דביר חדד

# **אלגברה מופשטת 1 – תרגול 2**

הקדמה לתורת המספרים:

הגדרה: יהי n טבעי נגדיר את $nZ=\{0,\pm n,\pm 2n,\dots\}$ להיות אוסף כל המספרים השלמים שמתחלקים ב n.

הגדרה: עבור $a,b\in\mathbb{Z}$ נאמר ש-a מחלק את b ונכתוב $a|b$ אם קיים $n\in\mathbb{Z}$ כך ש-na=b.

הגדרה: המחלק המשותף המקסימלי של n,m$\in\mathbb{Z}$ מסומן בgcd (Greatest Common Divisor) או ב(m,n)=gcd(m,n) ומוגדר להיות $\max\{d\in N: d|m\wedge d|n\}$=(m,n). אם (n,m)=1 נאמר ש-m ו-n זרים.

הערה: אם d|a ו d|b אזי d מחלק כל צירוף לינארי של a ו-b.

**טענה**: אם $n=qm+r$ אזי (n,m)=(m,r).

הוכחה: נסמן d=(n,m) . אנחנו יודעים מכאן ש d|n וגם d|m. כעת, מכיוון ש-r הוא צירוף ליניארי של n,m נקבל d|r. ולכן $d\le(m,r)$.

כעת נראה את הכיוון השני. (m,r)|r וגם (m,r)|m ז״א (m,r)|n וגם ידוע ש-(m,r)|n וגם (m,r)|m. לכן $d\ge$(m,r). ובסה״כ קיבלנו כי (m,r)=d=(n,m). מ.ש.ל. ■

אלגוריתם אוקלידס:

יהיו m,n$\in\mathbb{Z}$ . ניתן להניח כי $0\le m<n$. אם m=0 ברור ש-(m,n)=0. אחרת (m>0), ניתן לכתוב n=qm+r כאשר $0\le r<m$ ואז מתקיים (n,m)=(m,r).

**דוגמה (1)**: חישוב GCD באמצעות אלגוריתם אוקלידס: $(6,5)=(5,1)=1\ \underbrace{=}_{7\cdot 6+5}\ (47,6)\ \overset{1\cdot 47+6}{=}\ (53,47)$.

**דוגמה (2)**: $(28,7)=7\ \overset{1\cdot 28+7}{=}\ (35,28)\ \overset{1\cdot 35+28}{=}\ (63,35)\ \overset{3\cdot 63+35}{=}\ (224,63)$.

משפט איפיון הgcd.

מתקיים $u,v\in Z$ , $\gcd(a,b)=\min\{ua+vb>0\}$. ובפרט, קיימים $u,v\in Z$ כך ש-(a,b)=ua+vb.

**תרגיל**: הוכיח שלכל a,b,c שלמים מתקיים: (a,b)=1 וכן a|bc אזי a|c.

פתרון: ידוע כי (a,b)=1. לכן קיימים $\alpha,\beta\in Z$ כך ש $\alpha a+\beta b=1$. נכפול את שתי האגפים ב-c, וקיבלנו $a|\alpha ca\wedge a|\beta cb\to a|\alpha ca+\beta cb\to a|c$. מ.ש.ל. ■.

תכונות של הGCD:

1. d=(m,n) ויהי t כך ש t|m וגם t|n אזי t|d.
2. (am,an)=a(m,n)
3. אם p ראשוני וp|ab אזי p|a או p|b. (נובע מהתרגיל האחרון)

הגדרה: כפולה משותפת מינימלית (LCM=Least Common Multiple). ההגדרה הפורמלית הינה: $lcm(m,n)=[m,n]=\min\{d: n|d\wedge m|d\}$ .

<u>תכונות של הLCM:</u>

1. אם a|m וגם a|n אזי [m,n]|a
2. [n,m]·(n,m)=|nm|

**תרגיל**:

א. פתרו את המשוואה 7x=12(mod34) ;
ב. מצאו את הספרה האחרונה של $333^{333}$.

פתרון:

א. נכפיל בהופכי, כמו בהרצאה, ונקבל $7x = 12mod34 \rightarrow 35x = 60mod34 \rightarrow x = 26mod34$.

