מסג

Greatest common divisor = מחלק משותף מירבי = ממ״מ = GCD

דוגמא:

לא תמיד כותבים

$\overbrace{gcd}(18,12) = 6$

"המחלק המשותף המירבי של 18 ו-12"

= המספר הכי גדול שמחלק גם את 18 וגם את 12

$(102, 103) = 1$

$(15, -4) = 1$ (המחלקים של מספר והנגדי שלו הם אותו דבר, לכן בנושא של gcd בדרך כלל נדון רק עם חיוביים)

זרים
(אין להם אף משותף פרט ל-1)

הגדרה: יהיו $a,b\in\mathbb{Z}$ (לא שניהם 0), נאמר כי d הוא המחלק המשותף המירבי של a ו-b אם:

① $d|a$ וגם $d|b$.

② לכל שלם c כך ש- $c|a$ ו- $c|b$ מתקיים $c \le d$.

"לכל מחלק משותף אחר c של a ו-b $c \le d$"

נסמן $d=(a,b)$.

סימון אחר לאותו דבר:

נסמן $D(a)=\{m\in\mathbb{Z} \mid m|a\}$ אוסף המחלקים של a

אז $(a,b) = \max\{D(a)\cap D(b)\}$

"המס' המקסימלי שגם מחלק את a וגם מחלק את b."

דוגמא:

$D(18)=\{\pm1,\pm2,\pm3,\pm6,\pm9,\pm18\}$

$D(12)=\{\pm1,\pm2,\pm3,\pm6,\pm12\}$

$(18,12)=\max\{1,2,3,6\}=6$

תכונה של הממ״מ: "אם נחלק שני מספרים בממ״מ שלהם, יתקבלו זוג מס' זרים"

דוגמא: $(18,12)=6$

$\left(\frac{18}{6},\frac{12}{6}\right)=(3,2)=1$

טענה: יהיו a,b שלמים המקיימים $d=(a,b)$. אזי $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

הוכחה: (איך מראים ששני מספרים זרים? מניחים שיש להם מחלק משותף $e>1$ ומגיעים לסתירה!)

נניח בשלילה כי $e>1$ מחלק משותף של $\frac{a}{d}$ ושל $\frac{b}{d}$.

$\Leftarrow$ יש k,l שלמים כך ש- $\begin{cases}\frac{a}{d}=ek\\ \frac{b}{d}=el\end{cases} \Leftarrow \begin{cases}a=\underline{de}k\\ b=\underline{de}l\end{cases} \Leftarrow$ de מחלק משותף

של a,b הגדול מ-d (כי $e>1$). סתירה, לכך ש-d הממ״מ של a,b.

המשפט הבא שנלמד הנו משפט בזו שנותן לנו אפיון שקול ל-(a,b). בשביל אותו צריכים להכיר את המושג "צרוף לינארי".

הסבר אינטואיטיבי: $7a-3b$, $11a+6b$ - צרופים לינאריים של a,b. כל ביטוי $\square a+\square b$ (שלם, שלם) הינו צ"ל של a,b.

שיו פורמליות... ⇐ **הגדרה:**

$\mathcal{L}(a,b)=\{ma+nb \mid m,n\in\mathbb{Z}\}$ = אוסף הצרופים הלינאריים של a,b.

משפט בזו (Bézout's identity): לכל $a,b\in\mathbb{Z}$, ניתן להציג את (a,b) כצרוף לינארי של a ו-b. (או במילים אחרות $(a,b)\in\mathcal{L}(a,b)$).

הוכחה:

[יש פה בהוכחה מין שפן שנשלף מהכובע: אנחנו נסתכל על כל הצ"ל של a,b שנותנים מספר חיובי. נראה שהקטן מביניהם הוא (a,b). איך בזו הגיע לזה? סביר להניח שהוא התחיל לעשות רשימה של הצ"ל של (a,b) שנותנים מס' חיובי וראה שבכל הפעמים (a,b) הוא הקטן ביותר.

למשל $(18,12)=6$

$1\cdot 18+(-1)\cdot 12=6$

צ"ל של $18,12$ שנותנים מס' חיובי: $0\cdot 18+1\cdot 12=12,\ 2\cdot 18+(-1)12=24\ \ldots$]

$(\mathbb{N}\cap\mathcal{L}(a,b))\ni a\cdot a+b\cdot b>0$ ⇐ מעקרון הסדר הטוב יש ב-$\mathbb{N}\cap\mathcal{L}(a,b)$ איבר מינימלי d.

נראה כי d הוא הממ"מ של a,b כלומר נראה כי $d=(a,b)$.

נראה: ① $d\in D(a)\cap D(b)$ (d מחלק את a ואת b).

② כל מחלק משותף אחר, c, של a ושל b מקיים $c\le d$.

