כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}, \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}$$

از ה- $\gcd(a, b)$ הינו

$$\gcd(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_n, f_n)}.$$

הוכחה: נסמן $.d | b$ ראשית נראה כי $d | a$ וגם $d | b$.

$$\begin{aligned} a &= p_1^{e_1} \dots p_i^{e_i} \dots p_n^{e_n} \\ &= (p_1^{e_1 - \min(e_1, f_1)} \dots p_i^{e_i - \min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}) (p_1^{\min(e_1, f_1)} \dots p_i^{\min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}) \\ &= qd \end{aligned}$$

כאשר $e_i - \min(e_i, f_i) \geq 0$ החזקה $q = p_1^{e_1 - \min(e_1, f_1)} \dots p_i^{e_i - \min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)}$ הוא מספר שלם. אז $.d | a$.

באופן דומה אפשר להוכיח שגם $.d | b$.

הוכחנו כי d הוא מחלק משותף של a ו- b . כעת נראה כי d הוא המחלק המשותף הגדול ביותר.

נניח בsvilleה שקיימים c שלם כך $c | a$ ו- $c | b$ ו- $c > d$. כלומר נניח שקיימים מחלק c של a ושל b שגדול יותר מ- d . מכיוון ש- $c | a$ ו- $c | b$ אז בפירוק לראשוניים של c מופיע רק אותם ראשוניים $\{p_1, \dots, p_n\}$ שמופיעים בפירוקים של a ושל b . לכן יש לנו:

$$c = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n}.$$

מכיוון ש- $c | a$ אז $g_i \leq e_i$ לכל i , ומכיוון ש- $c | b$ אז $g_i \leq f_i$ לכל i . לכן

$$g_i \leq \min(e_i, f_i) \quad \text{לכל } i.$$

לפיכך

$$c = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \leq p_1^{\min(e_1, f_1)} \dots p_i^{\min(e_i, f_i)} \dots p_n^{\min(e_n, f_n)} = d$$

וז"א בסתיו $c > d$.

**דוגמה 1.10**

מצאו את $\gcd(19200, 320)$.

פתרונות:

הפיורוקים הראשונים של 19200 ושל 320 הם

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

לכן

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

דוגמה 1.11

מצאו את $\gcd(154, 36)$

פתרון:

הפיורוקים הראשונים של 154 ושל 36 הם

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

נרשום את 154 ו- 36 כמכפלות של אותם ראשוניים על ידי הוספת חזקות של 0:

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

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

משפט 1.7 \gcd של מספרים ראשוניים

יהיו p, q שני מספרים ראשוניים שונים ($p \neq q$). מתקיים

$$\gcd(p, q) = 1 .$$

הוכחה:

שיטת 1: הוכחה ישירה

p הוא ראשוני אז הפירוק הראשון לשלו הוא

$$p = p^1 q^0 .$$

q הוא ראשוני אז הפירוק הראשון לשלו הוא

$$q = p^0 q^1 .$$

לפי משפט 1.6,

$$\gcd(p, q) = p^{\min(1,0)} q^{\min(0,1)} = p^0 q^0 = 1 .$$

שיטת 2: הוכחה בשילילה

יהי $d = \gcd(p, q)$ ונניח כי $p < q$. אז d נמצא בטוחה של שלמים האפשריים $1 \leq d \leq q$.

נניח בשילילה כי $d > 1$.

.

מכיון ש- d מחלק משותף של p ושל q אז $d \mid p$ וגם $d \mid q$.

זה גורר ל- $d \mid p$ או גם $d \mid q$, בסתיו לכך $d = p$ ראשוני.



משפט 1.8 שיטת פירוק לראשוניים לחישוב lcm

יהיו a, b שלמים חיוביים כך שהפירוק לראשוניים שלהם הם:

$$a = p_1^{e_1} p_2^{e_2} \dots p_n^{e_n}, \quad b = p_1^{f_1} p_2^{f_2} \dots p_n^{f_n}.$$

ה- $\text{lcm}(a, b)$ נתונה על ידי הנוסחה

$$\text{lcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)}$$

הוכחה: נסמן $D = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)}$

$$\begin{aligned} D &= p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_n^{\max(e_n, f_n)} \\ &= (p_1^{\max(e_1, f_1) - e_1} \dots p_i^{\max(e_i, f_i) - e_i} \dots p_n^{\max(e_n, f_n) - e_n}) (p_1^{e_1} \dots p_i^{e_i} \dots p_n^{e_n}) \\ &= qa \end{aligned}$$

כאמור $\max(e_i, f_i) - e_i \geq 0$. החזקה אז $q = p_1^{\max(e_1, f_1) - e_1} \dots p_i^{\max(e_i, f_i) - e_i} \dots p_n^{\max(e_n, f_n) - e_n}$ הוא מספרשלם. אז $a \mid D$.

