שיעור 1
תורת המספרים

1.1 משפט החילוק של אוקלידס

הגדרה 1.1 מספר שלם שמחלק מספר שלם אחר

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 $b \mid a$ אומר כי "b מחלק את a".

דוגמה 1.1

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

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

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

משפט 1.1 תכונות של חילוק שלמים

יהיו a,b,d שלמים.

1) אם $d \mid a$ ו- $d \mid b$ אזי $d \mid (a+b)$.

2) יהיו x,y שלמים. אם $d \mid a$ ו- $d \mid b$ אזי $d \mid (xa+yb)$.

3) אם $b \mid a$ ו- $a \mid b$ אזי $a=\pm b$.

הוכחה:

1)

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

2)

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

3)

$$\left.\begin{array}{lll} a|b & \Rightarrow & b=ca \\ b|a & \Rightarrow & a=c'b \end{array}\right\} \quad \Rightarrow \quad b=ca=cc'b \quad \Rightarrow \quad cc'=1\ .$$

c ו- c' הם שלמים לכן $cc'=1$ אם ורק אם $c=1=c'$ או $c=-1=c'$. לפיכך

$$b=\pm a \ .$$

■

הגדרה 1.2 השארית

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

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

סימון חלופי לשארית בחלוקה a ב- b: $a \,\%\, b$.

הערה: השאירת מוגדרת באופן חד משמעי עובר שלמים חיוביים בלבד!

דוגמה 1.2

$$\begin{aligned}
43 \bmod 10 &= 43 - 10\cdot\left\lfloor \frac{43}{10} \right\rfloor &&= 43-10(4) &&= 3 \ ,\\
13 \bmod 4 &= 13 - 4\cdot\left\lfloor \frac{13}{4} \right\rfloor &&= 13-4(3) &&= 1 \ ,\\
8 \bmod 2 &= 8 - 2\cdot\left\lfloor \frac{8}{2} \right\rfloor &&= 8-2(4) &&= 0 \ .
\end{aligned}$$

משפט 1.2 משפט החילוק של אוקלידס

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

$$a = qb + r \tag{1.1}$$

כאשר $0\leq r<|b|$. השלם q נקרא **המנה** של a בחלוקה ב- b ו- r נקרא **השארית** של a בחלוקה ב- b.
המשוואה (1.1) נקרא ה**פירוק מנה-שארית** של השלמים a ו- b.

ההוכחה עצמה היא לא חלק של הקורס.

דוגמה 1.3

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

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

דוגמה 1.4

יהיו $a=-46$, $b=8$. המנה והשארית הם $q=-6$, $r=2$ והפירוק מהנ-שארית הוא

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

משפט 1.3 שיטה מעשית לחישוב הפירוק מנה-שארית

יהיו a,b שלמים (עם $b\neq 0$). אזי המנה q והשארית r במשפט החילוק של אוקלידס ניתנים כך:

(1 אם $a>0,b>0$ אז $q=\left\lfloor\frac{a}{b}\right\rfloor$ ו- $r=a \bmod b$.

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

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

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

הוכחה: נוכיח בכל אחד מארבעת המקרים.

מצב 1) נניח $a>0,b>0$. לפי משפט החילוק של אוקלידס קיימים שלמים r , q כך ש-

$$a=qb+r,\qquad 0\leq r<b. \tag{*}$$

נחלק ב-b:

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

מכיוון ש-$0\leq r<b$, מתקיים $0\leq\frac{r}{b}<1$, ולכן

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

הצבה חזרה ב-(*) נותנת

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

מצב 2) נניח $a>0,b<0$. לפי משפט החילוק של אוקלידס עבור הלשמים $|b|$, a קיימים שלמים $\bar{r}$, $\bar{q}$ כך ש:

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

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

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

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

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

השוואה של משוואה (#) ל-$a=qb+r$ נותנת

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

מצב 3) נניח $a<0, b>0$. ממשפט החילוק עבור הלשמים b , $|a|$ קיימים שלמים $\bar{r}$, $\bar{q}$ כך ש:

