תורת המספרים

בתורת המספרים חוקרים את קבוצת המספרים הטבעיים: $\mathbb{N}=\{1,2,3,...\}$. לפעמים יותר נוח לעבור עם המספרים השלמים: $\mathbb{Z}=\{0,1,-1,2,-2,...\}$. מוגדרות פעולות החיבור, החיסור והכפל.

<u>הערה:</u> 0 הוא אינו מספר טבעי.

<u>הגדרה:</u> מספר טבעי m **מורכב** אם $m=ab$, כאשר $a>1$ ו- $b>1$. מספר טבעי n **ראשוני** אם הוא לא מורכב ולא 1. לכן, 1 הוא לא ראשוני.

<u>הגדרה:</u> יהיו $a\in\mathbb{Z}$, $b\in\mathbb{Z}$ כאשר $a\neq 0$. אומרים ש- a **מחלק** את b ומסמנים $a|b$ אם $b=ac$ כאשר $x\in\mathbb{Z}$.

<u>תכונות של מחלק:</u>

1. $a|0$, $a|a$.
2. $a|b$ וגם $b|a$ $\Leftarrow$ $a=\pm b$.
3. $a|b$ וגם $b|c$ $\Leftarrow$ $a|c$.
4. $a|b$ וגם $a|c$ $\Leftarrow$ $a|bx+cy$ כאשר $x\in\mathbb{Z}$ ו- $y\in\mathbb{Z}$.

<u>הגדרה:</u> אם $a|b$ וגם $a|c$, אומרים ש- a הוא **מחלק משותף** של b ו- c.

קבוצת המספרים הראשוניים: $2,3,5,7,11,13,17,19,...$.

<u>שאלות על מספרים ראשוניים:</u>

1. האם יש מספר אינסופי של מספרים ראשוניים? כן, אוקלידס אמר את זה.
2. בעיית גולדבאך (*Goldbach*): האם ניתן לכתוב כל מספר זוגי כסכום של שני ראשוניים? לא ידוע.
3. **מספרים תאומים** הם מספרים ראשוניים שההפרש ביניהם הוא 2. השאלה היא: האם יש אינסוף מספרים תאומים? לא ידוע עד היום.
4. יהי $0<x\in\mathbb{R}$. נגדיר: $\pi(x)$ - מספר הראשוניים הקטנים מ- x. אזי $\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1$. זאת נוסחה שנסתכל עליה כנכונה בקורס הזה, והיא הוכחה במשפט *Hadamard-Vallé-Poussin* בערך מ-1890.

<u>הערה:</u> אם p ראשוני, אומרים גם ש- $-p$ ראשוני.

<u>למה:</u> כל מספר שלם $N\neq 0$ הוא מכפלת ראשוניים.

<u>הוכחה:</u> נניח בה"כ ש- N שלם. נוכיח באינדוקציה על N:

בסיס: עבור $N=1$ זה מתקיים באופן ריק. עבור $N=2$ זה מתקיים.

מעבר: מניחים שזה נכון לכל המספרים הקטנים מ- N. אם N ראשוני, אז זה ברור. אם $N=a\cdot b$, אז $a,b\leq N$, ולכן לפי הנחות האינדוקציה, הם גם מכפלות של ראשוניים.

מש"ל.

<u>מסקנה:</u> $n=(\pm 1)p_1^{a_1}\cdot\ldots\cdot p_m^{a_m}$ כאשר p_i ראשוניים, $a_i\in\mathbb{Z}$ ו- $a_i\geq 0$. כלומר: $n=(-1)^{\varepsilon(n)}\cdot\prod_{p\text{ ראשוניים}} p^{a(p)}$ כאשר $a(p)=0$ עבור כמעט כל p, $a(p)\neq 0$ רק למספר סופי של p-ים ו- $\varepsilon(n)\in\{0,1\}$.

<u>הגדרה:</u> יהיו $0\neq n\in\mathbb{Z}$ ו- $p\in\mathbb{Z}$ ראשוני. אז קיים $a\in\mathbb{N}$ כך ש- $p^a|n$ אבל $p^{a+1}\nmid n$. כותבים $a=\mathrm{ord}_p a$. זה נקרא **הסדר** של n ב- p.

<u>דוגמה:</u> $\mathrm{ord}_2 12=2, \mathrm{ord}_3 12=1, \mathrm{ord}_5 12=0,...$.

<u>למה:</u> אם $a,b\in\mathbb{Z}$ ו- $b>0$ אז קיימים $q,r\in\mathbb{Z}$ כך ש- $a=q\cdot b+r$ כאשר $0\leq r<b$, כאשר q זה **המנה** (*quotient*) ו- r זה **השארית** (*remainder*).

<u>הוכחה:</u> נסתכל של $\{a-x\cdot b|x\in\mathbb{Z}\}$. ברור שיש בקבוצה הזו מספרים אי שליליים, ולפי אקסיומת האינדוקציה, יש בקבוצה איבר אי שלילי מינימלי, שנסמנו ב- r. נסמן: $r=a-q\cdot b$. צ"ל: $0\leq r<b$. אם $r\geq b$, אז לוקחים $r'=r-b\geq 0$, והוא גם אי שלילי, בסתירה לכך ש- r אי שלילי מינימלי. מש"ל.

<u>הגדרה:</u> אם $a_1,...,a_n\in\mathbb{Z}$, נגדיר את **קבוצת הקומבינציות הליניאריות** על ידי $(a_1,...,a_n)=\left\{\sum_{i=1}^n a_i x_i \middle| x\in\mathbb{Z}\right\}$. אזי אם $x,y\in(a_1,...,a_n)$ אז גם $x\pm y\in(a_1,...,a_n)$, ולכל $r\in\mathbb{Z}$ מתקיים $r\cdot x\in(a_1,...,a_n)$.

<u>למה</u>: אם $a,b\in\mathbb{Z}$ אז קיים $d\in\mathbb{Z}$ כך ש- $(d)=(a,b)$.

<u>הוכחה</u>: אם $a,b=0$ אז $d=0$. אחרת, קיים $x>0$ כך ש- $x\in(a,b)$. לוקחים את d להיות החיובי המינימלי ב- (a,b). לכן, $(d)\subseteq(a,b)$. צ"ל כעת: $(a,b)\subseteq(d)$. יהי $c\in(a,b)$. לפי הלמה הקודמת, קיימים $q,r\in\mathbb{Z}$ כך ש- $c=q\cdot d+r$ כאשר $0\le r<d$. אזי $r=c-q\cdot d\in(a,b)$. אבל $0\le r<d$ ו- d מינימלי, ולכן $r=0 \Rightarrow c=q\cdot d$. מש"ל.

<u>הגדרה</u>: יהיו $a,b\in\mathbb{Z}$. מספר $d\in\mathbb{Z}$ נקרא **מחלק משותף מקסימלי** (*greatest common divisor*) של a,b אם $d|a$ וגם $d|b$, ולכל $c\in\mathbb{Z}$ מתקיים $c|a$ וגם $c|b \Rightarrow c|d$. נסמן: $d=\gcd(a,b)$ להיות החיובי, כלומר $d>0$.

<u>למה</u>: אם $(a,b)=(d)$, אז d הוא מחלק משותף מקסימלי של a,b.

<u>הוכחה</u>: ברור כי $d|a$ ו- $d|b$ כי $a,b\in(d)$. אזי d הוא מחלק משותף שלהם. אם c מחלק משותף, ו- $d=x\cdot a+y\cdot b$ ו- $c|a$ ו- $c|b$ אז $c|d$. מש"ל.

<u>הגדרה</u>: $a,b\in\mathbb{Z}$ נקראים **זרים** אם כל המחלקים המשותפים שלהם הם הפיכים. כלומר, ב- $\mathbb{Z}$ זה נכון אם ורק אם $\gcd(a,b)=1$.

<u>טענה</u>: נניח ש- $a|bc$ ו- $\gcd(a,b)=1$. אזי $a|c$.

<u>הוכחה</u>: מכיוון ש- $\gcd(a,b)=1$, אז קיימים r,s כך ש- $r\cdot a+s\cdot b=1$. לכן, $rac+sbc=c$. $a|rac$ ו- $a|sbc$ (כי $a|bc$), ולכן $a|c$. מש"ל.

<u>מסקנה</u>: אם p ראשוני ו- $p|bc$, אז $p|b$ או $p|c$.

<u>ניסוח שקול</u>: אם $p\nmid b$ וגם $p\nmid c$ אז $p\nmid bc$ כאשר p ראשוני.

<u>הוכחה</u> (של הניסוח הראשון): כל המחלקים של p הם $\pm1,\pm p$. לכן: $\gcd(p,b)\in\{1,p\}$. אם $\gcd(p,b)=p$ אז $p|b$. אם $\gcd(p,b)=1$, אז לפי הטענה, $p|c$. מש"ל.

<u>מסקנה</u>: יהי p ראשוני, $a,b\in\mathbb{Z}$, $a,b\neq0$. אזי $\mathrm{ord}_p(ab)=\mathrm{ord}_p a+\mathrm{ord}_p b$.

<u>הוכחה</u>: נסמן: $\alpha=\mathrm{ord}_p a,\beta=\mathrm{ord}_p b$. אזי: $a=p^{\alpha}c,b=p^{\beta}d$ כאשר $p\nmid c$ ו- $p\nmid d$. לכן, $ab=p^{\alpha+\beta}cd$. אבל $p\nmid cd$, ולכן $\mathrm{ord}_p(ab)=\alpha+\beta=\mathrm{ord}_p a+\mathrm{ord}_p b$. מש"ל.

<u>משפט</u>: לכל $0\neq n\in\mathbb{Z}$ קיים פירוק לגורמים ראשוניים $n=(-1)^{\varepsilon(n)}\cdot\prod_p p^{a(p)}$, כאשר $\varepsilon(n)$ ו- $a(p)$ נקבעים באופן יחיד על ידי n ומתקיים $a(p)=\mathrm{ord}_p n$.

<u>הוכחה</u>: יהי $q\in\mathbb{Z}$ מספר ראשוני. $\mathrm{ord}_q n=\varepsilon(n)\cdot\mathrm{ord}_q(-1)+\sum_p a(p)\mathrm{ord}_q p$. אבל $\mathrm{ord}_q(-1)=0$ וכמו כן, $\mathrm{ord}_q p=\begin{cases}1 & p=q\\ 0 & p\neq q\end{cases}$. לכן: $\mathrm{ord}_q n=a(q)$. מש"ל.

אלגוריתם אוקלידס

יהיו $a,b\in\mathbb{Z}$ כאשר $a,b\neq0$. איך ניתן לחשב מהר את $\gcd(a,b)$?

<u>למה</u>: יהיו $q,r\in\mathbb{Z}$ כך ש- $a=q\cdot b+r$ כאשר $0\le r<b$. אזי $\gcd(a,b)=\gcd(b,r)$.

<u>הוכחה</u>: אם $d|a$, וגם $d|b$ אז $d|r$. לכן, $\gcd(a,b)|r$. ולכן, $\gcd(a,b)|\gcd(b,r)$.
אם $d|b$ וגם $d|r$, אז $d|a$. לכן, $\gcd(b,r)|a$, ולכן $\gcd(b,r)|\gcd(a,b)$. מש"ל.

<u>אלגוריתם אוקלידס למציאת המחלק המשותף המקסימלי</u>: יהיו $a,b\in\mathbb{Z}$ כך ש- $a,b>0$. אזי:

$$\begin{gathered}a=q_1b+r_1,0\le r_1<b\\ b=q_2r_1+r_2,0\le r_2<r_1\\ r_1=q_3r_2+r_3,0\le r_3<r_2\\ \vdots\\ r_{k-1}=q_{k+1}r_k\end{gathered}$$

מהלמה נקבל: $\gcd(a,b)=\gcd(b,r_1)=\gcd(r_1,r_2)=\ldots=\gcd(r_{k-1},r_k)=r_k$.

<u>דוגמה</u>: $\gcd(252,198)=?$: $\left\{\begin{gathered}252=1\cdot198+54\\ 198=3\cdot54+36\\ 54=1\cdot36+18\\ 36=2\cdot18\end{gathered}\right\}$, ולכן $\gcd(252,198)=18$.

<u>קצב ההתכנסות של האלגוריתם</u> הוא $2\cdot\log_2 n$.

אנחנו יודעים שאם $\gcd(a,b)=d$ אז $(d)=(a,b)$, כלומר $d=ax+yb$ כאשר $x,y\in\mathbb{Z}$. אלגוריתם אוקלידס גם מאפשר לנו לחשב את x,y. למשל, בדוגמה:

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

לכן, $x=4,y=-5$.

<u>משפט אוקלידס</u>: יש אינסוף מספרים ראשוניים.

<u>הוכחה</u>: יהי p מספר ראשוני חיובי. הראשוניים החיוביים הקטנים או שווים ל-p: $2=p_1<p_2<\ldots<p_n=p$. נגדיר: $N=p_1 p_2\cdot\ldots\cdot p_n+1$. אזי N מתחלק במספר ראשוני p'. אבל לכל $1\le i\le n$, $p_i\nmid N$, כי יש שארית. לכן, לכל $1\le i\le n$, $p'\neq p_i$. לכן, $p'>p$. מש"ל.

<u>הגדרה</u>: **משוואה דיופנטית** היא משוואה שהפתרון שלה חייב להיות רציונלי או שלם.

<u>משפט</u>: נסתכל על $ax+by=c$ כאשר $a,b,c\in\mathbb{Z}$ והפתרונות $x,y\in\mathbb{Z}$. נגדיר: $d=\gcd(a,b)$. אזי אם $d\nmid c$ אזי אין פתרונות. אם $d|c$, יש אינסוף פתרונות. אם (x_0,y_0) פתרון פרטי, אז אפשר לכתוב את כל הפתרונות על ידי $x=x_0+\frac{b}{d}n$ ו-$y=y_0-\frac{a}{d}n$ כאשר $n\in\mathbb{Z}$.

<u>הוכחה</u>: נניח כי $d\nmid c$. נניח בשלילה שיש פתרון (x,y). אזי $ax+by=c$. אבל $d|a$ וגם $d|b$, ולכן $d|c$, וזו סתירה!

נניח כעת כי $d|c$. נסמן: $d=as+bt$, כאשר $s,t\in\mathbb{Z}$. $d|c$, ולכן קיים $e\in\mathbb{Z}$ כך ש-$c=de$, ואז $c=de=a\cdot es+b\cdot et$. נסמן: $x_0=es,y_0=et$. לכן, יש פתרון למשוואה. נגדיר $x=x_0+\frac{b}{d}n$, $y=y_0-\frac{a}{d}n$ כאשר $n\in\mathbb{Z}$. נציב:

$$ax+by=a\left(x_0+\frac{b}{d}n\right)+b\left(y_0-\frac{a}{d}n\right)=ax_0+by_0+\frac{ab}{d}n-\frac{ba}{d}n=ax_0+yb_0=c$$

נוכיח כעת שאין פתרונות אחרים: נניח ש-$ax+by=c$ פתרון כלשהו ו-$ax_0+by_0=c$. נחסר: $a(x-x_0)+b(y-y_0)=c-c=0$. אזי $\frac{d}{d}(x-x_0)=\frac{b}{d}(y_o-y)$. אבל $\gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$ ו-$\frac{a}{d}|\frac{b}{d}(y_0-y)$. לכן, $\frac{a}{d}|y_0-y$. לכן, קיים $n\in\mathbb{Z}$ כך שעבורו $y_o-y=\frac{a}{d}n\Leftarrow y=y_0-\frac{a}{d}n$. $\frac{a}{d}(x-x_0)=\frac{b}{d}\cdot\frac{a}{d}\cdot n$ $\Leftarrow$ $x-x_0=\frac{b}{d}n$ $\Leftarrow$ $x=x_0+\frac{b}{d}n$.

מש"ל.

<u>דוגמאות</u>:

1. $15x+6y=7$. אין פתרון, כי $\gcd(15,6)=3\nmid 7$.
2. איש רוצה לקנות המחאות נוסעים בסכום $5100\$$. יש המחאות ב-$200\$$ וב-$500\$$. כמה צ'קים מכל סוג הוא צריך לקחת? במילים אחרות, צריך לפתור את המשוואה $200x+500y=5100$ כאשר $x,y\in\mathbb{Z}$ ו-$x,y\ge 0$. אזי $\gcd(200,500)=100|5100$. מספיק לפתור את $2x+5y=51$ כאשר $x,y\in\mathbb{Z}$ ו-$x,y\ge 0$. נציב $x=51\alpha,y=51\beta$ ונקבל $2\alpha+5\beta=1$. אז: $\begin{Bmatrix}5=2\cdot 2+1\\2=2\cdot 1\end{Bmatrix}$, ולכן $1=1\cdot 5-2\cdot 2$, כלומר $\alpha=-2,\beta=1$. לכן, $x_0=-102,y_0=51$. לכן: $x=-102+5n$, $y=51-2n$. אבל $x,y\ge 0$, ולכן $21\le n\le 25$. לכן:

n	x	y
21	3	9
22	8	7
23	13	5
24	18	3
25	23	1

קונגרואנציה

<u>הגדרה</u> (של *Gauss – Gauß*): יהיו $a,b,m\in\mathbb{Z}$ כאשר $m>0$. אומרים ש-a **קונגרואנטי ל-b מודולו m** אם $m|(a-b)$. כותבים: $a\equiv b(\operatorname{mod} m)$ או $a\equiv b(m)$.

<u>דוגמאות</u>:

1. $2\equiv 30(7)$.
2. $2\equiv 9(7)$.
3. $4\not\equiv 8(3)$.

<u>למה</u>:

1. $a\equiv a(m)$.
2. $a\equiv b(m)\Rightarrow b\equiv a(m)$.
3. $a\equiv b(m)$ ו- $b\equiv c(m)$ $\Rightarrow$ $a\equiv c(m)$.

<u>הוכחה</u>: יהיו $a,b,c,m\in\mathbb{Z}$ כך ש- $m>0$.

