תזכורת מההרצאה הקודמת:

$gcd(a,b)$ = המחלק המשותף המרבי של a,b. $(18,12)=6$

משפט בזו:

$$(a,b) \in \mathcal{L}(a,b)$$

(a,b) ← הממ"מ של a,b

$\mathcal{L}(a,b)$ ← אוסף הלינארים בלינארים של a,b

בלומר האוסף $\{ma+nb \mid m,n \in \mathbb{Z}\}$

בלומר: אפשר להציג את (a,b) כצירוף לינארי של a,b.

שתי מסקנות חשובות מהוכחת משפט בזו:

1. (a,b) הוא הצירוף הלינארי המינימלי של a,b שיוצא חיובי.
2. כל מחלק משותף של a,b מחלק את (a,b).

בשני המימושים הבאים מצורף קוד "פנינה רוחנית" של תרגילים בסיסיים על משפט החילוק והם gcd, שדאי לנסות לפתור ולעיין לפתרונות המוצעים לפני שניגשים לפתרון המטלה.
(תזכרה לאלוף חורה שהכין את הקוד בסמסטר א').

פינות "קטנות"

לא פעם הדברים "הקטנים" שאנו לכאורה יודעים, הם בעוכרינו.
דף התרגילים הנוכחי הינו מקבץ של "תרגילים קטנים" פתורים (לא להגשה) לתירגול נוסף.

תרגיל 1

יהיו $a,b,c,m,n \in \mathbb{Z}$. הוכיחו כי אם $a \mid b$ וגם $a \mid c$ אזי $a \mid mb+nc$.

<u>פתרון:</u>

היות ולפי הנחה $a \mid b$ וגם $a \mid c$ נוכל לרשום $c = k \cdot a$ וגם $b = \ell \cdot a$ עבור $k,\ell \in \mathbb{Z}$ כלשהם. אזי

$$mb + nc = m\ell a + nka = a(m\ell + nk)$$

ולכן $a \mid mb+nc$.

תרגיל 2:

יהיו $a,b \in \mathbb{Z}$. הוכיחו כי $a \mid b$ אם"ם (אם ורק אם) $a \mid -b$.

<u>פתרון:</u>

נניח כי $a \mid b$, ואם כך, נוכל לרשום כי $b = k \cdot a$ עבור $k \in \mathbb{Z}$ כלשהו. נובע אם כן כי $-b = -ka$ ואזי $a \mid -b$.
נניח כי $a \mid -b$ ואזי נוכל לרשום $-b = k \cdot a$ עבור $k \in \mathbb{Z}$ כלשהו. אם כך, מתקיים $b = -(-b) = (-k)a$ ואזי נובע ש $a \mid b$.

תרגיל 3

הוכיחו כי אם $a \mid b$ וגם $a \mid c$, אזי $a \mid b \pm c$.

<u>פתרון:</u>

לפי ההנחה נוכל לרשום $b = ka$ ו $c = \ell a$ עבור $k,\ell \in \mathbb{Z}$ כלשהם. אזי מתקיים

$$b \pm c = ka \pm \ell a = (k \pm \ell)a$$

והטענה נובעת.

תרגיל 4

הוכיחו כי אם $a \mid b$ וגם $c \mid d$ אזי $ac \mid bd$.

<u>פתרון:</u>

לפי ההנחה נוכל לרשום כי $b = ka, d = \ell c$ עבור $k, \ell \in \mathbb{Z}$ כלשהם. אם כך,

$$bd = ka \cdot \ell c = (ac)(k\ell)$$

והטענה נובעת.

שני התרגילים הבאים עוסקים במשפט Bézout. להלן אחד הניסוחים של משפט זה כפי שזה סופק בהרצאות.

משפט Bézout: יהיו $a, b \in \mathbb{Z}$. אזי (a, b) הינו האיבר המינימלי בקבוצה $\mathscr{L}(a, b) \cap \mathbb{N}$.

נזכיר כי הקבוצה $\mathscr{L}(a, b)$ הוגדרה להיות קבוצת הקומבינציות הלינאריות של a, b. דהיינו,

$$\mathscr{L}(a, b) := \{ma + nb : m, n \in \mathbb{Z}\}$$

אנו מתמקדים בניסוח זה של משפט Bézout, שכן הוא מגלם בתוכו דרך יחסית פשוטה שבאמצעותה אנו יכולים להוכיח זרות של שני מספרים נתונים. התרגיל הבא ממחיש נקודה זו. בפרט, המסר של משפט זה בניסוח הנתון לגבי זרות הינו שעלינו לנסות להביע את 1 כקומבינציה לינארית של שני המספרים הנתונים. במקרה של הצלחה תהיה בידינו הוכחה ששני המספרים זרים, כאמור תוך כדי הפנייה למשפט Bézout כפי שזה מנוסח לעיל.