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

מהמקרה הראשון:

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

נציב $|a| = -a$:

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

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

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

כך קיבלנו את הצורה הנדרשת. מצד שני עבור השלמים b , a (כלומר a בלי הערך מוחלט) ממשפט החילוק קיימים שלמים q, r עבורם

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

השוואה של זה עם משוואה (**) נותנת:

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

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

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

מ-(1) נקבל

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

נציב $|a| = -a, |b| = -b$:

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

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

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

מצד שני ממשפט החילוק עבור השלמים b , a (לא הערכים מוחלטים שלהם) קיימים שלמים q, r עבורם:

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

השוואה של $a = qb + r$ למשוואה (##) נותנת:

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

לסיכום, מתקבלת הטבלה הבאה:

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	$-$	$-$	$\left\lfloor \frac{\lvert a\rvert}{\lvert b\rvert} \right\rfloor + 1$	$\lvert b\rvert - \lvert a\rvert \bmod \lvert b\rvert$

■

דוגמה 1.5

מצאו את הפירוק מנה-שארית של השלמים הבאים:

א) $a = 46\,,\ b = 8$.

ב) $a = -46\,,\ b = 8$.

ג) $a = 101\,,\ b = -7$.

ד) $a = -151\,,\ b = -12$.

פתרון:

א) במקרה זה $a > 0\,,\ b > 0$ אז

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

לכן:

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

ב) במקרה זה $a < 0\,,\ b > 0$ אז

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

ו-

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

לכן:

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

ג) במקרה זה $a>0\,,\,b<0$ אז

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

ו-

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

לכן:

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

ד) במקרה זה $a<0\,,\,b<0$ אז

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

ו-

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

לכן:

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

■

1.2 מספרים ראשוניים

הגדרה 1.3 מספר ראשוני

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

$$a\mid p\qquad\Longleftrightarrow\qquad a=1\vee p\ .$$

משפט 1.4 משפט הפירוק לראשוניים

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 $e_1,\ldots,e_n$ עבורם

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

כאשר $p_1,\ldots,p_n$ 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. אזי קיים לפחות מספר טבעי אחד שלא ראשוני וגם לא שווה למכפלה של ראשוניים.
- יהי $m \geq 2$ הטבעי הקטן ביותר שלא מקיים הטענה זו. (m הוא הדוגמה הנגדית הקטנה ביותר.)
- אזי m לא ראשוניי וגם לא שווה למכפלת ראשוניים.
- לכן m פריק, ז"א קיימים טבעיים $2 \leq a < m, \ 2 \leq b < m$ כך ש:
$$m = ab \ .$$
- m הוא הטבעי הקטן ביותר מסוג זה שמפריך את הטענה בעוד a, b הם קטנים ממש מ- m אז a ו- b בהכרח מקיימים את הטענה: ז"א a הוא או ראשוני או שווה למכפלת ראשוניים, ואותו דבר עבור b.
- לכן קיימים טבעיים $e_1, \ldots, e_n$ עבורם
$$a = p_1^{e_1} \ p_2^{e_2} \ \ldots \ p_n^{e_n}$$
כאשר $p_1, \ldots, p_n$ מספרים ראשוניים וקיימים טבעיים $f_1, \ldots, f_n$ עבורם
$$b = q_1^{f_1} \ q_2^{f_2} \ \ldots \ q_n^{f_n}$$
כאשר $q_1, \ldots, q_n$ מספרים ראשוניים.
- מכאן
$$m = ab = p_1^{e_1} \ p_2^{e_2} \ \ldots \ p_n^{e_n} \ q_1^{f_1} \ q_2^{f_2} \ \ldots \ q_n^{f_n} \ .$$
לכן m שווה למכפלה של מספרים ראשוניים, בסתירה לכך ש- m לא שווה למכפלה של ראשוניים!