1. $a-a=0$ ו- $m|0$, ולכן $a\equiv a(m)$.
2. $a\equiv b(m)$ $\Rightarrow$ $m|(a-b)$ $\Rightarrow$ $m|(b-a)$ $\Rightarrow$ $b\equiv a(m)$.
3. $a\equiv b(m)$ ו- $b\equiv c(m)$ $\Rightarrow$ $m|(a-b)$ ו- $m|(b-c)$. כמו כן, $a-c=(a-b)+(b-c)$. לכן, $m|(a-c)$ $\Rightarrow$ $a\equiv c(m)$.

מש"ל.

לכן, זהו יחס שקילות, ולכן יש מחלקות שקילות.

<u>הגדרה</u>: יהי m קבוע, ויהי $a\in\mathbb{Z}$. **מחלקת הקונגרואנציה** של a היא $\{a+km|k\in\mathbb{Z}\}$. סימון: $a+m\mathbb{Z}$.

<u>סימון</u>: $\mathbb{Z}/m\mathbb{Z}$ – קבוצת מחלקות הקונגרואנציה מודולו m. עבור $a\in\mathbb{Z}$, נגדיר: $\bar{a}=a+m\mathbb{Z}$.

<u>דוגמה</u>: $m=3$: $0+3\mathbb{Z}=\{0,\pm3,\pm6,\dots\}$, $1+3\mathbb{Z}=\{1,-2,4,-5,\dots\}$, $2+3\mathbb{Z}=\{2,-1,5,-4,\dots\}$.

<u>למה</u>: יש בדיוק m מחלקות קונגרואנציה מודולו m.

<u>הוכחה</u>: נגדיר קבוצה $S=\{0,\dots,m-1\}$. נוכיח כי אם $a,b\in S$ ו- $a\neq b$ אז $a\not\equiv b(m)$. נניח $a\equiv b(m)$. אזי $m|(a-b)$, ולכן $m||a-b|$. אבל $|a-b|<m$, ולכן $|a-b|=0$ $\Rightarrow$ $a=b$, בסתירה.

נוכיח כעת כי כל מספר $c\in\mathbb{Z}$ קונגרואנטי למספר ב-S. נסמן: $c=qm+r$ כאשר $0\le r<m$. לכן, $r\in S$ ו- $c\equiv r(m)$.

לכן, קיבלנו העתקה חח"ע ועל $S\to\mathbb{Z}/m\mathbb{Z}$. מש"ל.

<u>דוגמה</u>: עבור $m=2$, יש 2 מחלקות קונגרואנציה: $\bar{0}=0+2\mathbb{Z}$ ו- $\bar{1}=1+2\mathbb{Z}$.

<u>למה</u>: אם $a\equiv a'(m)$ ו- $b\equiv b'(m)$ אז $a+b\equiv a'+b'(m)$ ו- $a\cdot b\equiv a'\cdot b'(m)$.

<u>הוכחה</u>: $a\equiv a'(m)$ ו- $b\equiv b'(m)$ $\Rightarrow$ $m|(a-a')$ ו- $m|(b-b')$.

עבור חיבור: $(a+b)-(a'+b')=(a-a')+(b-b')$ $\Rightarrow$ $m|[(a+b)-(a'+b')]$ $\Rightarrow$ $a+b\equiv a'+b'(m)$.

עבור כפל: נסמן: $a'=a+km$, $b'=b+lm$ כאשר $k,l\in\mathbb{Z}$. אזי:
$a'\cdot b'=(a+km)\cdot(b+lm)=a\cdot b+m(al+bk+klm)$, ולכן $a'\cdot b'\equiv a\cdot b(m)$.

מש"ל.

<u>הגדרה</u>: **חיבור**: $(a+m\mathbb{Z})+(b+m\mathbb{Z})\coloneqq a+b+m\mathbb{Z}$. **כפל**: $(a+m\mathbb{Z})\cdot(b+m\mathbb{Z})=a\cdot b+m\mathbb{Z}$.

יש איבר ניטרלי ביחס לחיבור: $\bar{0}$, כי $\bar{a}+\bar{0}=\bar{a}$, ויש איבר ניטרלי ביחס לכפל: $\bar{1}$ כי $\bar{1}\cdot\bar{a}=\bar{a}$.

<u>הגדרה</u>: **חוג** (באנגלית: *ring*, ברוסית: *Кольцо*, בצרפתית: *Anneau*) הוא קבוצה A עם שתי פעולות – חיבור (+) וכפל (·), ואיבר 1 כך שמתקיים:

1. אסוציאטיביות של חיבור: $\forall a,b,c\in A.(a+b)+c=a+(b+c)$.
2. קומוטטיביות של חיבור: $\forall a,b\in A.a+b=b+a$.
3. קיום איבר ניטרלי ביחס לחיבור: $\exists 0\in A.\forall a\in A.a+0=a$.
4. קיום איבר נגדי ביחס לחיבור: $\forall a\in A.\exists b\in A.a+b=0$.
5. אסוציאטיביות של כפל: $\forall a,b,c\in A.(a\cdot b)\cdot c=a\cdot(b\cdot c)$.
6. דיסטריבוטיביות: $\forall a,b,c\in A.a\cdot(b+c)=a\cdot b+a\cdot c,(b+c)\cdot a=b\cdot a+c\cdot a$.
7. קיום איבר ניטרלי ביחס לכפל: $\exists 1\in A.\forall a\in A.1\cdot a=a=a\cdot 1$.

<u>הגדרה</u>: **חוג קומוטטיבי** הוא חוג A שמקיים קומוטטיביות בכפל: $\forall a,b\in A.a\cdot b=b\cdot a$.

<u>הערה</u>: בקורס הזה, כל החוגים הם חוגים קומוטטיביים.

דוגמאות:
1. **חוג השארית מודולו m** – $\mathbb{Z}/m\mathbb{Z}$.
2. $\{0,1,2,\dots\}$ לא חוג, כי למשל ל- 3 אין a כך ש- $a+3=0$.
3. $\mathbb{Z}$ – חוג.
4. $2\mathbb{Z}=\{0,\pm2,\pm4,\dots\}$ לא חוג, כי אין 1 .

הגדרה: איבר a בחוג A הוא **הפיך** אם קיים $b\in A$ כך ש- $a\cdot b=1$.
הגדרה: **שדה** הוא חוג K עם $1\neq0$ כך שאם $0\neq x\in K$ אז x הפיך.
הגדרה: איבר $a\in setA$ הוא **מחלק אפס** אם $a\neq0$ וקיים $b\in A$ כך ש- $b\neq0$ ו- $a\cdot b=0$.
דוגמה: ב- $\mathbb{Z}/6\mathbb{Z}$ מתקיים $\bar{2}\cdot\bar{3}=\bar{6}=\bar{0}$.
טענה: בשדה אין מחלקי אפס.
הוכחה: יהי K שדה. יהיו $a,b\in K$ כך ש- $a\cdot b=0$ ו- $b\neq0$. אזי קיים b^{-1} , ואז:

$$a=1\cdot a=(b^{-1}\cdot b)\cdot a=b^{-1}\cdot(b\cdot a)=b^{-1}\cdot(a\cdot b)=b^{-1}\cdot0=0$$

לכן, $a=0$. מש"ל.
קיבלנו בפרט, כי $\mathbb{Z}/6\mathbb{Z}$ אינו שדה.
הגדרה: חוג קומוטטיבי נקרא **תחום שלמות** אם אין בו מחלקי אפס.
לכן, כל שדה ו- $\mathbb{Z}$ (בפרט) הם תחומי שלמות.
טענה: אין פתרון ב- $\mathbb{Z}$ למשוואה $x^2-117x+31=0$.
הוכחה: אם היה לה פתרון ב- $\mathbb{Z}$, אז גם היה לה פתרון ב- $\mathbb{Z}/2\mathbb{Z}$. נוכיח כי אין לה פתרון ב- $\mathbb{Z}/2\mathbb{Z}$: כלומר צ"ל שלמשוואה $\bar{x}^2-\bar{1}\cdot\bar{x}+\bar{1}=\bar{0}$ אין פתרון. עבור $\bar{x}=\bar{0}$ נקבל $\bar{0}-\bar{0}+\bar{1}=\bar{1}$. עבור $\bar{x}=\bar{1}$ נקבל $\bar{1}-\bar{1}+\bar{1}=\bar{1}$. לכן, אין פתרון ב- $\mathbb{Z}/2\mathbb{Z}$, ולכן גם אין פתרון ב- $\mathbb{Z}$. מש"ל.
למה: אם $b,c\in\mathbb{Z}$ ו- $b\equiv1(4),c\equiv1(4)$, אזי $b\cdot c\equiv1(4)$. לכן, אם $a\equiv3(4)$ אז יש ל- a מחלק ראשוני p כך ש- $p\equiv3(4)$.
הוכחה: נניח שכל המחלקים הראשוניים p_i מקיימים $p_i\not\equiv3(4)$. אזי $a=p_1\cdot\ldots\cdot p_n\not\equiv3(4)$, בסתירה! מש"ל.
טענה: במחלקת השקילות $3+4\mathbb{Z}$ יש אינסוף מספרים ראשוניים.
הוכחה ראשונה: יש מספר ראשוני הקונגרואנטי ל- 3 מודולו 4 : $3\in3+4\mathbb{Z}$. נכתוב כעת את n המספרים הראשוניים הראשונים ב- $3+4\mathbb{Z}$: $3=p_0<p_1<\ldots<p_n$. נגדיר: $N=4p_1\cdot\ldots\cdot p_n+3$. אזי $N\equiv3(4)$. p_i ראשוניים ו- $p_i\equiv3(4)$. לכן, לכל $i=1,\dots,n$ מתקיים $p_i\nmid N$. גם $p_0=3\nmid N$. אזי N הוא מספר ראשוני חדש, קונגרואנטי ל- 3 מודולו 4 . מש"ל.
הוכחה שנייה: באותם הסימונים כמו קודם, נגדיר: $N=4p_0\cdot p_1\cdot\ldots\cdot p_n-1$. אזי $N\equiv3(4)$ ולכל i מתקיים $p_i\nmid N$. לכן, N הוא מספר ראשוני חדש, קונגרואנטי ל- 3 מודולו 4 . מש"ל.

קונגרואנציות לינאריות

הגדרה: משוואה מהצורה $a\cdot x\equiv b(m)$ (כאשר x הוא משתנה) נקראת **קונגרואנציה לינארית**.
האם ומתי יש לקונגרואנציות לינאריות פתרונות, וכמה?
משפט: לקונגרואנציה לינארית $a\cdot x\equiv b(m)$ יש פתרון $\Leftrightarrow$ $d|b$ כאשר $d=\gcd(a,m)$. אם x_0 פתרון, אז כל הפתרונות הם $x_0,x_0+m',\dots,x_0+(d-1)m'$ כאשר $m'=\frac{m}{d}$. כלומר, יש בדיוק d פתרונות.
הוכחה: $a\cdot x\equiv b(m)$ $\Leftarrow$ $a\cdot x+m\cdot y=b$, כאשר $y\in\mathbb{Z}$. נסמן: $d=\gcd(a,m)$. אזי יש פתרון לקונגרואנציה הלינארית $\Leftrightarrow$ יש פתרון למשוואה הדיופנטית $\Leftrightarrow$ $d|b$.
נניח כעת כי (x_0,y_0) פתרון (של המשוואה הדיופנטית, ובפרט x_0 פתרון של הקונגרואנציה הלינארית).
נסמן: $m'=\frac{m}{d},a'=\frac{a}{d}$. אזי, כל הפתרונות של המשוואה הדיופנטית הם $(x_0+m't,y_o-a't)$. לכן, כל הפתרונות של הקונגרואנציה הלינארית הם $x=x_0+m't$. הפתרונות $x_0,x_0+m't,\dots,x_0+(d-1)\cdot m'$ הם לא קונגרואנטיים אחד לשני. מכיוון ש- $m=dm'$ (לפי ההגדרה) ו- $t=qd+r$ כאשר $0\le r<d$, נקבל $x_1=x_0+qdm'+rm'$ $\Leftarrow$ $x_1\equiv x_0+rm'(m)$. מש"ל.
דוגמה: $6\cdot x\equiv3(15)$ $\Leftarrow$ $6x-15y=3$. $\gcd(6,15)=3$ ו- $3|3$ $\Leftarrow$ יש פתרון: $x_0=3$. מכיוון ש- $m=15,d=3$ $\Leftarrow$ $m'=\frac{15}{3}=5$. לכן, הפתרונות הם $3,3+5=8,3+2\cdot5=13$.

<u>מסקנה</u>: אם a ו- m זרים, אז לקונגרואנציה $a\cdot x\equiv b(m)$ יש בדיוק פתרון אחד.
<u>הוכחה</u>: אם $d=\gcd(a,m)=1$, נקבל $1=d|b$, ולכן יש בדיוק $d=1$ פתרונות. מש"ל.
<u>מסקנה</u>: אם p ראשוני ו- $a\not\equiv 0(p)$ אז לקונגרואנציה $a\cdot x\equiv b(p)$ יש פתרון יחיד.
<u>הוכחה</u>: $a\not\equiv 0(p)$ ⇐ a ו- p זרים. לכן, לפי המסקנה הקודמת, יש פתרון יחיד. מש"ל.
<u>מסקנה</u>: $\mathbb{Z}/p\mathbb{Z}$ שדה עבור p ראשוני.
<u>הוכחה</u>: אם $\bar{0}\neq\bar{a}\in\mathbb{Z}/p\mathbb{Z}$, אז $a\not\equiv 0(p)$. ניקח $a\cdot x\equiv 1(p)$. לפי המסקנה, יש פתרון ו- $\bar{a}\cdot\bar{x}=\bar{1}$. מש"ל.
לכן, למשל, $\mathbb{Z}/37\mathbb{Z}$ שדה. לכן, ל- $1,\dots,10$ יש הופכיים ב- $\mathbb{Z}/37\mathbb{Z}$.
<u>סימון</u>: מסמנים $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ (כי $\mathbb{F}$ - *Field*).
<u>הגדרה</u>: **קבוצת ההפיכים**: $U(\mathbb{Z}/m\mathbb{Z})=(\mathbb{Z}/m\mathbb{Z})^{\times}=(\mathbb{Z}/m\mathbb{Z})^{*}$.
השאלה היא כמה הפיכים יש ב- $\mathbb{Z}/m\mathbb{Z}$?
<u>טענה</u>: $\bar{a}$ הפיך אם יש פתרון למשוואה $\bar{a}\cdot\bar{x}=\bar{1}$ או לקונגרואנציה $a\cdot x\equiv 1(m)$.
<u>הוכחה</u>: יש פתרון ⇔ a זר ל- m ⇔ $\bar{a}$ הפיך. מש"ל.
<u>סימון</u>: **מספר המספרים הזרים ל- m מודולו m**: $\phi(m)=\varphi(m)$.
<u>דוגמה</u>: $\varphi(6)=2$. עבור p ראשוני, $\varphi(p)=p-1$.
$\varphi(m)$ נקרא **פונקציית אוילר** (*Euler*). $\varphi(m)=?$
<u>הגדרה</u>: $\bar{a}\in\mathbb{Z}/m\mathbb{Z}$ נקרא **הפיך** אם קיים $\bar{x}$ כך ש- $\bar{a}\bar{x}=\bar{1}$.
<u>למה</u>: אם $a_1,\dots,a_l\in\mathbb{Z}$ וגם $\gcd(a_i,m)=1$ לכל i, אזי $\gcd(a_1\cdot\ldots\cdot a_l,m)=1$.
<u>הוכחה</u>: אם $\gcd(a_1\cdot\ldots\cdot a_l,m)\neq 1$ אז קיים p ראשוני כך ש- $p|m$ ו- $p|a_1\cdot\ldots\cdot a_l$. אז קיים i כך ש- $p|a_i$, ואז $\gcd(a_i,m)\neq 1$, בסתירה! מש"ל.
<u>למה</u>: נניח ש- $a_i|n$ לכל $i=1,\dots,t$, ונניח ש- $\gcd(a_i,a_j)=1$ עבור $i\neq j$. אזי $a_1\cdot\ldots\cdot a_t|n$.
<u>הוכחה</u>: באינדוקציה על t:
בסיס – $t=1$: אין מה להוכיח.
מעבר – $t-1\to t$: נניח שהלמה נכונה עבור $t-1$. אזי: $a_1\cdot\ldots\cdot a_{t-1}|n$. לפי הלמה הקודמת, $\gcd(a_1\cdot\ldots\cdot a_{t-1},a_t)=1$. לכן, קיימים מספרים שלמים $r,s\in\mathbb{Z}$ כך ש- $ra_t+sa_1\cdot\ldots\cdot a_{t-1}=1$. נכפיל ב- n ונקבל: $nra_t+nsa_1\cdot\ldots\cdot a_{t-1}=n$. אזי $a_1\cdot\ldots\cdot a_{t-1}a_t|nra_t$, כי $a_1\cdot\ldots\cdot a_{t-1}|n$ וגם $a_1\cdot\ldots\cdot a_{t-1}a_t|nsa_1\cdot\ldots\cdot a_{t-1}$, כי $a_t|n$. לכן, $a_1\cdot\ldots\cdot a_{t-1}a_t|n$.
מש"ל.
<u>משפט השאריות הסיני</u>: נניח ש- $m=m_i\cdot\ldots\cdot m_t$, כך ש- $\gcd(m_i,m_j)=1$ עבור $i\neq j$. יהיו $b_1,\dots,b_t\in\mathbb{Z}$. נסתכל על מערכת הקונגרואנציות $x\equiv b_i(m_i)$. אזי המערכת הזאת ניתנת לפתרון, וכל שני פתרונות נבדלים בכפולה של m.
<u>הוכחה</u>: נגדיר: $n_i=\frac{m}{m_i}\in\mathbb{Z}$. לפי הלמה, $\gcd(m_i,n_i)=1$. לכן, קיימים $r_i,s_i\in\mathbb{Z}$ כך ש- $r_im_i+s_in_i=1$.
נגדיר: $e_i=s_in_i\in\mathbb{Z}$. אזי $e_i\equiv 1(m_i)$, וכן $e_i\equiv 0(m_j)$ עבור $j\neq i$, כי $m_j|n_i$. נגדיר: $x_0=\sum_{i=1}^{t}b_ie_i$. אזי $x_0\equiv b_ie_i\equiv b_i(m_i)$. לכן, x_0 הוא פתרון. אם x_1 הוא פתרון אחר, אזי $\forall i.x_1-x_0\equiv 0(m_i)$. לכן, $m_i|x_1-x_0$ לכל i, ולפי הלמה, מכיוון ש- $\{m_i\}_{i=1}^{t}$ זרים בזוגות, $m|x_1-x_0$. מש"ל.
<u>דוגמאות</u>:
1. הסיני סון צו (מהמאה הראשונה לספירה) ניסה למצוא מספר שלם, כך שהשאריות שלו מחלוקה ב- $3,5,7$ הן $2,3,3$ בהתאמה. בשפה קונגרואנטית: $x\equiv 2(3)$, $x\ equiv3(5)$, $x\equiv 2(7)$. אזי $m_1=3$, $m_2=5$, $m_3=7$, $m=3\cdot 5\cdot 7=105$, $n_1=\frac{m}{m_1}=5\cdot 7=35$, $n_2=\frac{m}{m_2}=3\cdot 7=21$, $n_3=\frac{m}{m_3}=3\cdot 5=15$. $r_1\cdot m_1+s_1\cdot n_1=r_1\cdot 3+s_1\cdot 35=1$ ⇐ $s_1\cdot 35\equiv 1(3)$ ⇐ $s_1\cdot 2\equiv 1(3)$ ⇐ $s_1=2$. באופן דומה, $s_2\cdot 21\equiv 1(5)$ ⇐ $s_1\cdot 1\equiv 1(5)$ ⇐ $s_2=1$, $s_3\cdot 15\equiv 1(7)$ ⇐ $s_3\cdot 1\equiv 1(7)$ ⇐ $s_3=1$. לכן, $e_1=s-1\cdot n_1=2\cdot 35=70$, $e_2=s_2\cdot n_2=1\cdot 21=21$, $e_3=s_3\cdot n_3=1\cdot 15=15$.
כעת: $x=2\cdot 70+3\cdot 21+2\cdot 15=233$. אבל $233\equiv 23(105)$, ולכן $x\equiv 23(105)$.