באופן דומה אפשר להוכיח שגם $b \mid D$.

הוכחנו כי D הוא כפולה של a ושל b .icut נראה כי D הוא הכפולה של a ושל b הקטנה ביותר.

נניח בsvilleה שקיימים C שלם כך $a \mid C$ ו- $b \mid C$ ו- $C < D$. כלומר נניח שקיימים C אשר כפולה של a ושל b שקיימת יותר מ- D . מכיוון ש- $b \mid C$ אז כל הראשוניים בקבוצת $\{p_1, \dots, p_n\}$ אשר בפירוקים של a ושל b חייבים להופיע גם בפירוק לראשוניים של C . לכן יש לנו:

$$C = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \dots$$

מכיוון ש- $e_i \leq g_i$ לכל i , ומכיון ש- $b \mid C$ אז $f_i \leq g_i$ לכל i . לכן

$$\max(e_i, f_i) \leq g_i \quad \text{לכל } i.$$

לפיכך

$$C = p_1^{g_1} \dots p_i^{g_i} \dots p_n^{g_n} \geq p_1^{\max(e_1, f_1)} \dots p_i^{\max(e_i, f_i)} \dots p_n^{\max(e_n, f_n)} = D$$

ז"א $C \geq D$ בסתירה לכך ש-

משפט 1.9

יהיו a, b שלמים חיוביים. אז $\gcd(a, b) \text{lcm}(a, b) = ab$.

הוכחה: יהיו הירוקים לראשוניים של a ושל b :

$$a = p_1^{e_1} \dots p_n^{e_n}, \quad b = p_1^{f_1} \dots p_n^{f_n}.$$

אזי ממפט 1.6 ומממפט 1.8:

$$\begin{aligned} \gcd(a, b) \operatorname{lcm}(a, b) &= p_1^{\min(e_1, f_1)} \cdots p_n^{\min(e_n, f_n)} p_1^{\max(e_1, f_1)} \cdots p_n^{\max(e_n, f_n)} \\ &= p_1^{\min(e_1, f_1) + \max(e_1, f_1)} \cdots p_n^{\min(e_n, f_n) + \max(e_n, f_n)} \\ &= p_1^{e_1+f_1} \cdots p_n^{e_n+f_n} \\ &= p_1^{e_1} \cdots p_n^{e_n} p_1^{f_1} \cdots p_n^{f_n} \\ &= ab, \end{aligned}$$

כasher נעזרנו בהזהות

$$\min(e, f) + \max(e, f) = e + f.$$



1.4 האלגוריתם של אוקלידס

משפט 1.10 האלגוריתם של אוקלידס

יהיו a, b מספרים שלמים חיוביים. קיים אלגוריתם אשר נותן את $d = \gcd(a, b)$ כדלקמן. ראשית מאותחים:

$:r_1 \rightarrow r_0$

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

אם $r_1 \neq 0$ אז מתחילה את הלולאה. בשלב $i = 1$ מחשבים את $q_1 = r_0 / r_1$ ו- $r_2 = r_0 - q_1 r_1$:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor, \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1.$$

אם $r_2 \neq 0$ ממשיכים לשלב $i = 2$ שבו מחשבים את $q_2 = r_1 / r_2$ ו- $r_3 = r_1 - q_2 r_2$:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor, \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2.$$

התהליק ממשיך עד שנקבל $r_{n+1} = 0$ בשלב ה- n -ית. כל השלבים של התהליק הם כדלקמן:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor \quad r_2 = r_0 - q_1 r_1 = r_0 - \left\lfloor \frac{r_0}{r_1} \right\rfloor r_1 \quad :i = 1$$

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor \quad r_3 = r_1 - q_2 r_2 = r_1 - \left\lfloor \frac{r_1}{r_2} \right\rfloor r_2 \quad :i = 2$$

$$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor \quad r_4 = r_2 - q_3 r_3 = r_2 - \left\lfloor \frac{r_2}{r_3} \right\rfloor r_3 \quad :i = 3$$

⋮

$$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor \quad r_n = r_{n-2} - q_{n-1} r_{n-1} = r_{n-2} - \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor r_{n-1} \quad :i = n-1$$

$$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor \quad r_{n+1} = 0 \quad :i = n$$

