# 1 [illegible]

בונוס: $gcd(252,198)=?$

$$252=1\cdot 198+54$$
$$198=3\cdot 54+36$$
$$54=1\cdot 36+18$$
$$36=2\cdot 18+0 \rightarrow gcd=(252,198)=18$$

$gcd(a,b)=ax+by$ .  $\underbrace{2\cdot \log_2 b \geq gcd(a,b)}_{\text{חסם עליון לאיטרציות.}}$ , $a,b>0$

$$36=198-3\cdot 54$$
$$54=252-1\cdot 198$$

$$18=54-1\cdot 36=54-(198-3\cdot 54)=4\cdot 54-1\cdot 198=$$
$$=54(252-1\cdot 198)-1\cdot 198=4\cdot 252-5\cdot 198$$
$$\Downarrow$$
$$x=4\ ,\ y=-5$$

צריך לפתור משלמים / רציונליים

## משוואות דיופנטיות לינאריות:

בעיה: איש רוצה לקנות $5100 במתנות (כלים). יש כלים ב- $200 וב- $500, כמה כלים מכל סוג הוא צריך לקנות?

נכתוב משוואה: $200x+500y=5100$   $x,y\geq 0, x,y\in\mathbb{Z}$

* דיופנטוס מאלכסנדריה, 200 לספירה נולד

$x,y,z\in\mathbb{Z}$   ; $x^n+y^n=1$ , $x=\frac{X}{Z}$ , $y=\frac{Y}{Z}$ .   משוואת פרמה. $X^n+Y^n=Z^n$

$$\boxed{ax+by=c}\ ,\ x,y\in\mathbb{Z}, a,b,c\in\mathbb{Z}$$
$$\downarrow$$

משוואה דיופנטית לינארית:

$d=gcd(a,b)$ .

משפט: נתון לנו: $ax+by=c$ , $a,b,c\in\mathbb{Z}$

(א) אם $d\nmid c$ אז אין פתרונות.

(ב) אם $d|c$ יש אין סוף פתרונות

(ג) אם $(x_0,y_0)$ פתרון הפרטי אז הפתרון הכללי הוא:

$$\boxed{x=x_0+\frac{b}{d}n \qquad y=y_0-\frac{a}{d}n \qquad n\in\mathbb{Z}}$$

הוכחה: (א) נניח $d\nmid c$. אם $ax+by=c$ אז $d|a$, $d|b$ אם $d\nmid ax+by$ סתירה.

(ב) נניח $d|c$. מבצרת אוקלידס קיימים $d=as+bt$   $s,t\in\mathbb{Z}$

$$c=ed$$
$$\Downarrow$$
$$ed=eas+ebt$$
$$c=ed=a\cdot(es)+b\cdot(et)$$
$$x_0=es\ .\quad y_0=et \rightarrow$$ יש פתרון!

המשך הוכחה:

נגדיר $x = x_0 + \frac{b}{d}n$, $y = y_0 - \frac{a}{d}n$ ⇐ $n \in \mathbb{Z}$

$$ax+by = a(x_0+\frac{b}{d}n)+b(y_0-\frac{a}{d}n) = \underbrace{ax_0+by_0}_{c}+\frac{ab}{d}n-\frac{ba}{d}n = c+0=c \ \checkmark$$

נראה כעת שכל פתרון הוא מהצורה הזאת.

נניח - $\begin{cases} ax+by=c \\ ax_0+by_0=c \end{cases}$

$$\Downarrow$$

$$a(x-x_0)=b(y_0-y)$$

$$\frac{a}{d}(x-x_0)=\frac{b}{d}(y_0-y)$$ מתקיים $gcd(\frac{a}{d},\frac{b}{d})=1$

⇐ $\frac{a}{d} \mid \frac{b}{d}(y_0-y)$ ומכיוון ש- $\frac{a}{d},\frac{b}{d}$ זרים נקבל - $\frac{a}{d} \mid (y_0-y)$

כלומר $\exists n\in\mathbb{Z}$ כך ש- $y_0-y=\frac{a}{d}n$ ⇐ $y=y_0-\frac{a}{d}n$ ✓

נציב חזרה $\frac{a}{d}(x-x_0)=\frac{b}{d}\cdot\frac{a}{d}n$ ⇐ $x-x_0=\frac{b}{d}n$ ⇐ $x=x_0+\frac{b}{d}n$ ✓ כנדרש!

דוגמאות

(1) $15x+6y=7$ ⇐ $gcd(15,6)=3$, $3\nmid 7$ ⇐ אין פתרון!

(2) $200x+500y=5100$ ⇔ $2x+5y=51$, $gcd(2,5)=1$, $1\mid 51$

⇐ ישנן כמה פתרונות. $1=2\alpha+5\beta$

$$\alpha=-2,\ \beta=1$$

$$1=2\cdot -2+5\cdot 1 \quad / \cdot 51$$

$$\cancel{51=2\cdot(51\cdot 2)\cdot 2+(51\cdot 5)\cdot 1}$$

$$51=2\cdot(51\cdot(-2))+5(51\cdot 1)$$

$$51=2\cdot(-102)+5(51)$$

$$\Downarrow$$

$$x_0=-102 \quad y_0=51$$

פתרון כללי: $x=-102+5\cdot n$, $y=51-2\cdot n$

אם אנחנו רוצים $x,y$ טבעיים לכן $\begin{cases} n\ge 21 \\ n\le 25 \end{cases}$ ⇐ $n=21,22,23,24,25$

$$\Downarrow$$

הפתרונות $=\{(3,9),(8,7),(13,5),(18,3),(23,1)\}$

# המשך תזכורת

## חוגים:

<u>הגדרה</u>: חוג זה קב' $A$ עם שתי פעולות $+/\cdot$ שמקיימות $a\in A$ המקיימים:

(1) $(a+b)+c=a+(b+c)$

(2) $a+b=b+a$

(3) $\exists 0$ כך שלכל $a\in A$: $a+0=a$

(4) $\forall a$ קיים $-a$ יחיד כך ש- $a+(-a)=0$

(5) $(ab)c=a(bc)$

(6) $a(b+c)=ab+ac$

(7) $\exists 1$: $1\cdot a=a$ $\leftarrow$ עם יחידה

(8) $ab=ba$ חוג קומוטטיבי.