2. נתון: $6x\equiv 9(15)$, $4x\equiv 1(7)$. נפתור כל אחת מהקונגרואנציות: עבור $6x\equiv 9(15)$: $\gcd(6,15)=3|9$, ולכן יש פתרון. $\Leftarrow$ $2x\equiv 3(5)$, כלומר $2x\equiv -2(5)$ $\Leftarrow$ $x\equiv -1(5)$ $\Leftarrow$ $x\equiv 4(5)$. עבור $4x\equiv 1(7)$: $\gcd(4,7)=1|1$, ולכן יש פתרון. $4x\equiv 1(7)$ $\Leftarrow$ $4x\equiv 8(7)$ $\Leftarrow$ $x\equiv 2(7)$. קיבלנו את המערכת: $x\equiv 4(5)$, $x\equiv 2(7)$. מהאלגוריתם שבהוכחה של משפט השאריות הסיני, $x\equiv 9(35)$.

<u>טענה</u>: $\mathbb{Z}/m\mathbb{Z}$ הוא שדה אם ורק אם m ראשוני.

<u>הוכחה</u>: יהי p ראשוני, ויהי $0\neq\bar{a}\in\mathbb{Z}/p\mathbb{Z}$. אזי $a\not\equiv 0(p)$ ו- $p\nmid a$. a זר ל- p, ולכן $\bar{a}$ הפיך. $\bar{0}\neq\bar{1}$, ולכן $\mathbb{Z}/p\mathbb{Z}$ שדה.

נניח כעת ש- m מורכב, כלומר $m=m_1\cdot m_2$ כאשר $m_1,m_2>1$. אזי $\bar{m}_1\cdot\bar{m}_2=\overline{m_1 m_2}=\bar{m}=0$. $m_1,m_2\neq 0$, ולכן יש מחלקי אפס ב- $\mathbb{Z}/m\mathbb{Z}$. לכן, $\mathbb{Z}/m\mathbb{Z}$ אינו שדה.

מש"ל.

<u>הגדרה</u>: אם R,R' חוגים, **הומומורפיזם** של חוגים הוא העתקה $\psi:R\to R'$ כך ש- $\psi(x+y)=\psi(x)+\psi(y)$, $\psi(x\cdot y)=\psi(x)\cdot\psi(y)$ ו- $\psi(1_R)=1_{R'}$.

<u>הגדרה</u>: **איזומורפיזם** של חוגים הוא הומומורפיזם חח"ע ועל.

<u>טענה</u>: נניח ש- $m=m_1\cdot m_2$, ו- $\gcd(m_1,m_2)=1$. אזי: $\varphi(m_1\cdot m_2)=\varphi(m_1)\cdot\varphi(m_2)$.

<u>הוכחה</u>: נגדיר: $\psi_1:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m_1\mathbb{Z}$ על ידי $\psi_1(x+m\mathbb{Z})=x+m_1\mathbb{Z}$. זה מוגדר היטב: אם $x+m\mathbb{Z}=y+m\mathbb{Z}$, אזי $m|x-y$, ומכיוון ש- $m_1|m$, אזי $m_1|x-y$, ולכן $x+m_1\mathbb{Z}=y+m_1\mathbb{Z}$. אזי $\psi_1(\bar{x}+\bar{y})=\psi_1(\bar{x})+\psi_1(\bar{y})$ וגם $\psi_1(\bar{x}\cdot\bar{y})=\psi_1(\bar{x})\cdot\psi_1(\bar{y})$ ו- $\psi(\bar{1})=\bar{1}$.

נגדיר: $\psi_2:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m_2\mathbb{Z}$ על ידי $\psi_2(x+m\mathbb{Z})=x+m_2\mathbb{Z}$. אותן התכונות של ψ_1 מתקיימות גם על ψ_2.

נגדיר: $\psi:\mathbb{Z}/m\mathbb{Z}\to\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}$ על ידי $\psi(\bar{x})=(\psi_1(\bar{x}),\psi_2(\bar{x}))$. אזי ψ חח"ע ועל, כי יצרנו כאן מערכת של קונגרואנציות, וזה נובע ישירות ממשפט השאריות הסיני.

נגדיר פעולות חיבור וכפל בקבוצה $\mathbb{Z}/m_1\mathbb{Z}\times\mathbb{Z}/m_2\mathbb{Z}$ לפי הקואורדינטות: $(x_1,y_1)+(x_2,y_2)=(x_1+x_2,y_1+y_2)$ ו- $(x_1,y_1)\cdot(x_2,y_2)=(x_1\cdot x_2,y_1\cdot y_2)$. איבר היחידה: $1=(1,1)$.

אזי נובע ישירות מההגדרות כי $\psi(x+y)=\psi(x)+\psi(y)$ ו- $\psi(x\cdot y)=\psi(x)\cdot\psi(y)$.

אזי ההעתקה שיצרנו מגדירה העתקה חח"ע ועל $U(\mathbb{Z}/m\mathbb{Z})\to U(\mathbb{Z}/m_1\mathbb{Z})\times U(\mathbb{Z}/m_2\mathbb{Z})$. נוכיח:

- נוכיח שההעתקה היא $U(\mathbb{Z}/m\mathbb{Z})\to U(\mathbb{Z}/m_1\mathbb{Z})\times U(\mathbb{Z}/m_2\mathbb{Z})$: יהי $u\in\mathbb{Z}/m\mathbb{Z}$. לכן, קיים $v\in\mathbb{Z}/m\mathbb{Z}$ כך ש- $uv=1$. אזי: $\psi_1(u)\cdot\psi_1(v)=\psi_1(u\cdot v)=\psi_1(1)=1$, ולכן $\psi_1(u)$ הפיך, כלומר $\psi_1(u)\in U(\mathbb{Z}/m_1\mathbb{Z})$. באופן דומה: $\psi_2(u)\cdot\psi_2(v)=\psi_2(u\cdot v)=\psi_2(1)=1$, ולכן גם $\psi_2(u)$ הפיך, כלומר $\psi_2(u)\in U(\mathbb{Z}/m_2\mathbb{Z})$. לכן: $\psi(u)=(\psi_1(u),\psi_2(u))\in U(\mathbb{Z}/m_1\mathbb{Z})\times U(\mathbb{Z}/m_2\mathbb{Z})$. לכן, ההעתקה היא אכן $U(\mathbb{Z}/m\mathbb{Z})\to U(\mathbb{Z}/m_1\mathbb{Z})\times U(\mathbb{Z}/m_2\mathbb{Z})$.
- ההעתקה היא חח"ע ב- $U(\mathbb{Z}/m\mathbb{Z})$ כי $U(\mathbb{Z}/m\mathbb{Z})\subseteq\mathbb{Z}/m\mathbb{Z}$, וההעתקה היא חח"ע ב- $\mathbb{Z}/m\mathbb{Z}$.
- נוכיח שההעתקה היא על: יהיו $u_1\in U(\mathbb{Z}/m_1\mathbb{Z})$, $u_2\in U(\mathbb{Z}/m_2\mathbb{Z})$. לכן, קיימים $v_1\in\mathbb{Z}/m_1\mathbb{Z},v_2\in\mathbb{Z}/m_2\mathbb{Z}$ כך ש- $u_1v_1=1,u_2v_2=1$. לפי משפט השאריות הסיני, קיימים $u,v\in\mathbb{Z}/m\mathbb{Z}$ כך ש- $\psi_1(u)=u_1$, $\psi_2(u)=u_2$, $\psi_1(v)=v_1$, $\psi_2(v)=v_2$. לכן, $\psi_1(uv)=\psi_1(u)\psi_1(v)=u_1v_1=1$, $\psi_2(uv)=\psi_2(u)\psi_2(v)=u_2v_2=1$. אבל $\psi_1(1)=1=\psi_1(uv)$ ו- $\psi_2(1)=1=\psi_2(uv)$. לפי המשפט הסיני, יש יחידות, ולכן $uv=1$, ולכן u הפיך, כלומר $u\in U(\mathbb{Z}/m\mathbb{Z})$.

לכן: $\#U(\mathbb{Z}/m\mathbb{Z})=\#U(\mathbb{Z}/m_1\mathbb{Z})\cdot\#U(\mathbb{Z}/m_2\mathbb{Z})$. לכן, $\varphi(m_1\cdot m_2)=\varphi(m_1)\cdot\varphi(m_2)$. מש"ל.

<u>משפט</u>: אם $n=p_1^{l_1}\cdot\ldots\cdot p_r^{l_r}$ אז $\varphi(n)=\prod_{i=1}^{r}(p_i-1)p_i^{l_i-1}=n\cdot\prod_{i=1}^{r}\left(1-\frac{1}{p_i}\right)$.

<u>הוכחה</u>: מהטענה הקודמת, מספיק להוכיח למקרה שבו $n=p^l$, כי ככה אפשר להכפיל את הכל (כי p_i ראשוניים). לפי ההגדרה: $\varphi(p^l)=\#\{0\leq a<p^l | p^l\text{ זר ל- } a\}$, כלומר $\varphi(p^l)=\#\{0\leq a<p^l | p\text{ זר ל- } a\}$. מכיוון ש-$p$ ראשוני, המספרים שאינם זרים ל-p הם: $0,p,2p,\ldots,p^l-p$. יש p^{l-1} מספרים כאלה. לכן, יש p^l-p^{l-1} מספרים זרים ל-p בקטע $[p,p^l)\subseteq\mathbb{Z}$. אבל $p^l-p^{l-1}=(p-1)p^{l-1}=p^l\left(1-\frac{1}{p}\right)$. מש"ל.

<u>דוגמה</u>: $18=2\cdot 3^2 \Rightarrow \varphi(18)=\varphi(2)\cdot\varphi(3^2)=(2-1)(3-1)\cdot 3=6$.

<u>הגדרה</u>: קבוצה G תקרא **חבורה** (באנגלית: *group*, בצרפתית: *group*, בגרמנית: *gruppe*, ברוסית: *Группа*) אם יש לה פעולה אחת $x,y\mapsto xy$ כך שמתקיימים:

1. אסוציאטיביות: $\forall x,y,z\in G.(xy)z=x(yz)$.
2. קיום איבר ניטרלי: $\exists e\in G.\forall x\in G.ex=x=xe$.
3. קיום איבר נגדי: $\forall x\in G.\exists x'\in G.xx'=x'x=e$.
4. G תקרא **חבורה אבלית** אם גם מתקיימת קומוטטיביות: $\forall x,y\in G.xy=yx$.

<u>דוגמאות</u>:

1. $(\mathbb{Z},+)$, כלומר $x,y\mapsto x+y$ עם $e=0$, $x'=-x$.

<u>הערה</u>: בשפה כפלית, $x'=x^{-1}$.

2. $(\mathbb{Z}/m\mathbb{Z},\cdot)$.
3. $(\{1,-1\},\cdot)$.
4. אם R חוג, אז $(R,+)$ חבורה.
5. אם $R^\times=U(R)$, אז $(R^\times,\cdot)$ חבורה. עבור $u\in R^\times$, קיים u' כך ש- $uu'=1 \Leftarrow u'u=1 \Leftarrow u'\in R^\times$. עבור $u,v\in R^\times$, נבדוק ש-$u,v\mapsto u\cdot v$ מוגדר: קיימים $u',v'\in R^\times$ כך ש- $uu'=1, vv'=1$. אזי $(uv)(v'u')=u(vv')u'=uu'=1 \Leftarrow u\cdot v\in R^\times$. לכן, $(R^\times,\cdot)$ חבורה.

<u>הגדרה</u>: אם G_1,G_2 חבורות, אז $G_1\times G_2$ חבורה:

1. $(x_1,y_1)(x_2,y_2)=(x_1x_2,y_1y_2)$.
2. $e_{G_1\times G_2}=(e_{G_1},e_{G_2})$.

<u>הגדרה</u>: אם G_1,G_2 חבורות, $\psi:G_1\to G_2$ תקרא **הומומורפיזם** של חבורות, אם $\psi(xy)=\psi(x)\psi(y)$.

<u>תכונות של הומומורפיזם</u>: אם $\psi:G_1\to G_2$ הומומורפיזם, אזי:

1. $\psi(e_{G_1})=e_{G_2}$.
2. $\psi(x^{-1})=\psi(x)^{-1}$.

<u>הגדרה</u>: הומומורפיזם של חבורות $\psi:G_1\to G_2$ יקרא **איזומורפיזם** של חבורות אם הוא חח"ע ועל.

<u>דוגמאות</u>:

1. $G_1=\mathbb{Z}$, $G_2=\{1,-1\}$, $\psi(n)=(-1)^n$, כי $(-1)^{n_1+n_2}=(-1)^{n_1}\cdot(-1)^{n_2}$.
2. אם G חבורה, $x\in G$ איבר, אזי $\mathbb{Z}\to G$, $n\mapsto x^n$ הומומורפיזם של חבורות, כי $x^{n_1+n_2}=x^{n_1}x^{n_2}$.
3. דוגמה לאיזומורפיזם של חבורות: $(\mathbb{Z}/2\mathbb{Z},+)\to(\{-1,1\},\cdot)$, $n+2\mathbb{Z}\mapsto(-1)^n$ איזומורפיזם, כי $\bar{0}\mapsto 1$, $\bar{1}\mapsto -1$.
4. אם $m=m_1\cdot m_2$ ו- $\gcd(m_1,m_2)=1$, אז $U(\mathbb{Z}/m\mathbb{Z})\tilde{\to}U(\mathbb{Z}/m_1\mathbb{Z})\times(\mathbb{Z}/m_2\mathbb{Z})$ איזומורפיזם של חבורות.

<u>הגדרה</u>: חבורה G נקראת **חבורה סופית** אם היא סופית.

<u>הגדרה</u>: חבורה G נקראת **חבורה ציקלית** אם יש איבר $x_0\in G$ כך שהקבוצה $\{x_0^n | n\in\mathbb{Z}\}$ היא כל החבורה. x_0 נקרא **יוצר** של G.

דוגמאות:

1. $\mathbb{Z}$ ציקלית, כי $1^n=n\cdot1$.
2. $\mathbb{Z}/m\mathbb{Z}$ ציקלית, למשל ±1 יוצרים.

הגדרה: **שורש פרימיטיבי** *(ש"פ)* מודולו m הוא מספר $a\in\mathbb{Z}$ כך ש- a זר ל- m ו- $a+m\mathbb{Z}$ הוא יוצר של $U(\mathbb{Z}/m\mathbb{Z})$.

דוגמאות:

1. 3 שורש פרימיטיבי מודולו 7, 2 לא.
2. אם $m=8$ אזי $1,3,5,7$ הם ש"פ: $7^2\equiv5^2\equiv3^2\equiv1(8)$.

למה (חוק הצמצום): אם $ax=bx$ אזי $a=b$.

הוכחה: קיים $x^{-1}\in G$ ואז: $ax=bx \Rightarrow (ax)x^{-1}=(bx)x^{-1} \Rightarrow a(xx^{-1})=b(xx^{-1}) \Rightarrow ae=be \Rightarrow a=b$. מש"ל.

הערה: בחוג, חוק הצמצום לא בהכרח עובד. למשל, ב- $\mathbb{Z}/6\mathbb{Z}$: $\bar0=\bar2\cdot\bar3=\bar4\cdot\bar3=\bar0$, אבל $\bar2\neq\bar4$.

טענה: תהי G חבורה אבלית סופית מסדר (מגודל) n. יהי $a\in G$ יוצר. אזי $a^n=e$.

הוכחה: נסמן: $G=g_1,g_2,\dots,g_n$, ואז $ag_1,\dots,ag_n$ שונים זה מזה (כי a יוצר), ולכן $\{ag_1,\dots,ag_n\}=\{g_1,\dots,g_n\} \Rightarrow ag_1\cdot\ldots\cdot ag_n=g_1\cdot\ldots\cdot g_n \Rightarrow a^n\cdot g_1\cdot\ldots\cdot g_n=g_1\cdot\ldots\cdot g_n$ (כי G אבלית) $\Rightarrow a^n=e$. מש"ל.