התהליק מסתיים בשלב ה- n -ית אם $r_{n+1} = 0$. ואז הפלט של האלגוריתם הוא

למטה רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 האלגוריתם של אוקליידס

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $n \leftarrow 1$ 
5: while  $r_n \neq 0$  do
6:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
7:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
8:    $n \leftarrow n + 1$ 
9: end while
10:  $n \leftarrow n - 1$ 
11: Output:  $r_n = \gcd(a, b)$ 
```

דוגמה 1.12מצאו את $\gcd(1071, 462)$ **פתרון:**

$$a = 1071, b = 462$$

נתחל $r_1 = b = 462$ ו $r_0 = a = 1071$ נבצע את האלגוריתם של אוקליידס:

r_i	q_i	שלב
$r_2 = r_0 - q_1 r_1$ $= 1071 - (2)(462) = 147$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{1071}{462} \right\rfloor = 2$: $i = 1$
$r_3 = r_1 - q_2 r_2$ $= 462 - (3)(147) = 21$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{462}{147} \right\rfloor = 3$: $i = 2$
$r_4 = r_2 - q_3 r_3$ $= 147 - (7)(21) = 0$	$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{147}{21} \right\rfloor = 7$: $i = 3$

לפיכך $\gcd(1071, 462) = r_3 = 21$ **דוגמה 1.13**מצאו את $\gcd(26, 11)$ **פתרון:**

$$a = 26, b = 11$$

נתחל $r_1 = b = 11$ ו $r_0 = a = 26$ נבצע את האלגוריתם של אוקליידס:

r_i	q_i	שלב
$r_2 = r_0 - q_1 r_1$ $= 26 - (2)(11) = 4$	$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor = \left\lfloor \frac{26}{11} \right\rfloor = 2$: $i = 1$
$r_3 = r_1 - q_2 r_2$ $= 11 - (2)(4) = 3$	$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor = \left\lfloor \frac{11}{4} \right\rfloor = 2$: $i = 2$
$r_4 = r_2 - q_3 r_3$ $= 4 - (1)(3) = 1$	$q_3 = \left\lfloor \frac{r_2}{r_3} \right\rfloor = \left\lfloor \frac{4}{3} \right\rfloor = 1$: $i = 3$
$r_5 = r_3 - q_4 r_4$ $= 3 - (3)(1) = 0$	$q_4 = \left\lfloor \frac{r_3}{r_4} \right\rfloor = \left\lfloor \frac{3}{1} \right\rfloor = 3$: $i = 5$

לפי כן $\gcd(26, 11) = r_4 = 1$



משפט 1.11 משפט בז' (Bezout's identity)

יהיו a, b . קיימים שלמים s, t, d עבורם

$$sa + tb = d , \quad (1.2)$$

כאשר $d = \gcd(a, b)$.

משפט 1.12 האלגוריתם המוכפל של אוקלידס

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

$$d = sa + tb$$

כאשר $d = \gcd(a, b)$. ראשית מתחילה:

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

אם $0 \neq r_1 = b$ מבצעים האיטרציה הראשונה של הלולאה. בשלב $i = 1$ מחשבים את q_1, r_2, s_2, t_2 כך:

$$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor , \quad r_2 = r_0 - q_1 r_1 , \quad s_2 = s_0 - q_1 s_1 , \quad t_2 = t_0 - q_1 t_1 .$$

אם $0 \neq r_2$ מבצעים לאיטרציה $i = 2$ שבה מחשבים את q_2, r_3, s_3, t_3 כך:

$$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor , \quad r_3 = r_1 - q_2 r_2 , \quad s_3 = s_1 - q_2 s_2 , \quad t_3 = t_1 - q_2 t_2 .$$

התהlik ממשיך עד השלב ה- n שבו מקבלים r_{n+1} , ו- 0 פולטים $d = r_n = \gcd(a, b)$, $s = s_n$, $t = t_n$. כל השלבים של האלגוריתם הם כדלקמן:

$q_1 = \left\lfloor \frac{r_0}{r_1} \right\rfloor$	$r_2 = r_0 - q_1 r_1$	$s_2 = s_0 - q_1 s_1$	$t_2 = t_0 - q_1 t_1$	שלב 1:
$q_2 = \left\lfloor \frac{r_1}{r_2} \right\rfloor$	$r_3 = r_1 - q_2 r_2$	$s_3 = s_1 - q_2 s_2$	$t_3 = t_1 - q_2 t_2$	שלב 2:
				⋮
$q_i = \left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$	$r_{i+1} = t_{i-1} - q_i t_i$	$s_{i+1} = s_{i-1} - q_i s_i$	$t_{i+1} = t_{i-1} - q_i r_i$	שלב i :
				⋮
$q_{n-1} = \left\lfloor \frac{r_{n-2}}{r_{n-1}} \right\rfloor$	$r_n = t_{n-2} - q_{n-1} t_{n-1}$	$s_n = s_{n-2} - q_{n-1} s_{n-1}$	$t_n = t_{n-2} - q_{n-1} r_{n-1}$	שלב $n-1$:
$q_n = \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$	$r_{n+1} = t_{n-1} - q_n t_n$	$s_{n+1} = s_{n-1} - q_n s_n$	$t_{n+1} = t_{n-1} - q_n r_n$	שלב n :

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

אוקלידס של המוכל האלגוריתם 2