$\blacksquare$

משפט 1.5 קיימים אינסוף מספרים ראשוניים

קיימים אינסוף מספרים ראשוניים.

הוכחה: נוכיח את הטענה דרך השלילה.
נניח כי $P = \{p_1, \ldots, p_n\}$ הוא הקבוצה של כל הראשוניים שקיימים וקבוצה זו נוצרת סופי.
נגדיר השלם $m = p_1 p_2 \ldots p_n + 1$.
לפי משפט הפירוק לראשוניים (ראו משפט 1.4) m הוא ראשוני או שווה למכפלה של ראשוניים.
לפי ההנחה ההתחלתית שלנו, אין מצב ש- m יכול להיות מספר ראשוני בגלל ש- m גדול ממש מכל הראשוניים בקבוצת כל ראשוניים P. כלומר, $m > p_i$ לכל $1 \leq i \leq n$.
גם לא קיים מספק ראשוני p_i אשר מחלק את m. הרי

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

הגענו לסתירה להמשפט הפירוק לראשוניים. לכן קיימים אינסוף מספרים ראשוניים. $\blacksquare$

1.3 המחלק המשותף הגדול ביותר

הגדרה 1.4 המחלק המשותף הגדול ביותר (gcd).

יהיו a, b שלמים. המחלק המשותף הגדול ביותר של a ו- b מסומן $\gcd(a, b)$ ומוגדר להיות השלם החיובי הגדול ביותר שמחלק גם a וגם b.

הסימון gcd מנובע מהשם אנגלית "greatest common divisor".

דוגמה 1.8

$$\begin{aligned} \gcd(2,6) &= 2 \ , \\ \gcd(3,6) &= 3 \ , \\ \gcd(24,5) &= 1 \ , \\ \gcd(20,10) &= 10 \ , \\ \gcd(14,12) &= 2 \ , \\ \gcd(8,12) &= 4 \ . \end{aligned}$$

הגדרה 1.5 כפולה המשותפת הקטנה ביותר

יהיו a, b שלמים. הכפולה המשותפת הקטנה ביותר מסומנת $\operatorname{lcm}(a, b)$ ומוגדרת להיות השלם החיובי החיובי הקטן ביותר עבורו גם a וגם b מחלקים אותו.

הסימון lcm מנובע מהשם אנגלית "lowest common multiple".

דוגמה 1.9

$$\begin{aligned} \operatorname{lcm}(6,21) &= 42 \ , \\ \operatorname{lcm}(3,6) &= 6 \ , \\ \operatorname{lcm}(24,5) &= 120 \ , \\ \operatorname{lcm}(20,10) &= 20 \ , \\ \operatorname{lcm}(14,12) &= 84 \ , \\ \operatorname{lcm}(8,12) &= 24 \ . \end{aligned}$$

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 לראשוניים לחישוב gcd

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

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

אז 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 $d = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \dots {p_n}^{\min(e_n,f_n)}$. ראשית נראה כי $a \mid d$ וגם $b \mid d$.

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

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

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

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

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

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

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

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

לפיכך

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

ז"א $d \leq c$ בסתירה לכך ש- $d > c$. ■

דוגמה 1.10

מצאו את $\gcd(19200, 320)$.

פתרון:

הפירוקים לראשוניים של 19200 ושל 320 הם

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

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:
הפירוקים לראשוניים של 154 ושל 36 הם

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

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

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

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

■

משפט 1.7 gcd של מספרים ראשוניים

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

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

הוכחה:

<u>שיטה 1: הוכחה ישרה</u>

p הוא ראשוני אז הפירוק לראשונים שלו הוא
$$p = p^1 q^0 \ .$$
q הוא ראשוני אז הפירוק לראשונים שלו הוא
$$q = p^0 q^1 \ .$$
לפי משפט 1.6,
$$\gcd(p,q) = p^{\min(1,0)} q^{\min(0,1)} = p^0 q^0 = 1 \ .$$