משפט אוילר (*Euler*): יהי $1<m\in\mathbb{Z}$. אם $a\in\mathbb{Z}$ וגם $\gcd(a,m)=1$ אז $a^{\varphi(m)}\equiv1(m)$.

הוכחה: $U(\mathbb{Z}/m\mathbb{Z})$ הוא חבורה מגודל $\varphi(m)$. אם $\bar a=a+m\mathbb{Z}$ ו- $\bar a\in U(\mathbb{Z}/m\mathbb{Z})$, אזי לפי תורת החבורות, $\bar a^{\varphi(m)}=\bar1$, ולכן $a^{\varphi(m)}\equiv1(m)$. מש"ל.

הוכחה אחרת: a זר ל- m $\Rightarrow \bar a\in U(\mathbb{Z}/m\mathbb{Z}) \Rightarrow \bar a^{\varphi(m)}=\bar1^{\varphi(m)} \Rightarrow a^{\varphi(m)}\equiv1(m)$. מש"ל.

משפט פרמה (*Fermat*) הקטן: יהי $p\in\mathbb{Z}$ ראשוני. אם $p\nmid a$ אז $a^{p-1}\equiv1(p)$.

הוכחה: ניקח $m=p$, ואז $\gcd(a,m)=1$ כי $p\nmid a$, ומכיוון ש- $\varphi(p)=p-1$, אז $a^{p-1}\equiv1(p)$. מש"ל.

פרמה כתב את המשפט במכתב, אבל לא פרסם והוכיח אותו. את ההוכחה כתב ופרסם אוילר – *Euler*.

דוגמאות:

1. $a=2$, $p=7$, ואז: $2^{7-1}\equiv2^6\equiv64\equiv1(7)$, $3^{7-1}\equiv3^6\equiv729\equiv1(7)$, $4^6\equiv(-3)^6\equiv3^6\equiv1(7)$, $5^6\equiv(-2)^6\equiv2^6\equiv1(7)$.
2. $p=11$, $5^{38}\equiv?(11)$. לפי פרמה: $5^{10}\equiv1(11)$, $5^{30}\equiv1^3\equiv1(11)$, $5^2\equiv25\equiv3(11)$, $5^4\equiv3^2\equiv-2(11)$, $5^8\equiv(-2)^2\equiv4(11)$, ולכן $5^{38}\equiv(5^{10})^3\cdot5^8\equiv1^4\cdot4\equiv4(11)$.

טענה: אם $\gcd(a,m)=1$ ו- $a^{m-1}\not\equiv1(m)$ אז m מורכב.

הוכחה: זאת בדיוק השלילה של משפט פרמה הקטן. מש"ל.

דוגמה: $m=117$, $a=2$: $a^{116}\equiv?(117)$. $2^7\equiv128\equiv11(117)$, $2^{14}\equiv121\equiv4(117)$, $116=14\cdot8+4$ $\Rightarrow 2^{116}\equiv4^8\cdot2^4\equiv2^{16}\cdot2^4\equiv4\cdot2^{14}\cdot2^4\equiv4\cdot4\cdot2^4\equiv2\cdot2^7\equiv2\cdot11\equiv22(117)$. לכן, 117 מורכב.

הגדרה: אם G חבורה ו- $x\in G$, אזי **הסדר** שמסומן ב- $\operatorname{ord}x$ הוא $0<k\in\mathbb{Z}$ הקטן ביותר כך ש- $x^k=e$.

דוגמאות:

1. $(G=\mathbb{Z}/6\mathbb{Z},+)$. אזי $\operatorname{ord}\bar3=2$ כי $\bar3+\bar3=\bar0$. כמו כן, $\operatorname{ord}\bar2=3$ כי $\bar2\neq\bar0$, $\bar2+\bar2\neq\bar0$, $\bar2+\bar2+\bar2=\bar0$.
2. $(U(\mathbb{Z}/8\mathbb{Z}),\cdot)$. אזי $\operatorname{ord}\bar1=1$ כי $\bar1=\bar1$ ו- $\operatorname{ord}\bar3=2$ כי $\bar3\cdot\bar3=\bar9=\bar1$. $\operatorname{ord}\bar5=2$ כי $\bar5\cdot\bar5=\bar1$. $\operatorname{ord}\bar7=2$ כי $\bar7\cdot\bar7=$ .2 $\#U(\mathbb{Z}/8\mathbb{Z})=4$.

למה: תהי G חבורה, $x\in G$. נסמן: $k=\operatorname{ord}x$. נניח ש- $x^m=e$. אזי $k|m$.

הוכחה: נסמן: $m=q\cdot k+r$ כאשר $0\le r<k$. אזי $x^m=x^{qk+r}=(x^k)^q\cdot x^r=e^q\cdot x^r=e$. מכיוון ש- $x^m=e$, אנו רואים ש- $x^r=e$. אבל $0\le r<k$. אם $r\neq0$, זו סתירה, כי k מינימלי. לכן, $r=0 \Rightarrow m=kq \Rightarrow k|m$. מש"ל.

מסקנה: אם G חבורה אבלית סופית ו- $\#G=n$ אזי לכל $x\in G$ מתקיים $\operatorname{ord}x|n$.

הוכחה: אמנם $x^n=e$. לכן, לפי הלמה, $\operatorname{ord}x|n$. מש"ל.

דוגמה: ב- $(\mathbb{Z}/6\mathbb{Z},+)$ אין איבר מסדר 4, כי $4\nmid6$.

<u>הגדרה:</u> אם G חבורה, $x\in G$, נגדיר את **החבורה הנוצרת** על ידי x על ידי $\langle x\rangle=\{x^n | n\in\mathbb{Z}\}$, כאשר $x^{-n}=(x^n)^{-1}$.

<u>למה:</u> אם $\operatorname{ord} x=k<\infty$ אזי $\langle x\rangle=\{e,x,x^2,\dots,x^{k-1}\}$.

<u>הוכחה:</u>

1. יהיו $0\le i,j<k$. נניח ש- $x^i=x^j$. צ"ל: $i=j$. נניח ש- $i>j$. אזי $x^j\cdot x^{i-j}=x^i=x^j \Leftarrow x^{i-j}=e$. מכיוון ש- $i-j<k$ נקבל $i-j=0 \Leftarrow i=j$.
2. יהי $y\in\langle x\rangle$. אזי $y=x^n$. נסמן: $n=qk+r$, כאשר $0\le r<k$. אזי: $y=x^n=x^{qk+r}=(x^k)^q\cdot x^r=e^q\cdot x^r=x^r$. לכן, אלה כל האיברים של $\langle x\rangle$.

מש"ל.

<u>הגדרה:</u> אם G חבורה ו- $x\in G$, אומרים ש- x **יוצר** של G אם $\langle x\rangle=G$.

<u>הערה:</u> אם G חבורה סופית, $\# G=m$ ו- $x\in G$ כך ש- $\operatorname{ord} x=m$, אז x הוא יוצר של G. ואומנם, $\#\langle x\rangle=m$, ולכן $\langle x\rangle=G$. אם $\operatorname{ord} x<m$, אזי $\langle x\rangle\ne G$.

<u>דוגמה:</u>

1. ב- $(U(\mathbb{Z}/5\mathbb{Z}),\cdot)$: $\operatorname{ord}\bar{4}=2$, ולכן $\bar{4}$ לא יוצר. $\operatorname{ord}\bar{2}=4$, ולכן $\bar{2}$ יוצר. גם $\operatorname{ord}\bar{3}=4$, כי $\bar{3}=\overline{(-2)}$, ולכן $\bar{3}$ יוצר.
2. $(U(\mathbb{Z}/8\mathbb{Z}),\cdot)$: $\operatorname{ord}\bar{1}=1$, $\operatorname{ord}\bar{3}=2$, $\operatorname{ord}\bar{5}=2$, $\operatorname{ord}\bar{7}=2$. לכן, אין יוצרים בחבורה הזאת.

פולינומים

<u>הגדרה:</u> יהי k שדה. נגדיר: $k[X]=\{a_0+a_1X^1+\dots+a_nX^n | \forall i.\, a_i\in k, n\in\mathbb{N}\}$ להיות **חוג הפולינומים** מעל k.

<u>דוגמה:</u> $k=\mathbb{F}_2$, $f(X)=X$, $g(X)=X^2$. אזי:

x	$\bar{0}$	$\bar{1}$
$f(x)$	$\bar{0}$	$\bar{1}$
$g(x)$	$\bar{0}$	$\bar{1}$

<u>הגדרה:</u> **פולינום** מעל שדה k הוא סכום פורמלי של מקדמים: $f(X)=a_0+a_1X+\dots+a_nX^n$.

<u>הגדרה:</u> אם $f(X)=\sum a_iX^i$ ו- $g(X)=\sum b_iX^i$ אזי **המכפלה** שלהם: $f(X)g(X)=\sum c_lX^l$ כאשר $c_l=\sum_{i+j=l} a_ib_j$.

<u>למה:</u> אם $a\in k$ אז $(f,g)(a)=f(a)g(a)$.

<u>דוגמה:</u> $k=\mathbb{F}_p$: הפולינום X^p-X הוא 0, לפי משפט פרמה, כי $X^p-X=X(X^{p-1}-1)$.

ב- $k\in[X]$, פולינום האפס: 0. פולינום היחידה: 1.

<u>הגדרה:</u> יהי A חוג, ויהיו $a,b\in A$. אזי a **מחלק** את b ומסמנים $a|b$ אם קיים $c\in A$ כך ש- $ac=b$.

<u>הגדרה:</u> יהי A חוג. אזי $U(A)=A^X=\{a\in A | a|1\}$.

<u>הגדרה:</u> אם $f(X)=a_0+a_1X+\dots+a_nX^n$ ו- $a_n\ne 0$, אזי **המעלה** של f היא n. מסמנים: $\deg f=n$. כמו כן, $\deg 0$ לא מוגדר.

<u>תכונות:</u>

1. $\deg(fg)=\deg f+\deg g$.
2. $\deg(f+g)\le max(\deg f,\deg g)$.

אזי: $k[X]^X=k^X$.

<u>הגדרה:</u> חוג A נקרא **תחום שלמות** אם אין ב- A מחלקי אפס.

$k[X]$ תחום שלמות, כי אם $0\ne f,g\in k[X]$ אזי $\deg(f,g)=\deg f+\deg g$, ולכן $fg\ne 0$. לכן, אין מחלקי אפס ב- $k[X]$.

<u>טענה:</u> בתחום שלמות יש חוק צמצום: יהי A תחום שלמות, ויהיו $a,b,c\in A$. נניח ש- $ac=bc$ ו- $c\ne 0$. אזי $a=b$.

<u>הוכחה:</u> $ac=bc \Leftarrow (a-b)c=0$. $c\ne 0$, ולכן אינו מחלק אפס $\Leftarrow a-b=0 \Leftarrow a=b$. מש"ל.

<u>הגדרה</u>: אם $f(X)=a_0+a_1X+\ldots+a_nX^n$, ו- $a_n\neq 0$, אזי a_n נקרא **המקדם העליון**. אם $a_n=1$, אזי f נקרא **מתוקן** ($monic$).

<u>דוגמה</u>: $2X-1$ אינו מתוקן, $X-\frac{1}{2}$ מתוקן, כאשר $k=\mathbb{Q}$.

<u>הגדרה</u>: אם $f(X)=a_0$, אזי f נקרא **קבוע**.

<u>הגדרה</u>: פולינום לא קבוע f נקרא **אי פריק** אם לכל פירוק $f=gh$, g הפיך או h הפיך.

<u>דוגמאות</u>: $X-1$ אי פריק, X^2-1 פריק, X^2+1 – תלוי בשדה. למשל, ב- $\mathbb{F}_2$: $(X+1)(X+1)=X^2+2X+1=X^2+1$.

<u>למה</u>: כל פולינום לא קבוע הוא מכפלה של פולינומים אי פריקים.

<u>הוכחה</u>: באונדוקציה על דרגת הפולינום:

בסיס - $\deg f=1$: הפולינום f הוא מהצורה a_0+a_1X, ולכן אינו פריק בעצמו.

מעבר – נניח שהלמה נכונה עבור $\deg f<n$, ונוכיח עבור $\deg f=n$: נניח כי $\deg f=n$. אם f אי פריק, אז סיימנו. נניח כי f פריק. אזי קיימים פולינומים g,h כך ש- $f=g\cdot h$. לכן, $\deg g,\deg h<\deg f=n$, ולכן לפי הנחת האינדוקציה, g ו- h הם מכפלה של פולינומים אי פריקים, ולכן גם f הוא מכפלה של פולינומים אי פריקים.

מש"ל.

<u>הגדרה</u>: יהי p פולינום אי פריק. **הסדר** של פולינום f על p הוא a (ומסמנים $a=\operatorname{ord}_p f$) אם $0\leq a\in\mathbb{Z}$ כך ש- $p^a|f$ ו- $p^{a+1}\nmid f$. קיים a כזה בהכרח, כי $p^0|f$ ו- $p^{\deg f+1}\nmid f$.

<u>למה</u>: יהיו $f,g\in k[X]$. נניח ש- $g\neq 0$. אזי קיימים $q,r\in k[X]$ כך ש- $f=gq+r$ כך ש- $\deg r<\deg g$ או $r=0$.

<u>הוכחה</u>: נניח $f\neq 0$. נסמן: $f(X)=a_nX^n+\ldots+a_0$, $g(X)=b_mX^m+\ldots+b_0$, כאשר $a_n\neq 0$ ו- $b_m\neq 0$. אזי $n=\deg f$ ו- $m=\deg g$. נוכיח באינדוקציה על n:

בסיס – $n=0$: כלומר, $\deg f=0$. אם $\deg g>0=\deg f$, אז לוקחים $q=0$ ו- $r=f$. אם $\deg g=0$, אז $r=0$ ו- $q=\frac{a_0}{b_0}$.

מעבר – $n-1\to n$: נניח ש- $n>0$, ונניח שהוכחנו עבור $\deg f\leq n-1$. נניח ש- $\deg f=n$. אם $\deg g>n$, אז לוקחים $q=0$, $r=f$. אם $\deg g\leq n$, אז $f(X)=\frac{a_n}{b_m}X^{n-m}\cdot g(X)+d_1(X)$. אזי $\deg\frac{a_n}{b_m}X^{n-m}\cdot g(X)=n$, ולכן $\deg f_1\leq n$. לפי הנחת האינדוקציה, $f(X)=\frac{a_n}{b_m}\cdot X^{n-m}g(X)+q_1(X)g(X)+r(X)$ כאשר $\deg r<\deg g$ או $r=0$. נגדיר: $q(x)=\frac{a_n}{b_m}X^{n-m}+q_1(X)$, ואז $f(X)=q(X)g(X)+r(X)$, כאשר $\deg r<\deg g$ או $r=0$.

מש"ל.

<u>דוגמה</u>: $k=\mathbb{Q}$, $f(X)=2X^3+7X^2-5$, $g(X)=X-1$. נבצע חילוק ארוך:

$$
\begin{array}{rrrrrrr|l}
2X^2 & + & 9X & + & 9 & & & \\
\hline
2X^3 & + & 7X^2 & + & 0X & - & 5 & X-1 \\
\cline{8-8}
2X^3 & - & 2X^2 & & & & & \\
\cline{1-3}
 & & 9X^2 & + & 0X & - & 5 & \\
 & & 9X^2 & - & 9X & & & \\
\cline{3-5}
 & & & & 9X & - & 5 & \\
 & & & & 9X & - & 9 & \\
\cline{5-7}
 & & & & & & 4 &
\end{array}
$$

לכן: $2X^3+7X^2-5=(2X^2+9X+9)(X-1)+4$.