① נראה כי $d|a$: נניח כי $d=ma+nb$. לפי משפט החלוקה (נחלק את a ב-d):

$a=dq+r \qquad 0\le r<d$

אם $r=0$ אז $d|a$ (וסיימנו). נניח בשלילה $r>0$ אז $\underbrace{a-qd}_{=r}>0$ ⇐ $\underbrace{a-q(ma+nb)}_{=r}>0$

⇐ $\underbrace{(1-qm)\cdot a-qn\cdot b}_{=r}>0$

צ"ל של a,b

⇐ $0<r<d$ ו-$r\in\mathcal{L}(a,b)\cap\mathbb{N}$ בסתירה לכך ש-d הוא האיבר המינימלי ב-$\mathcal{L}(a,b)\cap\mathbb{N}$.

(האם עכשיו נראה את ההוכחה מחדש אחרי זה? לא...)

לכן בהכרח $r=0$ ⇐ $d|a$. באופן סימטרי $d|b$ (הראינו את ①).

② נניח $c|a$ וגם $c|b$. אז $c\mid\underbrace{ma+nb}_{d}$ ⇐ $c|d$ ⇐ $c\le d$.

לפי סעיף ① קיימים m,n שלמים כך ש $d=ma+nb$

כי d חיובי

הסבר פורמלי ל"אז" הבא יגיע בהמשך.

מש"ל

יש שני רכיבים מתוך ההוכחה שחשוב שנזכור אותם גם באופן עצמאי:

> משהו מתוך ההוכחה שחשוב שתזכרו "באמצע הלילה": (a,b) הנו הצרוף הלינארי החיובי המינימלי של a ו-b.
>
> הכוונה שהצרוף כולו יוצא חיובי ולא שהמקדמים חיוביים

מהשורה האחרונה של ההוכחה

מסקנה: "כל מחלק משותף של a ו-b, מחלק את המחמ"מ (a,b)"
(לא רק שהמחמ"מ הוא גדול יותר מכל מחלק משותף אחר, אלא גם שהוא כפולה של כל מחלק משותף אחר)

משפט (הגדרה אלטרנטיבית ל-(a,b) ← שיכול לשמש גם מחלק את a ואת b ← כל מחלק משותף אחר שלהם מחלק גם אותו. לעומת שבהגדרה הקודמת היה לנו: "גדול או שווה ממנו")

יהיו $a,b\in\mathbb{Z}$ לא שניהם 0.
$d=(a,b)$ אמ"מ:

1. $d|a$ וגם $d|b$.
2. לכל c שמקיים $c|a$ וגם $c|b$ מתקיים $c|d$.

<u>הסבר</u> (לא כתיבת הוכחה פורמלית): אם $d=(a,b)$ לפי ההגדרה הקודמת אז 1 מתקיים אוטומטית והראינו במסקנה דלעיל שכל מחלק משותף c מחלק גם את d.
מצד שני, אם d מקיים את דרישות המשפט שלנו אז אוטומטית לכל מחלק משותף c מתקיים $c|d$ ומכאן $c\le d$ כמו בהגדרה המקורית.

<u>דרך אחרת לומר את אותו הסבר</u>: תנאי ① זהה בשתי ההגדרות. ② בקודמת ⇐ ② בחדשה לפי המסקנה, ואילו ② בחדשה ⇐ ② בקודמת כי אם $c|d$ אז $c\le d$.

<u>משפט</u>
המשפט הבא הוא משפט מבנה מפתיע - "אוסף הצרופים הלינאריים של a,b הם בדיוק אוסף הכפולות של (a,b)" $L(a,b)=\{k\cdot(a,b) \mid k\in\mathbb{Z}\}$

> דוגמה קטנה: $(18,12)=6$
>
> $L(18,12)=\{18a+12b \mid a,b\in\mathbb{Z}\}=\{0, 18, 30, 6, \ldots\}$ כלומר כפולות 6
> ($a=0, b=0$; $a=1, b=0$; $a=1, b=1$; $a=1, b=-1$)

<u>הוכחה</u> כדי להראות שוויון בין קבוצות עלינו להראות הכלה דו-כיוונית.

① נראה $L(a,b)\subseteq\overbrace{\{k\cdot(a,b) \mid k\in\mathbb{Z}\}}^{C}$: (לוקחים איבר באגף שמאל ומראים שהוא באגף ימין)
יהי $ma+nb\in L(a,b)$ ($m,n\in\mathbb{Z}$). (רוצים להראות שהוא מהצורה $k\cdot(a,b)$)

בהמשך הסבר פורמלי ל"איך" מצאו את ה-k הזה.

$(a,b)|a \Leftarrow a=k_1\cdot(a,b)$
$(a,b)|b \Leftarrow b=k_2\cdot(a,b)$
$\Rightarrow ma+nb=mk_1(a,b)+nk_2(a,b)=\underbrace{(mk_1+nk_2)}_{k}(a,b) \Rightarrow ma+nb\in C$

② נראה $C\subseteq L(a,b)$: יהי $k\cdot(a,b)\in C$ ($k\in\mathbb{Z}$). לפי משפט בזו יש $m,n\in\mathbb{Z}$
כך ש $(a,b)=ma+nb \Leftarrow k(a,b)=kma+knb\in L(a,b)$

כלומר $(20,9)=1$

מספרים זרים: $9,20$ הם זרים - אין להם מחלק משותף >1, ולפי כז"ו $9\cdot\boxed{-11}+20\cdot\boxed{5}=1$

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

הסבר: אם $(a,b)=1$ אז לפי כז"ו 1 צ"ל של a,b

ומצד שני אם 1 צ"ל של (a,b) הוא הכי הקטן בטבעיים שהוא ולכן לפי הוכחת כז"ו, 1 הוא המחלק המשו' של a,b.