```

1: Input: Integers  $a, b$  .
2:  $r_0 \leftarrow a$ 
3:  $r_1 \leftarrow b$ 
4:  $s_0 \leftarrow 1$ 
5:  $s_1 \leftarrow 0$ 
6:  $t_0 \leftarrow 0$ 
7:  $t_1 \leftarrow 1$ 
8:  $n \leftarrow 1$ 
9: while  $r_n \neq 0$  do
10:    $q_n \leftarrow \left\lfloor \frac{r_{n-1}}{r_n} \right\rfloor$ 
11:    $r_{n+1} \leftarrow r_{n-1} - q_n r_n$ 
12:    $s_{n+1} \leftarrow s_{n-1} - q_n s_n$ 
13:    $t_{n+1} \leftarrow t_{n-1} - q_n t_n$ 
14:    $n \leftarrow n + 1$ 
15: end while
16:  $n \leftarrow n - 1$ 
17: Output:  $r_n, s_n, t_n$   $\triangleright d = r_n = \gcd(a, b)$  and  $d = sa + tb$  where  $s = s_n, t = t_n.$ 

```

דוגמה 1.14 (אלגוריתם המוכל של אוקלידס)

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

פתרונות:

מאתחלים:

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

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

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

$$sa + tb = -9(240) + 47(46) = 2 .$$



דוגמה 1.15 (אלגוריתם המוכל של איוקליידס)

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

פתרונות:
מאתחלים:

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

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

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

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

1.5 יחס השקילות המודולרית

הגדרה 1.7 שיקילות מודולרית

יהיו n , a, b שלמים ($0 \neq n$). היחס:

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

אומר כי " n מחלק את ההפרש $a - b$ ".
כלומר:

$$a \equiv b \pmod{n} \quad \text{אם ורק אם} \quad n \mid a - b .$$

דוגמה 1.16

הוכחו כי

$$5 \equiv 2 \pmod{3} \quad \text{(א)}$$

$$43 \equiv 23 \pmod{10} \quad \text{(ב)}$$

$$7 \not\equiv 2 \pmod{4} \quad \text{(ג)}$$

פתרונות:

(א)

$$5 - 2 = 3 = 1 \cdot 3 \quad \Rightarrow \quad 3 \mid 5 - 2 \quad \Rightarrow \quad 5 \equiv 2 \pmod{3} .$$

(ב)

$$43 - 23 = 20 = 2 \cdot 10 \quad \Rightarrow \quad 10 \mid 43 - 23 \quad \Rightarrow \quad 43 \equiv 23 \pmod{10} .$$

$$(ג) 7 - 2 = 5$$

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

$$7 \not\equiv 2 \pmod{4} .$$

ההגדרה 1.7 של שיקילות מודולרית בין שלמים גוררת למשפט הבא באופן טבעי:

משפט 1.13

יהיו a, b, r שלמים, $r \neq 0$.

$$a = qr + b \quad \text{קיים שלם } q \text{ עבורו} \quad \text{אם ורק אם} \quad n \mid a - b \quad \text{אם ורק אם} \quad a \equiv b \pmod{n}$$

הוכחה:

הגרירה הראשונה r נובעת יש מההגדרה 1.7 של יחס שקולות.

נראה את הגרירה השנייה:

$$a = qn + b \iff a - b = qn \text{ עבור } q \mid a - b$$

משפט 1.14 תכונות של יחס השקילות המודולרי

יהיו a, b שלמים ו- $0 \neq n$ שלם.

(1) רפלקסיבי:

$.b \equiv a \pmod{n}$ אם ורק אם $a \equiv b \pmod{n}$

(2) סימטרי: אם $a \equiv c \pmod{n}$ אז $b \equiv c \pmod{n}$ אז $a \equiv b \pmod{n}$