<u>הגדרה</u>: אם $0\neq f,g\in k[X]$, אזי $d(X)$ נקרא **מחלק משותף מקסימלי** של f,g אם $d|f$, $d|g$ ולכל c שמקיים $c|f$, $c|g$ מתקיים $c|d$. מסמנים: $\gcd(f,g)$ - המחלק המשותף המקסימלי המתוקן של f,g.
ניתן להשתמש באלגוריתם אוקלידס כדי לחשב את מחלק משותף מקסימלי של פולינומים, ולכתוב $\gcd(f,g)(X)=a(X)f(X)+b(X)g(X)$.
<u>הגדרה</u>: יהי A תחום שלמות, ויהיו $0\neq a,b\in A$. אזי a,b **שקולים** אם $a=ub$ כאשר u הפיך.
<u>טענה</u>: יהיו $a,b\in A$. אם c,d שני מחלקים משותפים מקסימליים, אזי c,d שקולים.
<u>הוכחה</u>: $c|d \Leftarrow \exists s.d=sc$. מצד שני, $d|c \Leftarrow \exists t.c=td \Leftarrow c=tsc \Leftarrow c\cdot(1-ts)=0$. אבל $c\neq0$, ולכן $1-ts=0$. לכן, s,t הפיכים $\Leftarrow c$ שקול ל-d. מש"ל.
<u>דוגמה</u>: $A=k[X]$ ו-$f,g\in k[X]$. אם h,h' מחלקים משותפים מקסימליים, אזי $h=ch'$ כאשר $c\in k^X$.
לכן, מגדירים את $\gcd(f,g)$ להיות המתוקן.
<u>הגדרה</u>: $f,g\in k[X]$ **זרים** אם $\gcd(f,g)=1$.
<u>טענה</u>: אם f,g זרים ו-$f|gh$, אזי $f|h$.
<u>הוכחה</u>: $lf+mg=1 \Leftarrow lfh+mgh=h$. מש"ל.
<u>מסקנה</u>: אם $p\in k[X]$ מתוקן אי פריק ו-$p|gh$ אזי $p|g$ או $p|h$.
<u>הוכחה</u>: $\gcd(p,g)\in\{1,p\}$. אם $\gcd(p,g)=p$, אז $p|g$. אם $\gcd(p,g)=p$, אז p זר ל-g, ולפי הטענה, $p|h$. מש"ל.
<u>מסקנה</u>: אם p מתוקן ואי פריק, $0\neq f,g\in k[X]$, אז $\mathrm{ord}_p(fg)=\mathrm{ord}_p f+\mathrm{ord}_p g$.
<u>משפט</u>: יהי $0\neq f\in k[X]$. ניתן לכתוב $f=c\cdot\prod_p p^{a(p)}$ כאשר p פולינומים אי פריקים מתוקנים, $0\leq a(p)\in\mathbb{Z}$ ו-$c\in k^X$. אזי c ו-$a(p)$ נקבעים באופן יחיד על ידי f. כלומר, $a(p)=\mathrm{ord}_p f$.
<u>הוכחה</u>: יהי q אי פריק ומתוקן. אזי: $\mathrm{ord}_q f=\underbrace{\mathrm{ord}_q c}_{0}+\sum_p a(p)\cdot\mathrm{ord}\, q_p=a(q)$. מש"ל.
<u>הגדרה</u>: חבורות G,G' נקראות **איזומורפיות** אם יש איזומורפיזם $G\to G'$.
אם $m=m_1\cdot\ldots\cdot m_l$ ו-$\gcd(m_i,m_j)=1$ עבור $i\neq j$, אזי $\prod_{i=1}^{l}U(\mathbb{Z}/m_i\mathbb{Z})\underset{\text{איזומורפי}}{\simeq}U(\mathbb{Z}/m\mathbb{Z})$. אם $m=p_1^{a_1}\cdot\ldots\cdot p_l^{a_l}$, אזי $\prod_{i=1}^{l}U(\mathbb{Z}/p_i^{a_i}\mathbb{Z})\simeq U(\mathbb{Z}/m\mathbb{Z})$. אם $m=p^a$, למה איזומורפית $U(\mathbb{Z}/p^a\mathbb{Z})$?
<u>הגדרה</u>: $a\in\mathbb{Z}$ **שורש פרימיטיבי** מודולו m אם $\bar{a}=a+m\mathbb{Z}$ יוצר של $(\mathbb{Z}/m\mathbb{Z})^X$.
דוגמה: 2 שורש פרימיטיבי של $\mathbb{Z}/5\mathbb{Z}$.
<u>למה</u>: יהיו k שדה ו-$f\in k[X]$. נניח ש-$f\neq0$ ו-$\deg f=n$. אזי ל-f יש לכל היותר n שורשים שונים.
<u>הוכחה</u>: באינדוקציה על n:
בסיס - $n=1$: ברור.
מעבר - $n-1\to n$: נניח השלמה נכונה עבור $n-1$. אם ל-f אין שורשים, סיימנו. אם $\alpha\in k$ שורש, אזי $f(X)=q(X)\cdot(X-\alpha)+r$ כאשר $r\in k$. נציב $X=\alpha$ ונקבל: $0=0+r \Leftarrow r=0 \Leftarrow (X-\alpha)|f$. כמו כן, $\deg q=n-1$. אם β שורש אחר של f כך ש-$\beta\neq\alpha$, אזי $0=q(\beta)\cdot(\beta-\alpha)$. מכיוון ש-$\beta\neq\alpha$, נקבל $q(\beta)=0$. לפי הנחת האינדוקציה, יש לכל היותר $n-1$ β-ות כאלה. מש"ל.
<u>מסקנה</u>: יהיו $f,g\in k[X]$ כך ש-$\deg f=\deg g=n$. אם $f(\alpha_i)=g(\alpha_i)$ עבור $n+1$ איברים שונים $\alpha_1,\ldots,\alpha_{n+1}\in k$, אזי $f=g$.
<u>הוכחה</u>: נסתכל על $f-g\in k[X]$. אזי $f-g=0$ או $f-g\neq0$, ואז $\deg(f-g)\leq n$. אזי לפולינום $f-g\neq0$ ממעלה לכל היותר n יש $n+1$ שורשים שונים, וזו סתירה! לכן, $f-g=0 \Leftarrow f=g$. מש"ל.
<u>טענה</u>: בחוג $\mathbb{F}_p$ מתקיים: $X^{p-1}-\bar{1}=(X-\bar{1})(X-\bar{2})\cdot\ldots\cdot(X-\overline{p-1})$.
<u>הוכחה</u>: נסמן: $f(X)=(X^{p-1}-\bar{1})-(X-\bar{1})\cdot\ldots\cdot(X-\overline{p-1})$. אזי $f=0$ או $\deg f\leq p-2$. לפי משפט פרמה הקטן, $\forall\bar{a}\in\mathbb{F}_p.f(\bar{a})=0$. לכן, ל-$f$ יש $p-1$ שורשים. לכן, $f=0$. מש"ל.
<u>מסקנה - משפט</u> <u>*Wilson*</u>: $(p-1)!\equiv-1(p)$.
<u>הוכחה</u>: אם $p=2$ אז $1!\equiv-1(2)$. אם $p\neq2$, ניקח $x=\bar{0}$, ואז:
$-\bar{1}=(-\bar{1})\cdot(-\bar{2})\cdot\ldots\cdot(-\overline{p-1})=(-1)^{p-1}\cdot(p-1)! \Leftarrow -1\equiv(p-1)!(p)$. מש"ל.

<u>דוגמה</u>: $p=5$, ואז $4!\equiv 24\equiv -1(5)$.
<u>הערה</u>: אם n מורכב, $n>4$, אזי $(n-1)!\equiv 0(n)$.
<u>טענה</u>: אם $d|p-1$, אז לקונגרואנציה $x^q\equiv 1(p)$ יש בדיוק d פתרונות. באופן שקול: למשוואה $x^d=1$ יש בדיוק d פתרונות מעל $\mathbb{F}_p$.

<u>הוכחה</u>: נסמן: $dd'=p-1$ (כי $d|p-1$). נגדיר: $g(X)=\frac{X^{p-1}-1}{X^d-1}=\frac{(X^d)^{d'}-q}{X^d-1}=(X^d)^{d'-1}+\ldots+X^{d+1}$.
אזי $X^{p-1}-1=(X^d-1)g(X)$. לפי משפט פרמה הקטן, $x^{p-1}\equiv 1(p)$, ולכן לפולינום $X^{p-1}-1$ יש $p-1$ שורשים מעל $\mathbb{F}_p$. $\deg g=p-1-d$, ולכן ל- g יש לכל היותר $p-1-d$ שורשים. אבל ל- X^d-1 יש לכל היותר d שורשים, ולכן מכיוון שהכפל שלהם הוא $X^{p-1}-1$, יש ל- X^d-1 בדיוק d שורשים. מש"ל.
<u>משפט *Gauss-Gauß*</u>: עבור כל $n>1$ מתקיים $n=\sum_{d|n}\varphi(d)$.
<u>הוכחה</u>: לכל $0<d|n$ נגדיר: $S_d=\{m\in\mathbb{Z}|\gcd(m,n)=d\wedge 1\le m\le n\}$. אזי $\gcd(m,n)=d$ $\Leftrightarrow$ $\gcd\left(\frac{m}{d},\frac{n}{d}\right)=1$ $\Leftarrow$ $\#S_d=\#\left\{s\in\mathbb{Z}\middle|\gcd\left(s,\frac{n}{d}\right)=1,1\le s\le\frac{n}{d}\right\}$ $\Leftarrow$ $\{1,\ldots,n\}=\bigcup_{d|n}S_d$, כי לכל מספר ב- $\{1,\ldots,n\}$ יש מחלק משותף מקסימלי עם n . לכן, $n=\sum_{d|n}\varphi\left(\frac{n}{d}\right)$. אם d עבר על כל מחלקי של n , אז $\frac{n}{d}$ עובר על אותה קבוצה. לכן: $\sum_{d|n}\varphi\left(\frac{n}{d}\right)=\sum_{d|n}\varphi(d)$. מש"ל.
<u>דוגמה</u>: $n=10$ ו- $1,2,5,10$ מחלקים את 10 . ואז: $10=1+1+4+4=\varphi(1)+\varphi(2)+\varphi(5)+\varphi(10)$.
<u>משפט</u>: אם $d|p-1$ כאשר p ראשוני, אז יש ב- $U(\mathbb{Z}/p\mathbb{Z})$ בדיוק $\varphi(d)$ איברים מסדר d .
<u>הוכחה</u>: יהי $d|p-1$. נגדיר: $\psi(d)$ - מספר האיברים מסדר d . מכיוון ש- $\#U(\mathbb{Z}/p\mathbb{Z})=p-1$, נקבל כי $p-1=\sum_{d|p-1}\psi(d)$. אבל $p-1=\sum_{d|p-1}\varphi(d)$. נוכיח שלכל $d|p-1$ מתקיים $\psi(d)\le\varphi(d)$. יש שתי אפשרויות: אם $\psi(d)=0$, אזי ברור ש- $\psi(d)\le\varphi(d)$. אם $\psi(d)\ne 0$ אז יש איבר $x\in U(\mathbb{Z}/p\mathbb{Z})$ מסדר d . אזי $1,x,\ldots,x^{d-1}$ הם שונים. כל אחד מהם מקיים $x^d-\bar{1}=0$, כי $(x^k)^d=(x^d)^k=\bar{1}^k=\bar{1}$. קיבלנו d שורשים למשוואה $x^d-\bar{1}=0$, ולכן הם כל השורשים. אזי כל $y\in U(\mathbb{Z}/p\mathbb{Z})$ מסדר d הוא אחד מ- $1,x,\ldots,x^{d-1}$. אם $y=x^a$ כאשר $\gcd(a,d)=c>1$ אז $y^{\frac{d}{c}}=(x^a)^{\frac{d}{c}}=(x^d)^{\frac{a}{c}}=1^{\frac{a}{c}}=1$. לכן, אם $\operatorname{ord}y=d$ אז $y=x^a$ עם $\gcd(a,d)=1$. יש רק $\varphi(d)$ a -ים כאלה, ולכן $\psi(d)\le\varphi(d)$ גם במקרה $\psi(d)\ne 0$. מש"ל.
<u>מסקנה</u>: יש $\varphi(p-1)$ איברים מסדר $p-1$.
<u>למה</u>: תהי G חבורה, $x\in G$. נניח ש- $x^m=e$. נסמן: $m=p_1^{l_1}\cdot\ldots\cdot p_s^{l_s}$. נניח ש- $\forall i.x^{\frac{m}{p_i}}\ne e$. אז $\operatorname{ord}x=m$.
<u>הוכחה</u>: נסמן: $r=\operatorname{ord}x$. אזי $r|m$. נסמן: $r=p_1^{k_1}\cdot\ldots\cdot p_s^{k_s}$. נניח בשלילה ש- $r\ne m$. אזי $\exists i.k_i<l_i$. אזי $k_i\le l_i-1$. אזי $r|\frac{m}{p_i}$. אזי $x^{\frac{m}{p_i}}=e$. סתירה! מש"ל.
<u>דוגמה</u>: $p=19$. אזי $\varphi(19)=18$. המחלקים של 18 הם $1,2,3,6,9$. נבדוק: $2^2\equiv 4(19)$, $2^3\equiv 8(19)$, $2^6\equiv 64\equiv 8(19)$, $2^9\equiv 512\equiv -1(19)$, $2^{18}\equiv(2^9)^2\equiv 1(19)$. לכן, $\operatorname{ord}2=18$.
מתי יש שורש פרימיטיבי ל- m כללי? אם $m=p_1^{a_1}\cdot\ldots\cdot p_l^{a_l}$ אז $U(\mathbb{Z}/m\mathbb{Z})=U(\mathbb{Z}/p_1^{a_1}\mathbb{Z})\times\ldots\times U(\mathbb{Z}/p_l^{a_l}\mathbb{Z})$. לכן, מספיק לדעת איך מוצאים שורש פרימיטיבי בחבורות מהסוג $U(\mathbb{Z}/p^a\mathbb{Z})$ כאשר p ראשוני.
<u>הגדרה</u>: תהי G חברה. **תת חבורה** של G היא תת קבוצה לא ריקה $H\subseteq G$ כך שמתקיים:
1. $\forall x,y\in H.xy\in H$.
2. $\forall x\in H.x^{-1}\in H$. לכן, גם $e\in H$ בהכרח.

<u>דוגמאות:</u>

1. $G=(\mathbb{Z}/6\mathbb{Z},+)$, $H=(2\mathbb{Z}/6\mathbb{Z},+)$. אזי $H\subset G$ תת חבורה.
2. $2\mathbb{Z}\subset\mathbb{Z}$ עם $+$ היא תת חבורה.
3. דוגמה לא טריוויאלית: $G=U(\mathbb{Z}/p^l\mathbb{Z})$ עם $\cdot$, ו- $H=\bar{1}+p\mathbb{Z}/p^l\mathbb{Z}=\{1+pa | a\in\mathbb{Z}/p^l\mathbb{Z}\}\subset G$ כי $(\bar{1}+pa)^{-1}=1-pa+(pa)^2-(pa)^3+\ldots$. זה סכום סופי כי $p^l=\bar{0}\in\mathbb{Z}/p^l\mathbb{Z}$ וגם $(1+pa)(1-pa)^{-1}=1$. כמו כן, $(1+pa)(1+pb)=1+p(a+b+pab)$.

<u>למה:</u> אם p ראשוני ו- $1\le k\le p$ אז $p\left|\binom{p}{k}\right.$.

<u>הוכחה:</u> $\binom{p}{k}=\frac{p!}{k!\cdot(p-k)!}$ $\Leftarrow$ $p!=\binom{p}{k}\cdot k!\cdot(p-k)!$. $p|p!$ וגם $p\nmid k!$ ו- $p\nmid(p-k)!$ $\Leftarrow$ $p\left|\binom{p}{k}\right.$. מש"ל.

<u>למה:</u> אם $l\ge 1$ ו- $a\equiv b\,(p^l)$ אזי $a^p\equiv b^p\,(p^{l+1})$.

<u>הוכחה:</u> $a\equiv b\,(p^l)$ $\Leftarrow$ $a=b+cp^l$ $\Leftarrow$ $a^p=b^p+pb^{p-1}cp^l+A$ כאשר $A=\sum_{k=2}^{p}\binom{p}{k}c^kp^{lk}p^{b-k}$. $\forall k\ge 2.\,p^{2l}|p^{kj}$ $\Leftarrow$ $p^{2l}|A$ אבל $2k\ge l+1$ $\Leftarrow$ $p^{l+1}|A$. גם $p^{l+1}|pb^{p-1}cp^l$ $\Leftarrow$ $a^p\equiv b^p\,(p^{l+1})$. מש"ל.

<u>מסקנה:</u> אם $l\ge 2$ ו- $p\neq 2$ אזי $(1+ap)^{p^{l-2}}\equiv 1+ap^{l-1}\,(p^l)$ $\forall a\in\mathbb{Z}/$.

<u>הוכחה:</u> באינדוקציה על l :

בסיס – $l=2$: טריוויאלי.

נניח שזה נכון עבור $l\ge 2$. נוכיח עבור $l+1$. מהלמה, מכיוון ש- $(1+ap)^{p^{l-2}}\equiv 1+ap^{l-1}\,(p^l)$, אזי $(1+ap)^{p^{l-1}}\equiv((1+ap)^{l-2})^p\overset{\text{הנחת האינדוקציה}}{\equiv}(1+ap^{l-1})^p\,(p^{l+1})$. לפי נוסחת הבינום: $(1+ap^{l-1})^p=1+ap^l+B$ כאשר $B=\sum_{k=2}^{p}\binom{p}{k}a^kp^{k(l-1)}$. עבור $k\neq p$, המחובר מתחלק ב- $p\cdot p^{k(l-1)}=p^{k(l-1)+1}$, כלומר $p^{k(l-1)+1}\left|\binom{p}{k}\cdot a^kp^{k(l-1)}\right.$. אבל $k(l-1)+1\ge 2(l-1)+1=2k-1\ge l+1$. לכן, $p^{l-1}\left|\binom{p}{k}\cdot a^kp^{k(l-1)}\right.$ עבור $k\neq p$. המחובר האחרון מתחלק ב- $p^{p(l-1)}$, ו- $p(l-1)\ge 3(l-1)=l-1+2(l-1)\ge l-1+2=l+1$, כי $p\ge 3$. לכן, $p^{l+1}|B$. לכן, $(1+ap^{l-1})^p\equiv q+ap^l\,(p^{l+1})$. לכן, גם $(1+ap)^{p^{l-1}}\equiv 1+ap^l\,(p^{l+1})$. מש"ל.

<u>מסקנה:</u> אם $p\neq 2$ ו- $p\nmid a$ אזי הסדר של $1+ap$ מודולו p^l הוא p^{l-1} .

<u>הוכחה:</u> לפי המסקנה הקודמת, $(1+ap)^{p^{l-1}}\equiv 1+ap^l\,(p^{l+1})$ $\Leftarrow$ $(1+ap)^{p^{l-1}}\equiv 1\,(p^l)$ כי $(1+ap)^{p^{l-1}}=1+ap^l+cp^{l+1}$, ומתקיים $p^l|cp^{l+1}$, $p^l|ap^l$ $\Leftarrow$ $(1+ap)^{p^{l-1}}\equiv 1\,(p^l)$. אבל $(1+ap)^{p^{l-2}}\equiv 1+ap^{l-1}\,(p^l)$. מכיוון ש- $p\nmid a$, $(1+ap)^{p^{l-2}}\not\equiv 1\,(p^l)$ $\Leftarrow$ $\mathrm{ord}(1+ap)=p^{l-1}$. מש"ל.

<u>דוגמה:</u> $H=1+p\mathbb{Z}/p^l\mathbb{Z}\subset U(\mathbb{Z}/p^l\mathbb{Z})$: $\#H=p^{l-1}$, וגם יש יוצר $1+pa\in H$ מסדר p^{l-1} . לכן, H ציקלית.

<u>משפט:</u> אם $p\neq 2$ אז $U(\mathbb{Z}/p\mathbb{Z})$ היא ציקלית.

