gcd

$gcd(24,15)=3$

משפט: אם $gcd(a,b)=g\in\mathbb{Z}$ אז קיימים $x,y\in\mathbb{Z}$ כך ש- $g=xa+yb$

דוגמאות:

$3=2\cdot 24-3\cdot 15$ ✓

$2=\frac{4}{3}\cdot 24-2\cdot 15$ ✗

תרגיל: חשב את $y=gcd(210,135)$ והצג אותו כ- $x\cdot 210+y\cdot 135$, $x,y\in\mathbb{Z}$

פתרון:

$$210=\boxed{135}\cdot 1+\boxed{75}$$
$$135=\boxed{75}\cdot 1+\boxed{60}$$
$$75=\boxed{60}\cdot 1+\boxed{15}$$
$$60=4\cdot 15+0$$

$$15=75-60=75-(135-75)=2\cdot 75-135$$
$$=2(210-135)-135=2\cdot 210-3\cdot 135$$

תרגיל: אותו הדבר עם 187, 803:

$$803=187\cdot 4+55$$
$$187=55\cdot 3+22$$
$$55=22\cdot 2+11$$
$$22=11\cdot 2+0$$

$$11=55-2\cdot 22=55-2(187-3\cdot 55)$$
$$=7\cdot 55-2\cdot 187=7(803-4\cdot 187)-2\cdot 187$$
$$=7\cdot 803-30\cdot 187$$

דוגמה: $f=4x^4+4x^3+x$ $\quad g=2x^3+2x+1$

$$f=\boxed{g}(2x-1)+\boxed{2x^2+x+1}$$
$$g=(2x^2+x+1)(x+1)+0$$

לכן, $gcd(f,g)\overset{*}{=}2x^2+x+1=f-g(2x-1)\Rightarrow x^2+\frac{1}{2}x+\frac{1}{2}=\frac{1}{2}f-g(x-\frac{1}{2})$

עד כדי תיקון

(*) נשים לב שלמרות שכאן המקדמים הם שברים, זה בסדר כי מדובר על פולינום ושבר הוא פולינום, אם היינו מקבלים חלוקה של פולינומים זה לא היה בסדר כאן.

הגדרה $\mathbb{Z}_n$:

$$\mathbb{Z}_n=\{0,1,2,\dots,n-1\}$$

עם פעולות החיבור והכפל מודולו n. למשל: אם $n=5$ ולכן $\mathbb{Z}_5=\{0,1,2,3,4\}$

בתחום זה $3\cdot 3=4$ (כי $3\cdot 3=9=5\cdot 1+\boxed{4}$) ....

כך במספרים $2+4\equiv 6\equiv 1 \pmod 5$ אבל ב- $\mathbb{Z}_5$ $2+4=1$.

דוגמאות נוספות ב- $\mathbb{Z}_5$:

$$(4+3)\underbrace{(2+3)}_{0}+4=4$$
$$2^3\cdot(4+4)=3(3)=4$$
$$4^{100}=(-1)^{100}=1$$

⊛ נשים לב שחזקה אסור לצמצם "למספרים" בחוג הזה. לדוגמא: ב- $\mathbb{Z}_3$ $2^2=1$ אך $2^5=2$.

$\mathbb{Z}_n$ הוא חוג חילופי עם יחידה

טענה: א. $\mathbb{Z}_n$ הוא תחום שלמות $\Leftrightarrow$ n ראשוני.

ב. אם n ראשוני $\Leftrightarrow$ $\mathbb{Z}_n$ שדה.

תזכורת: תחום שלמות: $x\cdot y=0 \Rightarrow x=0$ או $y=0$.
שדה: $x\neq 0 \Rightarrow x$ הפיך
(שדה $\Rightarrow$ תחום שלמות - כי ניתן להכפיל בהופכי ולקבל שהגורם השני במכפלה שווה ל-0).

הוכחה: נניח ש-n לא ראשוני $n=m\cdot k$ כך ש- $1<m,k<n$, כלומר $m,k\in\mathbb{Z}_n$ אבל ב-$\mathbb{Z}_n$ $m\cdot k=0$, כלומר במקרה זה $\mathbb{Z}_n$ אינו תחום שלמות.

אם n ראשוני - נוכיח ש-$\mathbb{Z}_n$ שדה. נסמן $p=n$. יהי $a\in\{1,\dots,p-1\}$
ונראה כי a הפיך ב-$\mathbb{Z}_p$.

$\gcd(a,p)=1$ לכן קיימים $x,y\in\mathbb{Z}$ כך ש- $x\cdot a+y\cdot p=1$.
נכתוב $x=p\cdot m+r$, $0\le r\le p-1$

$(pm+r)a+y\cdot p=1 \Rightarrow p(ma+y)+ra=1 \Rightarrow ra\equiv 1 \pmod 1$
כלומר ב-$\mathbb{Z}_p$ $ra=1$. כיוון ש- $r\in\mathbb{Z}_p$, r הוא ההפכי של a.

תרגיל: יהי R תחום שלמות, ויהיו $0\neq a,b\in R$ כך ש- $a|b$ וגם $b|a$. הוכח ש- a,b חברים, כלומר קיים $u\in R^\times$ כך ש- $a=u\cdot b$.