אתנחתא קלה: מציאת ההופכי של a ב-$Z_n$: זהו בעצם אותו a שמקיים ax-nk=1 עבור ax=1(mod(n))

ב. $3^{333}111^{333} = x\ mod(10) \equiv 333^{333}$ אבל $111^{333}mod10 = 1^{333}mod10 = 1mod10$=
לכן ניתן לכתוב $3^{333} = x\ mod10$. שוב נפרק ונקבל $x\ mod10 = 3^{4\cdot 83+1} = 81^{83}\cdot 3 = 1^{83}\cdot 3$.
פתרנו.

<u>חבורות ציקליות ותתי חבורות:</u>

הגדרה: תהי G חבורה ויהי a ששייך ל-G. אם כל איבר ב-G מתקבל כחזקה חיובית או שלילית של a נאמר ש-G נוצרת ע"י a ונקרא ל-G חבורה ציקלית. סימון: $G =< a >= \{a^k | k \in Z\}$.

**דוגמאות**:

1. $Z$ נוצרת ע"י 1 ו-1-.
2. *kZ=<k>*
3. $Z_6 =< 1 >=< 5 >$ כל חבורה ציקלית הנוצרת ע"י איבר ניתן ליצור אותה גם בעזרת ההופכי.

<u>הגדרה</u>: תהי *(G,*)* חבורה. אם $\emptyset \neq H \subseteq G$ כך ש-*(H,*)* היא בעצמה חבורה (ביחס לאותה הפעולה!) אזי *H* היא תת חבורה של *G* ונסמן $H \leq G$.

הקריטריון המקוצר לבדיקת היותו של *H* תת חבורה הינו:

1. $\emptyset \neq H \subseteq G$ .2 $\forall a, b \in H : ab^{-1} \in H$.

**דוגמה (1)**: $4Z \leq 2Z \leq Z \leq Q \leq R \leq C$. כל זה לגבי חיבור..

**דוגמה (2)**: האם $\mathrm{Z_n}$ ת"ח של *Z*? לא! כי לא מדובר באותה פעולה בכלל (וזאת גם לא תת קבוצה).

**דוגמה (3)**: תהי *G* חבורה ויהי *a* שייך לה. אזי $< a > \leq G$ היא תת החבורה הציקלית הנוצרת על ידי *a*.

**דוגמה (4)**: $SLn(F) \leq GLn(F)$. (מטריצות עם דטרמיננטות 1)

**תרגיל**: $\Omega_n = \left\{cis\left(\frac{2\pi k}{n}\right) : 0 \leq k \leq n-1\right\}$. אוסף כל שורשי היחידה מסדר *n*.
צריך להוכיח כי: 1. $\Omega_n \leq (C^*,\cdot)$ .2 *m*/*n* אזי $\Omega_m \leq \Omega_n$.

פתרון:

1. נוכיח לפי הקריטריון המקוצר. זה מוכל, בוודאות. זה לא ריק כי 1 שייך אליו. התנאי הראשון הוכח. עבור התנאי השני $(\forall \mathrm{a,b} \in \mathrm{H} : \mathrm{ab}^{-1} \in H)$

מתקיים: $(\mathrm{ab}^{-1})^n = a^n(b^n)^{-1} = 1 \cdot 1 = 1$. ולכן זוהי תת חבורה.

2. אם $m/n$ אזי $\Omega_m \leq \Omega_n$ . בעצם נוכיח תחילה שזה מוכל, שזהו התנאי הראשון של הקריטריון המקוצר. נניח ש $a \in \Omega_m$ אבל בגלל ש-$m/n$ ניתן לרשום $n=mk$ ולכן $\mathrm{a^m} = 1$.

$a^{mk} = (a^m)^k = 1^k = 1$ לסיכום, ראינו ש $\Omega_m$ היא תת קבוצה, בנוסף בסעיף א' ראינו ש $\Omega_m$ היא בעצמה חבורה, לכן לפי ההגדרה (אפילו לא לפי הקריטריון המקוצר!) נקבל ש $\Omega_m$ תת חבורה של $\Omega_n$. ומ.ש.ל.

**תרגיל**: הוכיחו באמצעות לוחות כפל שכל חבורה עם שני איברים וכל חבורה עם 3 איברים היא ציקלית.

פתרון: *S={e,a}*

*<a>=S*

| * | e | a |
|---|---|---|
| e | e | a |
| a | a | e |

עבור *S={e,a,b}*

*S=<a>=<b>*

*aa=b* כי לא יכול להיות ש*aa=e*!

| * | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | b | e |
| b | b | e | a |