<u>הוכחה:</u> מכיוון ש- p ראשוני, יש שורש פרימיטיבי g מודולו p . אזי גם $g+p$ שורש פרימיטיבי מודולו p . נוכיח כי $g^{p-1}\not\equiv 1\,(p^2)$ או $(g+p)^{p-1}\not\equiv 1\,(p^2)$. נניח ש- $g^{p-1}\equiv 1\,(p^2)$. אזי $(g+p)^{p-1}\equiv g^{p-1}+(p-1)pg^{p-2}\,(p^2)$ (כי בכל שאר המחוברים יש p^2 $\Leftarrow$ מתאפסים). לפי ההנחה, $g^{p-1}\equiv 1\,(p^2)$, וגם $p-1\not\equiv 0\,(p^2)$, $p\not\equiv 0\,(p^2)$, $g^{p-2}\not\equiv 0\,(p^2)$ $\Leftarrow$ $(g+p)^{p-1}\not\equiv 1\,(p^2)$. נניח כי $g\in\mathbb{Z}$ שורש פרימיטיבי מודולו p כך ש- $g^{p-1}\not\equiv 1\,(p^2)$. נוכיח ש- g הוא שורש פרימיטיבי מודולו p^l לכל l . יהי $c\in\mathbb{Z}$ כך ש- $p\nmid c$. אזי קיים r כך ש- $g^r\equiv c\,(p)$. אזי $\frac{\bar{c}}{g^r}\in\mathbb{Z}/p^l\mathbb{Z}$. יהי $a\in\mathbb{Z}$. (כאן היה שקר כלשהו כי בורובוי מיהר...)

<u>משפט:</u> אם p אי זוגי ראשוני, נסתכל על $U(\mathbb{Z}/p^l\mathbb{Z})$. יהי $g\in\mathbb{Z}$ שורש פרימיטיבי מודולו p כך ש-$g^{p-1}\not\equiv 1(p^2)$. אזי g הוא שורש פרימיטיבי מודולו p^l לכל l.

<u>הוכחה:</u> יהי $\bar{c}\in U(\mathbb{Z}/p^l\mathbb{Z})$. נגדיר: $\bar{\bar{c}}=c+p\mathbb{Z}\in U(\mathbb{Z}/p\mathbb{Z})$. אזי $\exists r.\bar{\bar{c}}=\overline{\overline{g}}^r$, כלומר $c\equiv g^r(p)$. נסמן: $\bar{c}'=\frac{\bar{c}}{\bar{g}^r}\in U(\mathbb{Z}/p^l\mathbb{Z})$, כלומר $c'\equiv 1(p)$. g שורש פרימיטיבי מודולו p, ולכן $\gcd(g,p)=1$. לכן, $\gcd(g,p^l)=1$. לכן, $\bar{g}$ הפיך ב-$\mathbb{Z}/p^l\mathbb{Z}$. לפי משפט פרמה הקטן, $g^{p-1}\equiv 1(p)$ $\Leftarrow$ $g^{p-1}=1+pd$ כאשר $p\nmid d$, כי $g^{p-1}\not\equiv 1(p^2)$ $\Leftarrow$ $\bar{c}',\bar{g}^{p-1}\in 1+p\mathbb{Z}/p^l\mathbb{Z}$ $\Leftarrow$ $\bar{g}^{p-1}$ יוצר של החבורה $1+p\mathbb{Z}/p^l\mathbb{Z}$ מסדר p^{l-1} $\Leftarrow$ $\exists t\in\mathbb{Z}.c'\equiv(g^{p-1})^t(p^l)$. אבל $c\equiv c'g^r(p^l)$ $\Leftarrow$ $c\equiv g^{(p-1)t+r}(p^l)$. מש"ל.

<u>דוגמה:</u> $p=3$, $\varphi(3)=2$. 2 שורש פרימיטיבי מודולו 3, כי $2^2\equiv 1(p)$ ו-$2\not\equiv 1(p)$. אבל $2^2\equiv 4\not\equiv 1(9)$, ולכן 2 הוא שורש פרימיטיבי מודולו 3^l לכל l. עבור $l=3$: $3^3=27$, $\varphi(27)=18$. נראה שהסדר של 2 מודולו 27 הוא 18. צ"ל ש-$2^d\not\equiv 1(27)$ עבור $d\in\{1,2,3,6,9\}$. לא כדאי לבדוק עבור $d=2,3$ כי למשל $2^2\equiv 1(27)$ $\Leftarrow$ $2^6\equiv 1(27)$ (גם אם זה לא נכון). נבדוק עבור $d=6$: $2^6\equiv 64\equiv 10\not\equiv 1(27)$. עבור $d=9$: $2^9\equiv 512\equiv -1\not\equiv 1(27)$. לפי משפט אוילר, $2^{18}\equiv 1(27)$.

הוכחנו שאם $p>2$ ראשוני, ו-$m=p^l$, אזי $U(\mathbb{Z}/p^l\mathbb{Z})$ ציקלית.

<u>משפט:</u>
1. קיימים שורשים פרימיטיביים מודולו 2 ומודולו $4=2^2$, אבל לא מודולו 2^l עבור $l\geq 3$.
2. אם $l\geq 3$, אז 5 הוא מסדר 2^{l-2} מודולו 2^l. המספרים $(-1)^a 5^b$ כאשר $a\in\{0,1\}$, $0\leq b<2^{l-1}$ נותנים את כל השאריות ב-$U(\mathbb{Z}/2^l\mathbb{Z})$, כל שארית פעם אחת. לכן, עבור $l\geq 3$ יש איזומורפיזם $(\mathbb{Z}/2\mathbb{Z})\times(\mathbb{Z}/2^{l-2}\mathbb{Z})\to U(\mathbb{Z}/2^l\mathbb{Z})$.

<u>הוכחה:</u>
1. קל לראות.
2. נוכיח כי $5^{2^{l-3}}\overset{(1)}{\equiv}1+2^{l-1}(2^l)$ באינדוקציה על l:

בסיס - $l=3$: $5=1+3$.

מעבר - נניח שהוכחנו עבור איזשהו $l\geq 3$, ונוכיח עבור $l+1$. נחשב: $(1+2^{l-1})^2=1+2^l+2^{2l-2}$.

אבל $2l-2=l+l-2\geq l+1$ כי $l\geq 3$. מלמה קודמת, $(1+2^l)\overset{(2)}{\equiv}5^{2^{l-2}}\overset{(2)}{\equiv}(1+2^{p-1})^2(2^{l+1})$.

מש"ל אינדוקציה.

מ-(2) רואים ש-$5^{2^{l-2}}\equiv 1(2^l)$, ומ-(1): $1\not\equiv 5^{2^{l-3}}\equiv 1+2^{l-1}(2^l)$ $\Leftarrow$ $\mathrm{ord}_{2^l}5$ הוא מחלק של 2^{l-2}.

מכיוון ש-$\#U(\mathbb{Z}/2^l\mathbb{Z})=2^{l-1}$ ו-$\#U(\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2^{l-2}\mathbb{Z})=2\cdot 2^{l-2}=2^{l-1}$, מספיק להוכיח שקיימת פונקציה חח"ע, כי היא בהכרח גם תהיה על. נניח כי $(-1)^a 5^b\equiv(-1)^{a'}5^{b'}(2^l)$. אבל $5\equiv 1(4)$ $\Leftarrow$ $(-1)^a\equiv(-1)^{a'}(4)$ $\Leftarrow$ $a'\equiv a(2)$ $\Leftarrow$ $a'=a$ $\Leftarrow$ $5^b\equiv 5^{b'}(2^l)$ $\Leftarrow$ $5^{b-b'}\equiv 1(2^l)$ $\Leftarrow$ $\mathrm{ord}5|b-b'$ $\Leftarrow$ $2^{l-2}|b-b'$ $\Leftarrow$ $b\equiv b'(2^{l-2})$ $\Leftarrow$ $b=b'$.

מש"ל.

<u>דוגמאות:</u>
1. $U(\mathbb{Z}/8\mathbb{Z})=\{1,3,5,7\}$: $5^0\equiv 1(8)$, $5^1\equiv 5(8)$, $-5^0\equiv 7(8)$, $-5^1\equiv 3(8)$.
2. $U(\mathbb{Z}/16\mathbb{Z})$:

	5^0	5^1	5^2	5^3
+	1	5	9	13
−	15	11	7	3

<u>טענה</u>: יש שורש פרימיטיבי עבור 2 , 4 , $2p^l$ ($p>2$) ורק עבור המספרים האלה.
<u>הוכחה</u>: $U(\mathbb{Z}/2p^l\mathbb{Z})\simeq U(\mathbb{Z}/2\mathbb{Z})\times U(\mathbb{Z}/p^l\mathbb{Z})$ ו- $U(\mathbb{Z}/p^l\mathbb{Z})$ ציקלית. יהי g שורש פרימיטיבי מודולו p^l . אם הוא אי זוגי, הוא הפיך מודולו $2p^l$. אם g זוגי, לוקחים $g'=g+p^l$, ואז g' אי זוגי. אם m לא כזה, אז $m=m_1\cdot m_2$ כאשר $\gcd(m_1,m_2)=1$ ו- $m_1,m_2>2$. אזי $\varphi(m_1)$, $\varphi(m_2)$, $\varphi(m)=\varphi(m_1)\cdot\varphi(m_2)$ זוגיים. יהי $x\in U(\mathbb{Z}/m\mathbb{Z})$. נראה ש- $x^{\frac{\varphi(m)}{2}}\equiv 1(m)$. $U(\mathbb{Z}/m\mathbb{Z})\simeq U(\mathbb{Z}/m_1\mathbb{Z})\times U(\mathbb{Z}/m_2\mathbb{Z})$ $\Leftarrow$ אם $x_1\in U(\mathbb{Z}/m_1\mathbb{Z})$ אז $x_1^{\frac{\varphi(m)}{2}}\equiv\left(x_1^{\varphi(m_1)}\right)^{\frac{\varphi(m_2)}{2}}(m_1)$ ואם $x_2\in U(\mathbb{Z}/m_2\mathbb{Z})$ אז $x_2^{\frac{\varphi(m)}{2}}\equiv\left(x_2^{\varphi(m_2)}\right)^{\frac{\varphi(m_1)}{2}}(m_2)$, לפי משפט אוילר. לכן, בכל מקרה, $x^{\frac{\varphi(m)}{2}}\equiv 1(m)$, ולכן הוא לא שורש פרימיטיבי. מש"ל.
<u>דוגמה</u>: יש שורש פרימיטיבי עבור $2,4,7,49,3,9,18,14$, ואין עבור $21,35,8,16,12,20$.
סוף שיעור 9.
<u>משפט</u>: אם $n=2^a\cdot p_1^{a_1}\cdot\ldots\cdot p_l^{a_l}$ אזי $U(\mathbb{Z}/n\mathbb{Z})\simeq U(\mathbb{Z}/2^a\mathbb{Z})\times U(\mathbb{Z}/p_1^{a_1}\mathbb{Z})\times\ldots\times U(\mathbb{Z}/p_l^{a_l}\mathbb{Z})$, כאשר עבור $p_i>2$ החבורה $U(\mathbb{Z}/p_i^{a_i}\mathbb{Z})$ ציקלית, $U(\mathbb{Z}/2^a\mathbb{Z})$ ציקלית אם $a\in\{1,2\}$, או מכפלה ישרה של שתי חבורות ציקליות מסדרים 2 ו- 2^{a-2} עבור $a\geq 3$.

שארית מחזקת n

<u>הגדרה</u>: אם $1<m,n\in\mathbb{Z}$ ו- $a\in\mathbb{Z}$ ו- $\gcd(a,m)=1$, אז אומרים ש- a **שארית מחזקת n** (או *n^{th} power residue*) אם הקונגרואנציה $x^n\equiv a(m)$ ניתנת לפתרון.
<u>דוגמה</u>: מודולו 7 , 4 ריבוע, 3 לא.
<u>למה</u>: תהי G חבורה, $x\in G$ ו- $\operatorname{ord}x=n<\infty$. יהיו $a,b\in\mathbb{Z}$. אזי $x^a=x^b \Leftrightarrow a\equiv b(n)$.
<u>הוכחה</u>: אם $a\equiv b(n)$ אז $b=a+k\cdot n$ עבור $k\in\mathbb{Z}$. לכן $x^b=x^a\cdot(x^n)^k=x^a\cdot e^k=x^a$.
אם $x^a=x^b$ אז $x^{b-a}=e$, ולכן $n|b-a$ $\Leftarrow$ $a\equiv b(n)$.
מש"ל.
<u>טענה</u> (קריטריון *Euler* מוכלל): אם ל- m יש שורש פרימיטיבי ו- $\gcd(a,m)=1$ אז a הוא שארית מחזקת n $\Leftrightarrow$ $a^{\frac{\varphi(m)}{d}}\equiv 1(m)$ כאשר $d=\gcd(n,\varphi(m))$.
<u>הוכחה</u>: יהי g שורש פרימיטיבי מודולו m . אזי $a\equiv g^b(m)$. יהי $x\equiv g^y(m)$. אזי $x^n\equiv a(m)$ $\Leftrightarrow$ $g^{ny}\equiv g^b(m)$ $\Leftrightarrow$ $ny\equiv b(\varphi(m))$. נגדיר: $d=\gcd(n,\varphi(m))$. אזי יש פתרון $\Leftrightarrow$ $d|b$. אם $d|b$ אז $a^{\frac{\varphi(m)}{d}}\equiv g^{b\cdot\frac{\varphi(m)}{d}}\equiv\left(g^{\varphi(m)}\right)^{\frac{b}{d}}\equiv 1(m)$. בכיוון ההפוך: אם $a^{\frac{\varphi(m)}{d}}\equiv 1(m)$, אז $a^{\frac{\varphi(m)}{d}}\equiv g^{\frac{b\varphi(m)}{d}}\equiv 1(m)$. אבל $\operatorname{ord}g=\varphi(m)$ $\Leftarrow$ $\varphi(m)|\frac{b\varphi(m)}{d}$ $\Leftarrow$ $\frac{b}{d}\varphi(m)=k\cdot\varphi(m)$ עבור $k\in\mathbb{Z}$ כלשהו $\Leftarrow$ $b=kd$ $\Leftarrow$ יש פתרון. מש"ל.
<u>דוגמאות</u>:

1. $m=7$, $n=3$: $x^3\equiv a(7)$. אזי $\varphi(7)=6$ ו- $d=\gcd(3,6)=3$ ו- $\frac{\varphi(7)}{3}=2$ $\Leftarrow$ $a^2\equiv 1(7)$.

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1
a^3	1	1	6	1	6	6

לכן, 1 ו- 6 שאריות מחזקה 3 מודולו 7 . השאריות האחרות לא.

2. $m=7$, $n=2$: $x^2\equiv a(7)$. אזי $d=\gcd(2,6)=2$ ו- $\frac{\varphi(7)}{d}=3$, כלומר $a^3\equiv 1(7)$. מהטבלה, השאריות שמקיימות את זה הן $\{1,2,4\}$. לכן, הן כל השאריות מחזקה ריבועית מודולו 7 .

<u>קריטריון *Euler*</u> (לא מוכלל): יהי p ראשוני אי זוגי, ויהי $a\in\mathbb{Z}$ זר ל-p. אזי $x^2\equiv a(p)$ ניתנת לפתרון $\Leftrightarrow$ $a^{\frac{p-1}{2}}\equiv 1(p)$.

<u>הוכחה</u>: יהי g שורש פרימיטיבי מודולו p.

כיוון ראשון: נניח שיש פתרון לקונגרואנציה $x^2\equiv a(p)$, כלומר $\exists b.b^2\equiv a(p)$. נסמן: $b\equiv g^{\beta}(p)$. ואז $a\equiv g^{2\beta}(p)$ $\Leftarrow$ $a^{\frac{p-1}{2}}=g^{2\beta\cdot\frac{p-1}{2}}\equiv\left(g^{p-1}\right)^{\beta}\equiv 1(p)$.

בכיוון ההפוך: נניח ש-a אי שארית ריבועית מודולו p ו-$a\equiv g^{\gamma}(p)$. אזי γ אי זוגי (אחרת a הוא ריבוע). נסמן: $\gamma=2\beta+1$. אזי $a^{\frac{p-1}{2}}\equiv g^{(2\beta+1)\cdot\frac{p-1}{2}}\equiv g^{\beta(p-1)}\cdot g^{\frac{p-1}{2}}\equiv g^{\frac{p-1}{2}}\not\equiv 1(p)$, כי g שורש פרימיטיבי.

מש"ל.

הדדיות ריבועית (*reciprocity*)

<u>הגדרה</u>: אם $1<m\in\mathbb{Z}$ ו-$\gcd(a,m)=1$ אז a **שארית ריבועית** מודולו m אם יש פתרון לקונגרואנציה $x^2\equiv a(m)$.

<u>טענה</u>: יהי $m=2\cdot p_1^{e_1}\cdot\ldots\cdot p_t^{e_t}\in\mathbb{Z}$ כאשר p_i ראשוניים. נניח כי $\gcd(a,m)=1$. אזי הקונגרואנציה $x^2\equiv a(m)$ ניתנת לפתרון $\Leftrightarrow$:

1. $e=2$ ו-$a\equiv 1(4)$ או $e\geq 3$ ו-$a\equiv 1(8)$.
2. $\forall i.a^{\frac{p_i-1}{2}}\equiv 1(p_i)$.

נוכיח בהמשך טענה השקולה לטענה זו.

<u>למה</u>: אם $a\in\mathbb{Z}$ מקיים $a\equiv 1(8)$ אז הקונגרואנציה $x^2\equiv a\left(2^l\right)$ ניתנת לפתרון לכל l.

<u>הוכחה</u>: $a\equiv(-1)^u 5^v\left(2^l\right)$ כאשר $u\in\{0,1\}$, $v\in\left\{0,\ldots,2^{l-2}-1\right\}$ אם $l\geq 3$. אם $u=1$ אז $a\equiv -1(4)$, ולכן a אינו ריבוע. אם $a\equiv 1(8)$ אז $a\equiv 1(4)$, ואז $u=0$ (כי אם $u=1$ אז $(-1)^u 5^v\equiv -1(4)$) $\Leftarrow$ $a\equiv 5^v\left(2^l\right)$. אם $v=2k+1$ (אי זוגי) אזי $5^v\equiv 5^{2k+1}\equiv 25^k\cdot 5\equiv 5(8)$ $1\not\equiv$. לכן, v זוגי, כלומר $v=2k$. לכן, $a\equiv 5v\equiv\left(5^k\right)^2\left(2^l\right)$ $\Leftarrow$ a ריבוע מודולו 2^l. מש"ל.