<u>הגדרה</u>: שדה זה חוג $k$ כך שלכל $a\in k, a\neq 0$ קיים $x\in k$ כך ש- $ax=1$ $(x=a^{-1})$

$a^n=\underbrace{a\cdot a\cdots a}_{n \text{ פעמים}}$ $n\geq 1$ לכל טבעי, $a^0=1$. בשדה מתקיים $a^{-n}=(a^{-1})^n$ אם $a\neq 0$.

מתקיים: $a^{m+n}=a^m\cdot a^n$
$a^{mn}=(a^m)^n$

<u>דוגמאות</u>: $\mathbb{Z}$ חוג, $\mathbb{Q}$ שדה, $\mathbb{R}$ שדה, $\mathbb{C}$ שדה

$\mathbb{F}_2=\{\bar{0},\bar{1}\}$ שדה $(\bar{1}+\bar{1}=\bar{0}, \bar{1}\cdot\bar{1}=\bar{1})$

<u>הגדרה</u>: אידיאל בחוג $A$ הקומוט' עם יחידה זה תת הקבוצה $I\subset A$ כך ש- לכל $x,y\in I$, $r\in A$ מתקיים $x+y\in I$, $x-y\in I$, $rx,ry\in I$

<u>דוגמא</u>: $\mathbb{Z}_{even}\subset\mathbb{Z}$

$(a_1,\dots,a_n)\in A$ האידיאל $\{a_1x_1+\dots+a_nx_n \mid x_i\in A\}$ הוא האידיאל הנוצר ע"י $(a_1,\dots,a_n)$

במקרה $(a)=a\cdot A$ אידיאל ראשי.

<u>משפט</u>: ב-$\mathbb{Z}$ כל אידיאל הוא ראשי.

<u>הוכחה</u>: הוכחנו ש $\forall a,b\in\mathbb{Z}$, $(a,b)=(d)$. אותה הוכחה נותנת שכל אידיאל הינו ראשי.

<u>הגדרה</u>: יהי $A$ חוג. איבר $x\in A$ נקרא מחלק אפס אם $x\neq 0$ וקיים $y\neq 0$ כך ש- $0=xy$.

**טענה:** בשדה אין מחלקי אפס.

**הוכחה:** נאמר אם $xy=0$ ו- $y\neq 0$ אז קיים $y^{-1}$ כך ש- $y\cdot y^{-1}=1$

$$(xy)y^{-1}=0\cdot y^{-1}=0 \Leftrightarrow x(y\cdot y^{-1})=0 \Leftrightarrow x\cdot 1=0 \Leftrightarrow x=0 \quad \blacksquare$$

**הגדרה:** תחום שלמות זה חוג ללא מחלקי אפס.

**דוגמאות:** כל שדה הוא תחום שלמות.

$\mathbb{Z}$ תחום שלמות כי $\mathbb{Z}\subset\mathbb{Q}$

⚠ בנוסף כל תת חוג של שדה הוא תחום שלמות.

**הגדרה:** תחום ראשי זה תחום שלמות כך שכל אידיאל הוא ראשי.

**דוגמה:** $\mathbb{Z}$.

⚠ אין הוכחה אז אסור להשתמש במבחן!

**משפט:** בתחום שלמות יש פירוק יחיד לאי-פריקים.

**דוגמה:** $\mathbb{Z}[\sqrt{-5}]$ חוג. אין פירוק יחיד לאי-פריקים לכן ישנם אידיאלים לא ראשיים.

בתחום שלמות אפשר להגדיר ראשוניים/אי-פריקים.

**הגדרה:** $a\in A$ **הפיך** אם יש $b$ כך ש- $ab=1$. אז מתקיים $b=a^{-1}$.

$\mathbb{Z}[i]$ הפיכים: $\{1,-1,i,-i\}$

## קונגרואנציה:

**הגדרה:** $a,b\in\mathbb{Z}$, $m\in\mathbb{Z}$, $m>1$. אומרים ש-$a$ **קונגרואנטי** ל-$b$ מודולו $m$

אם $m|(a-b)$ : $a\equiv b\,(m)$

**דוגמה:** $2\equiv 30\,(7)$ ; $3\not\equiv 8\,(7)$

$2-30=-28$, $7|-28$ ; $3-8=-5$, $7\nmid -5$

**למה:** ① $a\equiv a\,(m)$ $\forall a$ ② $a\equiv b\,(m)\Rightarrow b\equiv a\,(m)$

③ $a\equiv b\,(m)$ , $b\equiv c\,(m) \Rightarrow a\equiv c\,(m)$

**מסקנה:** $\equiv$ זהו יחס שקילות.

**הגדרה:** $\mathbb{Z}/m\mathbb{Z}=\{$מחלקות שקילות$\}$

**דוגמה:** $m=2$ זוגיים, אי זוגיים.