<u>שיטה 2: הוכחה בשלילה</u>

יהי $d=\gcd(p,q)$ ונניח כי $q<p$. אז d נמצא בטווח של שלמים האפשריים $1\leq d\leq q$.
נניח בשלילה כי $d>1$.
מכיוון ש- d מחלק משותף של p ושל q אז $d\mid p$ וגם $d\mid q$.
q הוא ראשוני אז $d\mid q$ רק אם $q=d$. לכן אם גם $d\mid p$ אז זה גורר ל- $p\mid q$, בסתירה לכך ש- p ראשוני. ■

משפט 1.8 שיטת פירוק לראשוניים לחישוב lcm

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

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

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

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

הוכחה: נסמן $D = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \ldots {p_n}^{\max(e_n,f_n)}$. ראשית נראה כי $D \mid a$ וגם $D \mid b$.

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

כאשר $q = p_1^{\max(e_1,f_1)-e_1} \ldots p_i^{\max(e_i,f_i)-e_i} \ldots p_n^{\max(e_n,f_n)-e_n}$. החזקה $\max(e_i,f_i) - e_i \geq 0$ אז q הוא מספר שלם. אזי $D \mid a$.

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

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

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

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

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

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

לפיכך

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

ז"א $C \geq D$ בסתירה לכך ש- $D < C$. ■

משפט 1.9

יהיו a,b שלמים חיוביים. אזי

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

הוכחה: יהיו הירוקים לראשוניים של a ושל b:

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

אזי ממשפט 1.6 וממשפט 1.8:

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

כאשר 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 מאתחלים r_0 ו- r_1:

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

אם $r_1=b\neq 0$ אז מתחילים את הלולאה. בשלב $i=1$ מחשבים את q_1 ו- r_2 כך:

$$q_1=\left\lfloor\frac{r_0}{r_1}\right\rfloor\ ,\qquad r_2=r_0-q_1r_1=r_0-\left\lfloor\frac{r_0}{r_1}\right\rfloor\ .$$

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

$$q_2=\left\lfloor\frac{r_1}{r_2}\right\rfloor\ ,\qquad r_3=r_1-q_2r_2=r_1-\left\lfloor\frac{r_1}{r_2}\right\rfloor\ .$$

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

שלב $i=1$: $$q_1=\left\lfloor\frac{r_0}{r_1}\right\rfloor\qquad r_2=r_0-q_1r_1=r_0-\left\lfloor\frac{r_0}{r_1}\right\rfloor r_1$$

שלב $i=2$: $$q_2=\left\lfloor\frac{r_1}{r_2}\right\rfloor\qquad r_3=r_1-q_2r_2=r_1-\left\lfloor\frac{r_1}{r_2}\right\rfloor r_2$$

שלב $i=3$: $$q_3=\left\lfloor\frac{r_2}{r_3}\right\rfloor\qquad r_4=r_2-q_3r_3=r_2-\left\lfloor\frac{r_2}{r_3}\right\rfloor r_3$$

$\vdots$

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

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

התהליך מסתיים בשלב ה-n-ית אם $r_{n+1}=0$. ואז הפלט של האלגוריתם הוא $r_n=\gcd(a,b)$.

למטה רשום ייצוג פסאודו-קוד של האלגוריתם של אוקלידס:

Algorithm 1 האלגוריתם של אוקלידס

```
Input: Integers a, b .
r_0 ← a
r_1 ← b
n ← 1
while r_n ≠ 0 do
    q_n ← ⌊ r_{n-1} / r_n ⌋
    r_{n+1} ← r_{n-1} − q_n r_n
    n ← n + 1
end while
n ← n − 1
Output: r_n = gcd(a, b)
```

דוגמה 1.12

מצאו את ה- $\gcd(1071, 462)$.

פתרון:

$a = 1071, b = 462$.