הוכחה: לפי הנתון קיים $c,d\in R$ כך ש:

$$\left.\begin{array}{l}a=b\cdot c\\ b=a\cdot d\end{array}\right\}\Rightarrow b=a\cdot d=b\cdot c\cdot d\Rightarrow b(1-cd)=0\Rightarrow 1-cd=0\Rightarrow cd=1\Rightarrow$$
c,d הפיכים

מש"ל ☒

תרגיל: יהי R תחום שלמות, $q\in R$ אי פריק, $u\in R^\times$. להוכיח ש- $q\cdot u$ אי פריק.

פתרון: נניח בשלילה ש- $q\cdot u=q_1\cdot q_2$ כך ש- q_1,q_2 אינם הפיכים, לכן $q=(u^{-1}q_1)(q_2)$
(נשים לב ש- $u^{-1}q_1$ אינו הפיך (אם $(pu^{-1})q_1=p(u^{-1}q_1)=1 \Rightarrow q_1$ הפיך - סתירה).
אז קיבלנו פירוק של q למכפלה של איברים לא הפיכים וזו סתירה.

תרגיל: הוכח או הפרך: אם $f\in K[x]$ פולינום פריק, אזי יש לו שורש.

פתרון: לא נכון! דוגמה נגדית: $(x^2+1)^2\in\mathbb{R}[x]$ הוא פולינום פריק: $(x^2+1)(x^2+1)$ אבל
אין לו שורש ב- $\mathbb{R}$.

תרגיל: הוכח או הפרך: יהי K שדה, ויהי $p\neq$ פולינום ממעלה ≤ 3 אז
p פריק $\Leftrightarrow$ ל-p שורש ב- K.

פתרון: $\Leftarrow$: נכון תמיד.

(כי אחרת זה היה קבוע וקבוע הוא הפיך).

$\Rightarrow$: נפרק $p=q\cdot r$, $q,r\in K[x]$ ממעלה >0 אזי $\underset{\le 3}{\deg(p)}=\underset{>0}{\deg(q)}+\underset{>0}{\deg(v)}$

⇐ לפחות לאחד מהפולינומים q או r הדרגה גדולה מ-1. נניח בה"כ $deg(q)=1$

⇐ $q=(ax+b)\neq 0$ ולכן ל-q יש שורש: $-\frac{b}{a}$ ⇐ ל-p יש שורש!

<u>תרגיל:</u> $b,c\in\mathbb{R}$ כך ש $b^2-4c<0$. הוכח שהפולינום $f=x^2+bx+c$ אי פריק ב-$\mathbb{R}[x]$.

<u>פתרון:</u> נניח בשלילה ש-f פריק, אזי לפי התרגיל הקודם, היה ל-f שורש ב-$\mathbb{R}$.
אבל השורשים של הפולינום: $\frac{-b\pm\sqrt{b^2-4c}}{2}\in\mathbb{C}/\mathbb{R}$ וזו סתירה!

<u>תרגיל:</u> נסתכל בפולינום x^3-1. מצא את השורשים שלו:

א. מעל $\mathbb{C}$.

ב. מעל $\mathbb{R}$.

ג. מעל $\mathbb{Z}_5$.

<u>פתרון:</u> <u>א:</u> 1 הוא שורש אזי x^3-1 מתחלק ב $x-1$ (לחלק בשיטה):

$$\left.\begin{array}{l} \begin{array}{r|l} \overline{x^2+x+1} & \\ x^3-1 & x-1 \\ \underline{x^3-x^2} & \\ x^2-1 & \\ \underline{x^2-x} & \\ x-1 & \end{array}\end{array}\right\} \Rightarrow \quad x^3-1=(x-1)(x^2+x+1)$$

נמצא את השורשים של (x^2+x+1): $\frac{-1\pm\sqrt{1-4}}{2}=-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$

לכן ב-ⓒ השורשים הם 1, $-\frac{1}{2}\pm\frac{\sqrt{3}}{2}i$.

ב-ⓑ השורשים הם 1 וזהו.

<u>ג:</u> $\mathbb{Z}_5=\{0,1,2,3,4\}$. השורשים הם (ע"פ בדיקה אחד אחד ידנית): 1. בלבד.

$x^3-1=(x-1)\underline{(x^2+x+1)}$ הוא הפירוק ב $\mathbb{Z}_5$. וזה במקרה גם הפירוק כמו ב-$\mathbb{R}$. נשים לב שלפולינום אין שורשים ב-$\mathbb{Z}_5$.

<u>דוגמאות:</u> x^2+1 ב-$\mathbb{Z}_2$: $1^2+1=0$ $(x^2+1)=(x-1)(x-1)=(x+1)(x+1)$

$x^2-2=(x-\sqrt{2})(x+\sqrt{2})$ מעל $\mathbb{Z}_3$ $\sqrt{2}$ אינו מוגדר ולכן אי אפשר להשתמש בפירוק שביצענו ב-$\mathbb{R}$.

<u>תרגיל:</u> נתון פולינום $f(x)=x^n+a_{n-1}x^{n-1}+\dots+a_0$ כאשר $a_i\in\mathbb{Z}$ ונניח $b\in\mathbb{Z}$ שורש של f, הוכח ש $b|a_0$.

<u>פתרון:</u> נניח ש-b שורש $b^n+a_{n-1}b^{n-1}+\dots+a_1b+a_0=0$ ⇐ $b(b^{n-1}+a_{n-1}b^{n-2}+\dots+a_1)=-a_0$

⇐ $b|a_0$.

⊛ כלומר, כדי למצוא את השורשים של פולינום מתוקן מעל $\mathbb{Z}$, נמצא את המחלקים של a_0 ונבדוק אחד אחד, בשיטה. נשתמש בקריטריון איזנשטיין (ע"י משהו כזה).