<u>למה</u>: לכל p אי זוגי, אם $x^2\equiv a(p)$ ניתנת לפתרון, אז גם $x^2\equiv a\left(p^l\right)$ ניתנת לפתרון עבור כל l.

<u>הוכחה</u>: יש שורש פרימיטיבי g מודולו p^l. נסמן: $a\equiv g^{\alpha}\left(p^l\right)$. נניח שיש פתרון ל-$x^2\equiv a(p)$, כלומר $a\equiv c^2(p)$. נסמן: $c\equiv g^{\gamma}\left(p^l\right)$. אבל g הוא גם שורש פרימיטיבי מודולו p, ולכן $g^{\alpha}\equiv a\equiv c^2\equiv g^{2\gamma}\left(p^l\right)$. לכן, $\alpha\equiv 2\gamma(\varphi(p))$ $\Leftarrow$ $\alpha=2\gamma+k\cdot(p-1)$ עבור $k\in\mathbb{Z}$. מכיוון ש-$p-1$ זוגי, נקבל ש-α זוגי $\Leftarrow$ $\exists\beta\in\mathbb{Z}.\alpha=2\beta$ $\Leftarrow$ $a\equiv g^{\alpha}\equiv g^{2\beta}\equiv\left(g^{\beta}\right)^2\left(p^l\right)$. לכן, a ריבוע מודולו p^l. מש"ל.

<u>שאלה</u>: יהי $p\in\mathbb{Z}$ ראשוני. איזה a ריבוע מודולו p? אפשר גם בכיוון ההפוך: יהי $a\in\mathbb{Z}$. עבור איזה $p\in\mathbb{Z}$ ראשוני, a הוא ריבוע מודולו p?

<u>סימן לז'נדר</u> (*Legender*): אם p ראשוני אי זוגי, ו-a זר ל-p אז מגדירים סימן לז'נדר, כלומר את a מעל p להיות $\left(\frac{a}{p}\right)=\begin{cases}1 & \text{ריבוע מודולו } p \text{ } a\\ -1 & \text{אחרת}\end{cases}$.

<u>דוגמה</u>: $\left(\frac{1}{p}\right)=1$, $\left(\frac{-1}{5}\right)=1$, $\left(\frac{2}{5}\right)=-1$.

<u>טענה</u>:

1. $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(p)$.
2. $\left(a\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. $a\equiv b(p)\Rightarrow\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

<u>הוכחה</u>:

1. נגדיר: $b=a^{\frac{p-1}{2}}$. אזי $b^2\equiv 1(p)$. מכיוון שזה בשדה $\mathbb{Z}/p\mathbb{Z}$, אזי $b\equiv\pm 1(p)$. לפי קריטריון *Euler*, אם a שארית ריבועית אז $\left(\frac{a}{p}\right)=1$ ו- $b\equiv 1(p)$. אם a לא שארית ריבועית, אזי $b\not\equiv+1(p)$ $\Leftarrow$ $b\equiv-1(p)$ ו- $\left(\frac{a}{p}\right)=-1$. בכל מקרה, $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(p)$.
2. מהסעיף הקודם: $\left(a\frac{b}{p}\right)\equiv(ab)^{\frac{p-1}{2}}\equiv a^{\frac{p-1}{2}}b^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)(p)$. לכן, הם קונגרואנטיים מודולו p. אבל $\left(\frac{a}{p}\right),\left(\frac{b}{p}\right),\left(a\frac{b}{p}\right)\in\{-1,1\}$ ו- $1\not\equiv-1(p)$ כי $p>2$ $\Leftarrow$ $\left(a\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. ברור.

מש"ל.

<u>מסקנה</u>: יש בדיוק $\frac{p-1}{2}$ שאריות ריבועיות.

<u>הוכחה</u>: a שארית ריבועית $\Leftrightarrow$ $a^{\frac{p-1}{2}}\equiv 1(p)$ $\Leftrightarrow$ $\gcd\left(\frac{p-1}{2},p-2\right)=\frac{p-1}{2}$. לכן, יש בדיוק $\frac{p-1}{2}$ שאריות ריבועיות. מש"ל.

<u>מסקנה</u>: מכפלה של שתי שאריות ריבועיות היא שארית ריבועית. מכפלה של שארית ריבועית ואי שארית ריבועית היא אי שארית ריבועית. מכפלה של שתי אי שאריות ריבועיות היא שארית ריבועית.

<u>הוכחה</u>: אם a,b שאריות ריבועיות, אזי $\left(a\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=1\cdot 1=1$. אם a שארית ריבועית ו- b אי שארית ריבועית אזי $\left(a\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=1\cdot(-1)=-1$. אם a,b אי שאריות ריבועיות אזי $\left(a\frac{b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)=(-1)\cdot(-1)=1$. מש"ל.

<u>מסקנה</u>: $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

<u>הוכחה</u>: לפי המשפט, $\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}(p)$. מכיוון ש- $p>2$, נקבל $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. מש"ל.

<u>דוגמאות</u>:

1. אם $p=4k+1$ אז $\frac{p-1}{2}=2k$ ו- $(-1)^{\frac{p-1}{2}}=1$, ולכן $\left(\frac{-1}{p}\right)=1$, כלומר -1 ריבוע מודולו p.
2. אם $p=4k+3$ אז $\frac{p-1}{2}=2k+1$, ו- $(-1)^{\frac{p-1}{2}}=-1$, ולכן $\left(\frac{-1}{p}\right)=(-1)$, ולכן -1 אינו ריבוע מודולו p.

בפרט, -1 שארית ריבועית מודולו $5,13,29$ ו- -1 אי שארית ריבועית מודולו $7,11,19,23,31$.

<u>טענה</u>: יש אינסוף מספרים ראשוניים מהצורה $4k+1$.

<u>הוכחה</u>: יהיו $p_1,\ldots,p_m$ קבוצה סופית של ראשוניים מהצורה $4k+1$. נגדיר: $N=(2p_1\cdot\ldots\cdot p_m)^2+1$. אזי קיים מחלק ראשוני p של N. אזי $p\neq 2$ ו- $\forall i.p\neq p_i$. נסתכל על הקונגרואנציה $x^2\equiv-1(p)$. אזי $x=2p_1\cdot\ldots\cdot p_m$ כי $p|(x^2+1)=N$ $\Leftarrow$ $x^2+1\equiv 0(p)$ $\Leftarrow$ $x^2\equiv-1(p)$. לכן, $p=4k+1$. מש"ל.

<u>הגדרה</u>: יהי $p\in\mathbb{Z}$. נגדיר את **קבוצת השאריות הקטנות** (*least residues*):

$$S=\left\{-\frac{p-1}{2},-\frac{p-3}{2},\ldots,-1,1,\ldots,\frac{p-1}{2}\right\}$$

יהיו $a,p\in\mathbb{Z}$ כך ש- $p\nmid a$. נסמן: μ – מספר השאריות הקטנות השליליות של $a,2a,\dots,\frac{p-1}{2}\cdot a$.

<u>דוגמה</u>: $p=7$, $a=4$. לכן, $\frac{p-1}{2}=3$. אזי $S=\{-3,-2,-1,1,2,3\}$. נחשב: $1\cdot4\equiv4\equiv-3(7)$, $2\cdot4\equiv8\equiv1(7)$, $3\cdot4\equiv12\equiv-2(7)$. לכן, $\mu=2$.

<u>למת *Gauss-Gauß*</u>: $\left(\frac{a}{p}\right)=(-1)^{\mu}$, כאשר p ראשוני אי זוגי ו- $a\in\mathbb{Z}$ כך ש- $p\nmid a$.

<u>הוכחה</u>: יהי $a\in\mathbb{Z}$. יהי $1\le l\le\frac{p-1}{2}$. נסמן: $\pm m_l$ – השארית הקטנה של $l\cdot a$ (כאשר $m_l>0$). אזי μ הוא מספר המינוסים בסדרה $\pm m_l$. נוכיח כי $m_l\ne m_k$ עבור $l\ne k$. ואמנם, אם $m_l=m_k$ אז $la\equiv\pm ka(p)$ $\Leftarrow$ $a(l\pm k)\equiv0(p)$ $\Leftarrow$ $p|(l\pm k)\cdot a$. לפי ההנחה, $p\nmid a$, ולכן $p|l\pm k$. זה לא אפשרי, כי $|l\pm k|\le|l|+|k|\le\frac{p-1}{2}+\frac{p-1}{2}=p-1<p$. לכן, לא ייתכן ש- $p|l\pm k$. סתירה! לכן, קיבלנו כי הקבוצות $\{m_1,\dots m_{\frac{p-1}{2}}\}$, $\{1,\dots,\frac{p-1}{2}\}$ מתלכדות. לכן, $1\cdot a\equiv\pm m_1(p)$, ... , $\frac{p-1}{2}\equiv\pm m_{\frac{p-1}{2}}(p)$. נכפול את כל הקונגרואנציות: $\left(\frac{p-1}{2}\right)!\cdot a\equiv(-1)^{\mu}\cdot\left(\frac{p-1}{2}\right)!(p)$. מכיוון ש- $p\nmid\left(\frac{p-1}{2}\right)!$, נקבל $a\equiv(-1)^{\mu}(p)$. אבל $a^{\frac{p-1}{2}}\equiv\left(\frac{a}{p}\right)(p)$. לכן, $\left(\frac{a}{p}\right)\equiv(-1)^{\mu}(p)$. מכיוון ש- $p>2$, נקבל $\left(\frac{a}{p}\right)=(-1)^{\mu}$. מש"ל.

<u>דוגמה</u>: $\left(\frac{4}{7}\right)=1=(-1)^2$.

<u>טענה</u>:

1. 2 הוא שארית ריבועית מודולו p אם $p\equiv\pm1(8)$.
2. 2 הוא אי שארית ריבועית מודולו p אם $p\equiv\pm3(8)$.
3. $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

<u>הוכחה</u>:

1+2. מלמת גאוס עבור $a=2$, מכיוון ש- $\{2\cdot1,\dots,\frac{p-1}{2}\cdot2\}=\{2,\dots,p-1\}$, נקבל כי μ הוא מספר הגדולים מ- $\frac{p-1}{2}$. נגדיר: $m\in\mathbb{Z}$ כך ש- $2m\le\frac{p-1}{2}$ אבל $2(m+1)>\frac{p-1}{2}$. אזי $\mu=\frac{p-1}{2}-m$.

1. אם $p=8k+1$ אזי $\frac{p-1}{2}=4k$ $\Leftarrow$ $m=2k$ $\Leftarrow$ $\mu=2k$ $\Leftarrow$ $\left(\frac{2}{p}\right)=(-1)^{\mu}=1$.

   אם $p=8k+7$ אזי $\frac{p-1}{2}=4k+3$ $\Leftarrow$ $m=2k+1$ $\Leftarrow$ $\mu=2k+2$ $\Leftarrow$ $\left(\frac{2}{p}\right)=(-1)^{\mu}=1$.
2. אם $p=8k+3$ אזי $\frac{p-1}{2}=4k+1$ $\Leftarrow$ $m=2k$ $\Leftarrow$ $\mu=2k+1$ $\Leftarrow$ $\left(\frac{2}{p}\right)=(-1)^{\mu}=-1$.

   אם $p=8k+5$ אזי $\frac{p-1}{2}=4k+2$ $\Leftarrow$ $m=2k+1$ $\Leftarrow$ $\mu=2k+1$ $\Leftarrow$ $\left(\frac{2}{p}\right)=(-1)^{\mu}=-1$.
3. אם $p\equiv\pm1(8)$ אז $p=8k\pm1$, ולכן $\frac{p^2-1}{8}=\frac{64k^2\pm16k+1-1}{8}=8k^2\pm2k$. לכן, $(-1)^{\frac{p^2-1}{8}}=1$ וגם $\left(\frac{2}{p}\right)=1$ (לפי סעיף 1 של הטענה).

אם $p\equiv\pm3(8)$ אז $p=8k\pm3$, ולכן $\frac{p^2-1}{8}=\frac{64k^2\pm48k+9-1}{8}=8k^2\pm6k+1$. $2\nmid$ לכן, $(-1)^{\frac{p^2-1}{8}}=-1$, וגם $\left(\frac{2}{p}\right)=-1$ (לפי סעיף 2 של הטענה).

מש"ל.

דוגמאות:

p	3	5	7	17
$p \bmod 8$	3	5	7	1
$\left(\frac{2}{p}\right)$	-1	-1	1	1

ועבור $p=5$:

x	1	2	3	4
x^2	1	4	4	1

שאלה: בהינתן p,q ראשוניים, מהו $\left(\frac{p}{q}\right)$? האם יש קשר בין $\left(\frac{p}{q}\right)$ ל- $\left(\frac{q}{p}\right)$?

דוגמאות: $\left(\frac{3}{5}\right)=-1$, $\left(\frac{5}{3}\right)=-1$, $\left(\frac{3}{7}\right)=-1$, $\left(\frac{7}{3}\right)=\left(\frac{1}{3}\right)=1$. קיבלנו כי לפעמים $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ ולפעמים $\left(\frac{p}{q}\right)\neq\left(\frac{q}{p}\right)$.

השערת *Euler* בסימוני *Legender*: $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$.

זה נקרא חוק ההדדיות הריבועיות (באנגלית: *quadratic reciprocity law*, ברוסית: *Квадратичный закон взаимности*). לאחר מכן, *Gauß* הוכיח אותו 6 פעמים, והיום ידועות 100 הוכחות.

משפט (חוק ההדדיות הריבועיות של *Gauß*): אם p,q ראשוניים אי זוגיים שונים, אז $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. כמו כן, $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$ ו- $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$. כלומר, אם p,q ראשוניים אי זוגיים שונים, אזי:

1. $\left(\frac{p}{q}\right)=\left(\frac{q}{p}\right)$ אם $p=4k+1$ או $q=4l+1$.
2. $\left(\frac{p}{q}\right)=-\left(\frac{q}{p}\right)$ אם $p=4k+3$ ו- $q=4l+3$.

דוגמאות:

1. $\left(\frac{29}{43}\right)=?$: $29=4\cdot7+1 \Leftarrow \left(\frac{29}{43}\right)=\left(\frac{43}{29}\right)=\left(\frac{14}{29}\right)=\left(\frac{2}{29}\right)\cdot\left(\frac{14}{29}\right)$. $29=8\cdot3+5 \Leftarrow \left(\frac{2}{29}\right)=-1$, $\left(\frac{7}{29}\right)=\left(\frac{29}{7}\right)=\left(\frac{1}{7}\right)=1 \Leftarrow \left(\frac{29}{43}\right)=-1$.
2. $\left(\frac{89}{101}\right)=?$: $101=4\cdot25+1 \Leftarrow \left(\frac{79}{101}\right)=\left(\frac{101}{79}\right)=\left(\frac{22}{79}\right)=\left(\frac{2}{79}\right)\cdot\left(\frac{11}{79}\right)$. $79=8\cdot10-1 \Leftarrow$ $\left(\frac{2}{79}\right)=1 \Leftarrow \left(\frac{2}{79}\right)\cdot\left(\frac{11}{79}\right)=\left(\frac{11}{79}\right)$. $79=4\cdot20-1$, $11=4\cdot3-1 \Leftarrow$ $1=-(-1)=-\left(\frac{2}{11}\right)=-\left(\frac{79}{11}\right)=\left(\frac{11}{79}\right)$.

3. לאיזה p ראשוני, $\left(\frac{5}{p}\right)=1$? $5=4\cdot1+1 \Leftarrow \left(\frac{5}{p}\right)=\left(\frac{p}{5}\right)$. לכן, נחפש p כך ש- $\left(\frac{p}{5}\right)=1$.

x	1	2	3	4
x^2	1	4	4	1

לכן, $p\equiv\pm1(5)$.

4. לאיזה p ראשוני, $\left(\frac{3}{p}\right)=1$? $3=1\cdot4-1 \Leftarrow \left(\frac{3}{p}\right)=(-1)^{\frac{p-1}{2}}\cdot\left(\frac{p}{3}\right)$. לכן, נחפש p כך ש- $\left(\frac{p}{3}\right)\cdot(-1)^{\frac{p-1}{2}}=1$.
   1. מקרה 1: אם $\left(\frac{p}{3}\right)=1=(-1)^{\frac{p-1}{2}}$. אזי $p\equiv1(3)$ ו- $p\equiv1(4)$. לכן, $p\equiv1(12)$.
   2. מקרה 2: אם $\left(\frac{p}{3}\right)=-1=(-1)^{\frac{p-1}{2}}$. אזי $p\equiv-1(3)$ ו- $p\equiv-1(4)$. לכן, $p\equiv-1(12)$.

   לכן, בסך הכל, $p\equiv\pm1(12)$.

סימן יעקובי (*Jacobi*)

<u>הגדרה</u>: יהי $0<b\in\mathbb{Z}$ אי זוגי. נסמן: $b=p_1\cdot\ldots\cdot p_m$ כאשר p_i ראשוניים אי זוגיים (ויכולים להופיע מספר פעמים). יהי $a\in\mathbb{Z}$ זר ל- b. אזי $\left(\frac{a}{b}\right)=\left(\frac{a}{p_1}\right)\cdot\ldots\cdot\left(\frac{a}{p_m}\right)$.

<u>הערה</u>: אם $a\equiv c^2(b)$ אזי $a\equiv c^2(p_i)$ ולכן $\forall i. \left(\frac{a}{p_i}\right)=1$, ולכן $\left(\frac{a}{b}\right)=1$. אבל אפשרי ש- $\left(\frac{a}{b}\right)=1$ ו- a אינו ריבוע מודולו b.