נאתחל $r_0 = a = 1071$ ו- $r_1 = b = 462$ נבצע את האלגוריתם של אוקלידס:

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

לפיכך $\gcd(1071, 462) = r_3 = 21$.

■

דוגמה 1.13

מצאו את $\gcd(26, 11)$.

פתרון:

$a = 26, b = 11$.

נאתחל $r_0 = a = 26$ ו- $r_1 = b = 11$ נבצע את האלגוריתם של אוקלידס:

שלב	q_i	r_i
$i=1$:	$q_1=\left\lfloor \frac{r_0}{r_1}\right\rfloor = \left\lfloor \frac{26}{11}\right\rfloor =2$	$r_2 = r_0-q_1r_1 = 26-(2)(11)=4$
$i=2$:	$q_2=\left\lfloor \frac{r_1}{r_2}\right\rfloor = \left\lfloor \frac{11}{4}\right\rfloor =2$	$r_3 = r_1-q_2r_2 = 11-(2)(4)=3$
$i=3$:	$q_3=\left\lfloor \frac{r_2}{r_3}\right\rfloor = \left\lfloor \frac{4}{3}\right\rfloor =1$	$r_4 = r_2-q_3r_3 = 4-(1)(3)=1$
$i=5$:	$q_4=\left\lfloor \frac{r_3}{r_4}\right\rfloor = \left\lfloor \frac{3}{1}\right\rfloor =3$	$r_5 = r_3-q_4r_4 = 3-(3)(1)=0$

לפיכך $\gcd(26,11)=r_4=1$.

■

משפט 1.11 משפט בזו (Bezout's identity)

יהיו a,b. קיימים שלמים s,t,d עבור

$$sa+tb=d\ , \tag{1.2}$$

כאשר $d=\gcd(a,b)$. משוואה (1.2) נראת ה**פירוק אוקלידס** של a ו- b.

משפט 1.12 האלגוריתם המוכלל של אוקלידס

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

$$d=sa+tb$$

כאשר $d=\gcd(a,b)$, כדלקמן. ראשית מאתחלים:

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

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

$$q_1=\left\lfloor \frac{r_0}{r_1}\right\rfloor\ ,\quad r_2=r_0-q_1r_1\ ,\quad s_2=s_0-q_1s_1\ ,\quad t_2=t_0-q_1t_1\ .$$

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

$$q_2=\left\lfloor \frac{r_1}{r_2}\right\rfloor\ ,\quad r_3=r_1-q_2r_2\ ,\quad s_3=s_1-q_2s_2\ ,\quad t_3=t_1-q_2t_2\ .$$

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

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

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

למטה רשום ייצוג פסאודו-קוד של האלגוריתם:

Algorithm 2 אוקלידס של המוכלל האלגוריתם

```
Input: Integers a, b .
r_0 ← a
r_1 ← b
s_0 ← 1
s_1 ← 0
t_0 ← 0
t_1 ← 1
n ← 1
while r_n ≠ 0 do
    q_n ← ⌊ r_{n-1} / r_n ⌋
    r_{n+1} ← r_{n-1} − q_n r_n
    s_{n+1} ← s_{n-1} − q_n s_n
    t_{n+1} ← t_{n-1} − q_n t_n
    n ← n + 1
end while
n ← n − 1
Output: r_n, s_n, t_n        ▷ d = r_n = gcd(a, b) and d = sa + tb where s = s_n, t = t_n.
```

דוגמה 1.14 (אלגוריתם המוכלל של איוקלידס)

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

פתרון:

מאתחלים:

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

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

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

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

■

דוגמה 1.15 (אלגוריתם המוכלל של איוקלידס)

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

פתרון:

מאתחלים:

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

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

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

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

■

1.5 יחס השקילות המודולרית

הגדרה 1.7 שקילות מודולרית

יהיו a,b,n שלמים ($n\neq 0$). היחס:

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

אומר כי "n מחלק את ההפרש $a-b$".