(3) טרנזיטיבי: אם $a \equiv b \pmod{n}$ ו- $b \equiv c \pmod{n}$ אז $a \equiv c \pmod{n}$

הוכחה:

(1) רפלקסיבי:

$.a \equiv a \pmod{n}$ מתקיים $a = 0 \cdot n + a$, כלומר $a \mid a - a$, לכן $n \mid a - a$.

(2) סימטרי:

נניח ש- $a \equiv b \pmod{n}$. אז קיימים שלמים q עבורו

$$a = qn + b \iff b = (-q)n + a .$$

זה אומר קיימים שלמים $\bar{q} = -q$ עבורו $b = \bar{q}n + a$, כלומר $a \equiv b \pmod{n}$.

(3) טרנזיטיבי: נניח ש- $a \equiv b \pmod{n}$ ו- $b \equiv c \pmod{n}$

$$\begin{array}{l} a = qn + b \\ b = \bar{q}n + c \end{array} \Rightarrow a = qn + \bar{q}n + c = (b + \bar{q})n + c$$

זה אומר קיימים שלמים $Q = q + \bar{q}$ עבורו $a = Qn + c$, כלומר $a \equiv c \pmod{n}$.

משפט 1.15 הקשר בין יחס השקילות מודולרי והשארית

יהיו $a, b, n > 0$ שלמים.

$$a \equiv b \pmod{n} \iff a \bmod n = b \bmod n$$

הוכחה:

כיוון \Leftarrow

נניח ש- $a \equiv b \pmod{n}$. אז קיימים שלם Q כך ש:

$$a = qn + b.$$

לפי משפט החלוקת של אוקלידס,

$$b = \bar{q}n = r_1, \quad r_1 = b \pmod{n}.$$

לכן

$$a = (q + \bar{q})n + r_1 = Qn + r_1$$

כאשר \bar{q} שלם ו- $r_1 = b \pmod{n}$ הוא השארית n . מכאן נובע ש:

$$a \pmod{n} = a - n \left\lfloor \frac{a}{n} \right\rfloor = Qn + r_1 - Qn = r_1$$

$$a \pmod{n} = r_1 = \pmod{n} \text{ נ"א}$$

כיוון \Rightarrow

נניח ש- $a \pmod{n} = b \pmod{n}$. אז

$$a - n \left\lfloor \frac{a}{n} \right\rfloor = b - n \left\lfloor \frac{b}{n} \right\rfloor \Rightarrow a = \left(\left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor \right) n + b \Rightarrow a = qn + b$$

כלומר קיימים שלם $q = \left\lfloor \frac{a}{n} \right\rfloor - \left\lfloor \frac{b}{n} \right\rfloor$ עבורו $a = qn + b$ ו- $a \equiv b \pmod{n}$.

משפט 1.16 חיבור וכפל של שלמים השקולים מודולריים

יהיו a, b, c, d שלמים ו- $0 \neq n$ שלם.

(1) חיבור:

אם $a \equiv b \pmod{n}$ ו- $c \equiv d \pmod{n}$ אז $a + c \equiv b + d \pmod{n}$ וכן $a \equiv b \pmod{n}$

(2) כפל:

אם $a \equiv b \pmod{n}$ ו- $c \equiv d \pmod{n}$ אז $ac \equiv bd \pmod{n}$ וכן $a \equiv b \pmod{n}$

הוכחה:

(1) חיבוריות:

אם $a \equiv b \pmod{n}$ אז קיימים שלם q עבורו $a = qn + b$ וכן אם $c \equiv d \pmod{n}$ אז קיימים שלם q עבורו $c = \bar{q}n + d$.

$$a + c = (q + \bar{q})n + b + d \Rightarrow a + c = Qn + (b + d),$$

כאשר $Q = q + \bar{q}$. הוכחנו שקיימים שלם Q עבורו $a + c \equiv b + d \pmod{n}$.

(2) כפל:

אם $a \equiv b \pmod{n}$ אז קיימים שלם q עבורו $a = qn + b$ וכן אם $c \equiv d \pmod{n}$ אז קיימים שלם q עבורו $c = \bar{q}n + d$.

$$ac = (qn + b)(\bar{q}n + d) \Rightarrow ac = (q\bar{q}n^2 + dq + b\bar{q}n + bd) \Rightarrow ac = Qn + bd,$$

כאשר $Q = (q\bar{q} + dq + b\bar{q})$. הוכחנו שקיימים שלם Q עבורו $ac \equiv bd \pmod{n}$.