תרגיל 5

יהי $n \in \mathbb{N}$. הוכיחו כי $(n, (n-1)(n+1)) = 1$.

<u>פתרון:</u>

היות ו $(n-1)(n+1) = n^2 - 1$ נוכל לרשום כי $1 = n \cdot n + (-1)(n^2 - 1)$ ואזי הטענה נובעת ממשפט Bézout.

יש שני נבדים מתוך הבנה שחשוב שנעבור אותה גם באופן לשוני:

משהו מתוך ההבנה שחשוב שתעבור "באמצע הלילה": (a,b) הנו הגדול הגיעי החיובי המינימלי של a ו-b.

בדוגמה שהגדל מה יוצא חיובי ולא שהקבועים חיוביים.

מהשורה האחרונה של ההגדרה

מסקנה: "כל מחלק משותף של a ו-b, מחלק את המא"מ (a,b)"
(לאור שהמא"מ הוא גדול יותר מכל מחלק משותף אחר, אלא גם שגבו כבוה של כל מחלק משותף אחר)

משפט (בהגדרה אלטרנטיבית) $\{(a,b)-\}$ כל מחלק משותף אחר אם מחלק גם אותו. (בגלל שבעצם קיבלנו הה לנו: "יש לא שוה מחלק.") שגבו לשמש גם מחלק את a ואת b

יהיו $a,b\in\mathbb{Z}$ לא שניהם 0.
$d=(a,b)$ אזי:
1. $d|a$ וגם $d|b$.
2. לכל c שגם קיים $c|a$ וגם $c|b$ מתקיים $c|d$.

הסבר (לא נכתב הוכחה פורמלית): אם $d=(a,b)$ לפי ההגדרה הקודמת אז 1 מתקיים אוטומטית והרעיון במסקנה בעמוד שגיבא של מחלק משותף c מחלק גם את d.
מצד שני, אם d מקיים את דרישת המשפט שלנו אז אוטומטית לכל מחלק משותף c מתקיים $c|d$ ומאחר $c\le d$ כמו בהגדרה המקורית.

דרך אחרת לומר את אותו הסבר: תנאי 1 נבדק בשתי ההגדרות. 2 בקודמת $\Leftarrow$ 2 בחדשה.
לפי המסקנה, (אולם) 2 בחדשה $\Leftarrow$ 2 בקודמת כי אם $c|d$ אז $c\le d$.

משפט המשפט הבא הוא מעין מבקר מפגש - "אוסף הצירופים הלינאריים של a,b הם בדיוק אוסף הכפולות של (a,b)" $L(a,b)=\{k\cdot(a,b)\mid k\in\mathbb{Z}\}$

דוגמה בלבד: $(18,12)=6$

$L(18,12)=\{18a+12b \mid a,b\in\mathbb{Z}\}=\{0,18,36,6,\ldots\}$ כלומר כפולות 6
$a=0,b=0$; $a=1,b=0$; $a=1,b=1$; $a=1,b=-1$

הוכחה כדי להראות שוויון בין קבוצות אנחנו נתייחס הכלה דו-כיוונית.
1. נראה $L(a,b)\subset\{k\cdot(a,b)\mid k\in\mathbb{Z}\}$: (לקחים איבר באיזשהו ונראים שהוא גם כולל ימין)
יש $ma+nb\in L(a,b)$ $(m,n\in\mathbb{Z})$. (בגלל הגדרה שהוא מהצורה $k\cdot(a,b)$)

$a|(a,b) \Leftarrow a=k_1\cdot(a,b)$
$(a,b)|b \Leftarrow b=k_2\cdot(a,b)$
$ma+nb=mk_1(a,b)+nk_2(a,b)=\underbrace{(mk_1+nk_2)}_{k}(a,b) \Leftarrow ma+nb\in C$
בגלל הסבר פורמלי ליאל" שלו הוא קבוע.

2. נראה $C\subset L(a,b)$: הי $k\cdot(a,b)\in C$ $(k\in\mathbb{Z})$. לפי משפט כנ"ל יש $m,n\in\mathbb{Z}$
עם $(a,b)=ma+nb \Rightarrow k(a,b)=kma+knb\in L(a,b)$

מספרים זרים 25, 9 הם זרים - אין להם מחלק משותף >1. למשל כאן $9\cdot\boxed{-11}+25\cdot\boxed{5}=1$ כמו כן $(25,9)=1$

$$\boxed{(a,b)\text{ זרים} \iff (a,b)=1 \iff 1\in L(a,b)}$$

הגדרה

אם $(a,b)=1$ אז לפי כן 1 ג"ל של a,b

ומצד שני אם 1 ג"ל של a,b הרי בגלל הרקע בתור שהם ולא לפי הגדרה כנ"ל, 1 הוא המינימום של a,b.