כלומר:

$$a\equiv b \pmod{n} \qquad \text{אם ורק אם} \qquad n\,|\,a-b\ .$$

דוגמה 1.16

הוכיחו כי

א) $5\equiv 2 \pmod{3}$

ב) $43\equiv 23 \pmod{10}$

ג) $7\not\equiv 2 \pmod{4}$

פתרון:

א)

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

ב)

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

ג) $7-2=5$.

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

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

■

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

משפט 1.13

יהיו a,b,r שלמים, $b\neq 0$.

$a\equiv b \pmod{n}$ אם ורק אם $n\,|\,a-b$ אם ורק אם קיים שלם q עבורו $a=qn+b$.

הוכחה:
הגרירה הראשונה $b \mid a-r \Leftrightarrow a \equiv r \pmod{b}$ נובעת ישר מההגדרה 1.7 של יחס שקילות.
נראה את הגרירה השנייה:
$n \mid a-b$ אם ורק אם קיים שלם q עבורו $a-b=qn \quad \Longleftrightarrow \quad a=qn+b$.

■

משפט 1.14 תכונות של יחס השקילות המודולרית

יהיו a,b שלמים ו- $n \neq 0$ שלם.

1) רפלקסיבי: $a \equiv a \pmod{n}$.

2) סימטרי: $a \equiv b \pmod{n}$ אם ורק אם $b \equiv a \pmod{n}$.

3) טרנזיטיבי: אם $a \equiv b \pmod{n}$ וכן $b \equiv c \pmod{n}$ אזי $a \equiv c \pmod{n}$.

הוכחה:

1) רפלקסיבי:

לכל שלם $n \neq 0$ מתקיים $n \mid a-a$, או במילים אחרות $a = 0 \cdot n + a$, לכן $a \equiv a \pmod{n}$.

2) סימטרי:

נניח ש- $a \equiv b \pmod{n}$. אזי קיים שלם q עבורו

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

ז"א קיים שלם $\bar{q}=-q$ עבורו $b=\bar{q}n+a$ לכן $b \equiv a \pmod{n}$.

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

$$\left.\begin{aligned} a &= qn+b \\ b &= \bar{q}n+c \end{aligned}\right\} \quad \Rightarrow \quad a=qn+\bar{q}n+c=(b+\bar{q})n+c$$

ז"א קיים שלם $Q=q+\bar{q}$ עבורו $a=Qn+c$ לכן $a \equiv c \pmod{n}$.

■

משפט 1.15 הקשר בין יחס שקילות מודולרית והשארית

יהיו $a,b,n>0$ שלמים.

$$a \equiv b \pmod{n} \quad \Longleftrightarrow \quad a \bmod n = b \bmod n$$

הוכחה:
כיוון $\Leftarrow$

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

$$a = qn + b \ .$$

לפי משפט החילוק של אוקלידס,

$$b = \bar{q}n = r_1 \ , \qquad r_1 = b \bmod n \ .$$

לכן

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

כאשר $Q = q + \bar{q}$ שלם ו- $0 \leq r_1 < b$ הוא השארית $r_1 = b \bmod n$. מכאן נובע ש:

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

ז"א $a \bmod n = r_1 = \bmod n$.

<u>כיוון $\Rightarrow$</u>

נניח ש- $a \bmod n = b \bmod n$. אזי

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

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

משפט 1.16 חיבור וכפל של שלמים השקולים מודולריים

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

1) <u>חיבור:</u>

אם $a \equiv b \pmod{n}$ וכן $c \equiv d \pmod{n}$ אזי $a + c \equiv b + d \pmod{n}$.

2) <u>כפל:</u>

אם $a \equiv b \pmod{n}$ וכן $c \equiv d \pmod{n}$ אזי $ac \equiv bd \pmod{n}$.

הוכחה:

1) <u>חיבוריות:</u>

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

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

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

2) <u>כפל:</u>

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

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

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