דוגמה: $(100,99)=1$ ובאופן כללי לכל שני מספרים עוקבים $(a,a-1)=1$ כי אפשר לכתוב את 1 כצירוף לינארי: $\boxed{1}a+\boxed{-1}(a-1)=1$

אמת או שקר?

אם $a|c$ וגם $b|c$ אז $ab|c$

שקר! לדוג' $6|12$ וגם $4|12$ אבל $6\cdot4\nmid12$

הסבר אינטואיטיבי: $12=\underbrace{2\cdot\overbrace{2}^{}}_{4}\cdot 3$ (6 $=2\cdot3$)

חישוב

אם $a|c$ וגם $b|c$ וגם $\boxed{(a,b)=1}$ אז $ab|c$

אמת!

<u>הוכחה</u>: קושי: רוצים להציג את c ככפולה של $a\cdot b$ אבל אנחנו יודעים רק להציג ככפולה של כל אחד בנפרד.

לכן יש פה טריק שמשתמש במשפט כז"ו. $\boxed{\text{להשתמש במקום בהגדרה בהוכחה}}$

$(a,b)=1 \overset{\text{כז"ו}}{\Longrightarrow}$ קיימים $m,n\in\mathbb{Z}$ כך ש $ma+nb=1$

הטריק: (נציג את c כצ"ל של a,b ע"י...)

$$c=c\cdot1=\underbrace{c\cdot ma+c\cdot nb}=$$

רוצים להראות שזה כפולה של ab. איך נראה שכל מחובר כפולה של ab? כשמשתמשים ב-a אבל לא, נציב כפולה והבקשה כ"כ

חיבור 2 כפולות מהווה תרגיל כפולה מהשני

$$\underbrace{k_2\cdot b\cdot m\cdot a}\quad\underbrace{k_1 a n b}$$

מעקום שהשאלו לרשום:
$a|c \Leftarrow$ קיים $k_1\in\mathbb{Z}$ כך ש $c=k_1a$
$b|c \Leftarrow$ קיים $k_2\in\mathbb{Z}$ כך ש $c=k_2b$

$$=(k_2m)(ab)+(k_1n)(ab)$$

$$\Leftarrow ab|c$$

$\boxed{\text{כלומר "אם שני מספרים זרים מחלקים את } c \text{ גם מכפלתם מחלקת את } c\text{".}}$

אמת או שקר! "אם מספר מחלק מכפלת שני מספרים הנו מחלק לפ' אחד מהם"

כלומר: אם $a|bc$ אז $a|b$ או $a|c$

שקר! $4|\underbrace{6\cdot 2}_{2\cdot3\cdot2}$ אבל $4\nmid 6$ וגם $4\nmid 2$

הסבר

4 לוקח ($\diagup\diagdown$ 2·3·2)

(דיון אפשרי: "אם מספר a מחלק מכפלת שני מספרים זרים הנו מחלק אחד מהם" - שקר! לדוג'
$\underbrace{3\cdot5}_{15}\,|\,\underbrace{2\cdot3}_{6}\cdot\underbrace{5\cdot7}_{35}=210$
$a \quad b \quad c$)

אך נכון!

הלמה 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: $\overset{a}{4}\,|\,\underbrace{\overset{b}{3}\cdot\overset{c}{8}}_{24}$, $(4,3)=1 \Rightarrow 4|8$

$2\cdot2 \qquad 3\cdot2\cdot2\cdot2$

אם 4 זר ל-3 סימן שכל הגורמים רק מ-8

הוכחת הלמה של אוקלידס:

שוב נשתמש בלמה: $(a,b)=1 \overset{\text{בזו}}{\Rightarrow}$ יש $m,n\in\mathbb{Z}$ כך ש $ma+nb=1 \Rightarrow$

$\underbrace{cma}+\underbrace{cnb} = c(ma+nb) = c\cdot 1 = c$ נרצה להראות כי c כפולה של a.

כפולה של a - ברור

ואכן כפולה a כי $a|bc$

מכאן שמתקיים הדבר המבוקש

$$\left.\begin{array}{l} a|cma \\ a|cnb \ \text{כי נתון}\ a|bc \end{array}\right\} \Rightarrow a|\underbrace{cma+cnb}_{=c}$$

טענה: "הוצאת גורם משותף" ממממ"

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

הוכחה:

נסמן $(a,b)=d \overset{\text{הערה בזו}}{\Longrightarrow} d$ הוא המס' החיובי הקטן ביותר בקב'

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

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

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

הדרך להגדיר הוא: הקטן ביותר שלגביו מספרים הנ"ל המינ' אלה