פיתרון: $(100,99)=1$ ומאותן סיבות לכל שני מספרים עוקבים $(a,a-1)=1$ כי אפשר לבחור את 1 בצורה $\boxed{1}a+\boxed{-1}(a-1)=1$

אומר אז שקר?

אם $a|c$ ואם $b|c$ אז $ab|c$

שקרן לפני בגלל שמה $12|6$ אבל $12|6\cdot 4$

הסבר אינטואיטיבי: $12=2\cdot 2\cdot 3$

אם $a|c$ ואם $b|c$ אז $ab|c$ **אם** $(a,b)=1$

אמת!

הוכחה: מקום: רוצים להגיע את c כמכפלה $a\cdot b$ אבל אומרים יודעים רק להגיע כמכפלה של כל כפולה.

לכן יש פה טריק שמשתמש בעובדה כנ"ל.

$(a,b)=1 \overset{\text{כנ"ל}}{\iff} \exists m,n\in\mathbb{Z}$ כך ש $ma+nb=1$

הטריק: נכפיל את c בכל של a,b ו...)

$$c=c\cdot 1=\underbrace{c\cdot ma}_{k_2\cdot b\cdot m\cdot a}+\underbrace{c\cdot nb}_{k_1 a n b}=$$

הרעיון להראות שכל כפולה ab. אין ערך שכל מחזר כפולה ab ? בעזרת שימוש a אבל c לעשות כפולה b ובדומה כמו מן

מקום הריק:

אם $\exists k_1\in\mathbb{Z}$ כך ש $c=k_1 a$

אם $\exists k_2\in\mathbb{Z}$ כך ש $c=k_2 b$

$$=(k_2 m)(ab)+(k_1 n)(ab)$$

$$\iff ab|c$$

מקום ריק

תגיד לו לעשות הפרדה בגלל הכפל כמו כל

$$\boxed{(a,b)=1}$$

במילים "אם שני מספרים זרים מחלקים את c אם מכפלתם מחלקת את c".

אמר לו שקר! "אם מספר מחלק מכפלת שני מספרים הרי מחלק אחד מהם"

כלומר: אם $a|bc$ אז $a|b$ או $a|c$

שקר! $4 \mid \underbrace{6\cdot 2}_{2\cdot 3\cdot 2}$ אבל $4\nmid 6$ ולא $4\nmid 2$

הפרכה

אין נתקן? (עלינה **שימו לב:** האם מספר a מחלק מכפלת שני מספרים b ו-c הרי מחלק אחד מהם?)

$\underbrace{3\cdot 5}_{15} \mid \underbrace{2\cdot 3}_{6}\cdot\underbrace{5\cdot 7}_{35}$ סה"כ

a b c

הגמה של אוקלידס:

"אם a מחלק מכפלת שני מספרים וזר לאחד מהם אז הוא מחלק את השני".

אם $a|bc$ ו-$(a,b)=1$ אז $a|c$.

דוגמה: $\underbrace{4}_{a} \mid \underbrace{3\cdot 8}_{24}$, $(4,3)=1 \Leftarrow 4\mid 8$

$2\cdot 2$ $3\cdot 2\cdot 2\cdot 2$ אם יש גורם משותף סימן שהגורמים לא זרים

הוכחת הגמה של אוקלידס:

שם נשתמש בעובדה: $(a,b)=1 \overset{\text{מכיוון}}{\Leftarrow}$ יש $m,n\in\mathbb{Z}$ עבורם $ma+nb=1 \Leftarrow$

$bc = \underbrace{cma}_{\text{כפולה של } a} + \underbrace{cnb}_{\text{כפולה של } a} = c(mc+nb) = c\cdot 1 = c$ מתקיים לכן c כפולה של a.

נתון כי $a|bc$

מעבר שלישי הפך נמצא לשון עבר

$a|cma$

$a|cnb$ כי נתון $a|bc$

$\Leftarrow a|\underbrace{cma+cnb}_{c}$

טענה: "הגדר גורם משותף מקסימלי"

יהיו $a,b\in\mathbb{Z}$ $c\in\mathbb{N}$ אז $(ca,cb)=c(a,b)$.

הוכחה:

נסמן $(a,b)=d \overset{\text{הגדרה מכיוון}}{\Longleftarrow}$ d הוא המס' החיובי הקטן ביותר בקבוצה

$\{ma+nb \mid m,n\in\mathbb{Z}\} \Leftarrow$ cd הוא " " " " "

$\{c(ma+nb) \mid m,n\in\mathbb{Z}\} \Leftarrow$ cd " " " " " "

$\{m(ca)+n(cb) \mid m,n\in\mathbb{Z}\} \Longleftarrow cd=(ca,cb)$

הבטוח לכך המס' הקטן ביותר שאינו מספר חיובי הוא המינימום שלהם