<u>דוגמה</u>: $\left(\frac{2}{15}\right)=\left(\frac{2}{3}\right)\cdot\left(\frac{2}{5}\right)=(-1)\cdot(-1)=1$, אבל מכיוון ש- 2 אינו ריבוע מודולו 3 (למשל), אזי גם 2 אינו ריבוע מודולו 15.

<u>הערה</u>: אם $\left(\frac{a}{b}\right)=-1$, אז בהכרח a אינו ריבוע מודולו b.

<u>טענה</u>:
1. אם $a_1\equiv a_2(b)$ אזי $\left(\frac{a_1}{b}\right)=\left(\frac{a_2}{b}\right)$.
2. $\left(a_1\frac{a_2}{b}\right)=\left(\frac{a_1}{b}\right)\cdot\left(\frac{a_2}{b}\right)$.
3. $\left(\frac{a}{b_1b_2}\right)=\left(\frac{a}{b_1}\right)\cdot\left(\frac{a}{b_2}\right)$.

<u>למה</u>: יהיו $r,s\in\mathbb{Z}$ אי זוגיים. אזי:
1. $\frac{rs-1}{2}\equiv\frac{r-1}{2}+\frac{s-1}{2}(2)$.
2. $\frac{(rs)^2-1}{8}\equiv\frac{r^2-1}{8}+\frac{s^2-1}{8}(2)$.

<u>הוכחה</u>:
1. $rs-1=((r-1)+1)((s-1)+1)-1=(r-1)(s-1)+(r-1)+(s-1) \Leftarrow rs-1\equiv r-1+s-1(4)$

   $\Leftarrow \frac{rs-1}{2}\equiv\frac{r-1}{2}+\frac{s-1}{2}(2)$.

2. $(rs)^2-1=((r^2-1)+1)((s^2-1)+1)-1=(r^2-1)(s^2-1)+(r^2-1)+(s^2-1)$. מכיוון ש- r,s אי זוגיים, $16|(r^2-1)(s^2-1)$ (כי אם $r=2k+1$ אז $4|(r^2-1)$). לכן: $r^2s^2-1\equiv(r^2-1)+(s^2-1)(16)$
$\Leftarrow$ $\frac{(rs)^2-1}{8}\equiv\frac{r^2-1}{8}+\frac{s^2-1}{8}(2)$.

מש"ל.

<u>מסקנה</u>: יהיו $r_1,\dots,r_m\in\mathbb{Z}$ אי זוגיים. אזי:

1. $\frac{r_1\cdot\ldots\cdot r_m}{2}\equiv\sum_{i=1}^{m}\frac{r_i-1}{2}(2)$.
2. $\frac{r_1^2\cdot\ldots\cdot r_m^2-1}{8}\equiv\sum_{i=1}^{m}\frac{r_i^2-1}{8}(2)$.

<u>הוכחה</u>: באינדוקציה.

<u>טענה</u> (חוק ההדדיות עבור סימן יעקובי): יהיו $a,b>0$ אי זוגיים זרים. אזי:

1. $\left(\frac{-1}{b}\right)=(-1)^{\frac{b-1}{2}}$.
2. $\left(\frac{2}{b}\right)=(-1)^{\frac{b^2-1}{8}}$.
3. $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right)=(-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

<u>הוכחה</u>:

1. $\left(\frac{-1}{b}\right)=\prod\left(\frac{-1}{p_i}\right)=\prod(-1)^{\frac{p_i-1}{2}}=(-1)^{\sum\frac{p_i-1}{2}}=(-1)^{\frac{b-1}{2}}$.
2. דומה.
3. נסמן: $a=q_1\cdot\ldots\cdot q_l$, $b=p_1\cdot\ldots\cdot p_m$. אזי:

$$\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right)=\prod_{i,j}\left(\frac{q_j}{p_i}\right)\cdot\prod_{i,j}\left(\frac{p_i}{q_j}\right)=\prod_{i,j}\left(\frac{q_j}{p_i}\right)\cdot\left(\frac{p_i}{q_j}\right)=\prod_{i,j}(-1)^{\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}=(-1)^{\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}$$

$$\sum_{i,j}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}=\left(\sum_i\frac{p_i-1}{2}\right)\cdot\left(\sum_j\frac{q_j-1}{2}\right)\equiv\frac{p_1\cdot\ldots\cdot p_m-1}{2}\cdot\frac{q_1\cdot\ldots\cdot q_l-1}{2}\equiv\frac{b-1}{2}\cdot\frac{a-1}{2}(2)$$

$\Leftarrow$ $\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right)=(-1)^{\frac{b-1}{2}\cdot\frac{a-1}{2}}$.

מש"ל.

כמה מספרים ראשוניים יש? ומשפט *Dirichlet*

יש כמה קבוצות של מספרים ראשוניים:

- $\{2\}$.
- $p_1=\{p\in\mathbb{Z}|(p\text{ is prime})\wedge\exists k\in\mathbb{Z}.p=4k+1\}$.
- $p_3=\{p\in\mathbb{Z}|(p\text{ is prime})\wedge\exists k\in\mathbb{Z}.p=4k+3\}$.

אזי המספרים הראשוניים הם $\{2\}\cup p_1\cup p_3$. יש אינסוף מספרים ראשוניים ב- p_1,p_3. יש אינסוף ראשוניים מהצורה $8k+7$, ואין אינסוף ראשוניים מהצורה $8k+6$. באופן כללי יותר: אם $1<a,m\in\mathbb{Z}$ ועבור $0\le k\in\mathbb{Z}$ נסמן $a_k=a+km$, ונסמן $d=\gcd(a,m)$. אם $a=d$ ו- d ראשוני אז אין אינסוף ראשוניים.

<u>משפט *Dirichlet*</u> (משנת 1837): יהיו $1<a,m\in\mathbb{Z}$. נניח ש- $\gcd(a,m)=1$. אז יש אינסוף מספרים ראשוניים מהצורה p כך ש- $p\equiv a(m)$.

<u>הגדרה</u>: יהי $0<x\in\mathbb{Z}$. אזי $\pi(x)=\#\{p\in\mathbb{Z}|p<x\wedge(p\text{ is prime})\}$.

<u>דוגמה</u>: $\pi(10)=4$, כי הראשוניים הם $2,3,5,7$.

x	10	25	50	100	200	500	1000	5000
$\pi(x)$	4	9	15	25	46	95	168	669
$\frac{\pi(x)}{x}$	0.4	0.36	0.3	0.25	0.23	0.19	0.168	0.134

ניתן לראות בטבלה כי $\frac{\pi(x)}{x}\underset{x\to\infty}{\to}0$.

<u>משפט המספרים הראשוניים</u> (*Prime number theorem*): $\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1$.

<u>השערת *Goldbach*</u> (משנת 1742): כל מספר זוגי $4\le n\in\mathbb{Z}$ הוא סכום של שני מספרים ראשוניים.
ב-1937 הוכיח *Vinogradov* כי כל מספר אי זוגי מספיק גדול הוא סכום של שלושה מספרים ראשוניים.
ב-1966 הוכיח *Cheng Jingrum* שכך מספר זוגי מספיק גדול n הוא סכום $n=p+q$ כאשר p ראשוני ו- q או ראשוני או מכפלה של שני ראשוניים.
<u>השערת התאומים</u>: מספרים תאומים הם שני ראשוניים שההפרש ביניהם הוא 2 . ההשערה היא שיש אינסוף מספרים תאומים.
בשנת 1966 הוכיח *Chen Jingrum* שקיימים אינסוף p ראשוניים כך ש- $p+2$ או ראשוני או מכפלה של שני ראשוניים.
<u>הראשוניים של *Mercenne*</u>: ראשוניים מהצורה $q=a^n-1$. עבור איזה a,n המספר q יהיה ראשוני? נשים לב לכך ש- $q=(a-1)(a^{n-1}+\ldots+a+1)$. לכן, $a-1|q$, ולכן אם $a\neq2$ אז q מורכב. לכן, $q=2^n-1$. אם $n=mk$ אז $2^n-1=(2^m)^k-1$. ניקח $a=2^m$, ואז $2^m-1|q$. אם $q=2^n-1$ ו- $n=mk$ אז q מורכב אם $m\neq1$ ו- $m\neq n$. אם $q=2^p-1$ עבור p ראשוני, האם q ראשוני? אלה נקראים המספרים הראשוניים של *Mercenne*. האב *Martin Mercenne* טען ש- 2^p-1 ראשוני עבור $p\in\{2,3,5,7,13,17,19,31,67,127,257\}$, ורק עבור $p<528$ האלה 2^p-1 ראשוני. הוא עשה 5 טעויות, כי עבור $p=67,257$ מקבלים ש- 2^p-1 לא ראשוני ועבור $p=61,89,107$ מקבלים ש- 2^p-1 ראשוני. בשנת 1999 גילו שעבור $p=6972593$ מתקיים ש- $M_p=2^p-1$ ראשוני, בן 1,098,960 ספרות.
<u>מספרים ראשוניים של *Fermat*</u>: $F_n=2^{2^n}+1$. פרמה העלה השערה ש- F_n ראשוני לכל $0\le n\in\mathbb{Z}$.ואכן $F_0=3$, $F_1=5$, $F_2=17$, $F_3=257$, $F_4=65537$ ראשוניים, אבל *Euler* גילה שהמספר $F_5=2^{2^5}+1$ מורכב ו- $641|F_5$. בעזרת מחשבים, לא גילו מספרי *Fermat* חדשים עד $n=160$.
<u>משפט *Crauß*</u>: נסתכל על מצולע משוכלל בן m צלעות. האם אפשר לבנות את המצולע בעזרת מחוקה וסרגל? אפשר עבור $m=2\cdot p_1\cdot\ldots\cdot p_l$ כאשר p_i מספרים ראשוניים שונים של *Fermat*, ולמשל עבור $7,9$ אי אפשר.

סימן יעקובי

עם סימן יעקובי יותר קל לחשב את סימן לג'נדר, כי לא צריך לפרק מספרים כל הזמן.
<u>דוגמה</u>:

$$\left(\frac{2819}{4177}\right)\underset{4177\equiv1(4)}{=}\left(\frac{4177}{2819}\right)\underset{4177\equiv1358(2819)}{=}\left(\frac{1358}{2819}\right)\underset{1358=2\cdot679}{=}\left(\frac{2}{2819}\right)\cdot\left(\frac{679}{2819}\right)\underset{2819\equiv3(8)}{=}-\left(\frac{679}{2819}\right)\underset{2819\equiv679\equiv3(4)}{=}$$
$$=\left(\frac{2819}{679}\right)\underset{2819\equiv103(679)}{=}\left(\frac{103}{679}\right)\underset{103\equiv679\equiv3(4)}{=}-\left(\frac{679}{103}\right)\underset{679\equiv61(103)}{=}-\left(\frac{61}{103}\right)\underset{61\equiv1(4)}{=}-\left(\frac{103}{61}\right)\underset{103\equiv42(61)}{=}-\left(\frac{42}{61}\right)=$$
$$\underset{42=2\cdot21}{=}-\left(\frac{2}{61}\right)\cdot\left(\frac{21}{61}\right)\underset{61\equiv5(8)}{=}\left(\frac{21}{61}\right)\underset{61\equiv1(4)}{=}\left(\frac{61}{21}\right)\underset{61\equiv19(21)}{=}\left(\frac{19}{21}\right)\underset{21\equiv1(4)}{=}\left(\frac{21}{19}\right)\underset{21\equiv2(19)}{=}\left(\frac{2}{19}\right)\underset{19\equiv3(8)}{=}-1$$

מספרים טרנסצנדנטיים של *Liouville*

<u>הגדרה</u>: $x\in\mathbb{R}$ נקרא **אלגברי** אם הוא שורש של פולינום עם מקדמים רציונליים. כלומר $a\in\mathbb{R}$ אלגברי אם הוא שורש של $a_0x^n+\ldots+a_n=0$ כאשר $\forall i.\,a_i\in\mathbb{Q}$.
האם כל המספרים ב- $\mathbb{R}$ הם אלגבריים? מכיוון ש- $\mathbb{Q}$ היא קבוצה בת מניה, גם קבוצת כל הפולינומים עם מקדמים רציונליים היא בת מניה. אבל $\mathbb{R}$ אינה בת מניה, ולכן קיימים מספרים ב- $\mathbb{R}$ שאינם אלגברים.

<u>הגדרה:</u> $x\in\mathbb{R}$ נקרא **טרנסצנדנטי** אם הוא אינו אלגברי.
<u>דוגמאות:</u>
1. e,π הם טרנסצנדנטיים (ההוכחה היא קשה).
2. $\xi=\sum_{k=1}^{\infty}\frac{1}{2^{k!}}$. המספר הזה לא יכול להיות רציונלי, כי בבסיס 2 הוא שבר בינארי בלי מחזור.

<u>הגדרה:</u> יהי $x\in\mathbb{R}$ מספר אלגברי. אזי f נקרא **הפולינום המינימלי** של x אם $f(x)=0$ ו-f מתוקן ממעלה מינימלית.

<u>משפט *Liouville*:</u> אם $\alpha\in\mathbb{R}$ מספר אלגברי ממעלה $n>1$, אז קיים קבוע $c=c(\alpha)>0$ כך ש- $\left|\alpha-\frac{p}{q}\right|\overset{(*)}{>}\frac{c}{q^n}$ לכל $p,q\in\mathbb{Z}$ ו- $q>0$.

<u>הוכחה:</u> יהי α שורש של $f\in\mathbb{Z}[X]$ אי פריק ממעלה n פרימיטיבי, כלומר $\gcd(a_0,a_1,\dots,a_n)=1$. אזי $f(\alpha)=0$. יהי $\frac{p}{q}$ קירוב של α. אזי $f\left(\frac{p}{q}\right)\neq0$, כי הפולינום אי פריק.

<u>הערה:</u> אם המשפט נכון עבור c ו- $c'<c$, אז הוא גם נכון עבור c'. לכן, אפשר להניח ש- $c<1$, כלומר $(*)$ נכון גם עבור כל $\frac{p}{q}$ כך ש- $\left|\alpha-\frac{p}{q}\right|\geq1$. לכן, מספיק להוכיח עבור $\left|\frac{p}{q}-\alpha\right|<1$.

$\frac{p}{q}$ חסום: $\left|\frac{p}{q}\right|<|\alpha|+1$. כמו כן, $f\left(\frac{p}{q}\right)\neq0$, ולכן $\left|q^nf\left(\frac{p}{q}\right)\right|=\left|a_np^n+a_{n-1}p^{n-1}q+\ldots+a_0q^n\right|\geq1$ (כי כל המחוברים שם שלמים, והביטוי שונה מ- 0). כמו כן, $f\left(\frac{p}{q}\right)=f\left(\frac{p}{q}\right)-f(\alpha)=\left(\frac{p}{q}-\alpha\right)\cdot f'(\xi)$ לפי משפט לגרנז', כאשר $\xi\in\mathbb{R}$ בין $\frac{p}{q}$ ל- α. אזי ξ חסום, כי $\left|\alpha-\frac{p}{q}\right|\leq1$, ולכן $|\xi|\leq|\alpha|+1$. גם $f'(\xi)$ חסום, כלומר $|f'(\xi)|<C_1$ ו- C_1 תלוי רק ב- α. $f'(\xi)$ חסום כי מסתכלים רק על הקטע $\left[|\alpha|-1,|\alpha|+1\right]$. אזי:

$$\left|\alpha-\frac{p}{q}\right|=\frac{\left|q^nf\left(\frac{p}{q}\right)\right|}{q^n\cdot|f'(\xi)|}\geq\frac{1}{q^nC_1}$$

לכן, $(*)$ נכון עבור $c=\frac{1}{C_1}$. מש"ל.

<u>מסקנה:</u> תהי $(s_i)=s_1,s_2,\ldots$ סדרה אינסופית, $s_i=\pm1$. אזי המספר $\xi=1+\frac{s_1}{2^{1!}}+\frac{s_2}{2^{2!}}+\ldots+\frac{s_n}{2^{n!}}+\ldots$ הוא מספר טרנסצנדנטי.
הוכחה: בפיתוח (עשרוני או בינארי), זה שבר בלי מחזור, ולכן ξ הוא לא רציונלי. נוכיח כעת שהוא גם לא אלגברי. נסמן: $q_n=2^{(n-1)!}$ ו- $p_n=q_n\cdot\left(1+\frac{s_1}{2^{1!}}+\ldots+\frac{s_{n-1}}{2^{(n-1)!}}\right)$. אזי $\left|\xi-\frac{p_n}{q_n}\right|\overset{(1)}{\leq}\frac{1}{2^{n!}}+\frac{1}{2^{(n+1)!}}+\ldots$. עבור $k\geq1$ מתקיים $2^{(n+k)!}\geq2^{n!\cdot(n+k)}\geq\left(2^{n!}\right)^k$. לכן, הצד הימני של (1) קטן מ- $\frac{1}{2^{n!}}+\frac{1}{2^{n!}}+\frac{1}{\left(2^{n!}\right)^2}+\cdots$. לכן, נקבל:

$$\left|\xi-\frac{p_n}{q_n}\right|\leq\frac{1}{2^{n!}}+\frac{1}{2^{(n+1)!}}+\ldots\leq\frac{1}{2^{n!}}+\frac{1}{2^{n!}}+\frac{1}{\left(2^{n!}\right)^2}+\ldots=\frac{1}{2^{n!}}+\frac{1/2^{n!}}{1-1/2^{n!}}\leq2\cdot\frac{1/2^{n!}}{1-1/2^{n!}}\leq\frac{4}{2^{n!}}=\frac{4}{q_n^n}$$

לכן, $\left|\xi-\frac{p_n}{q_n}\right|\leq\frac{4}{q_n^n}$ לכל n. לכן, ξ אינו אלגברי. ואמנם, אם ξ היה אלגברי ממעלה $m>1$, אז קיים $c>0$ כך ש- $\left|\xi-\frac{p_n}{q_n}\right|>\frac{c}{q^m}$ לכל $p,q\in\mathbb{Z},q\neq0$. אבל עבור ξ שלנו, $q_n^m\cdot\left|\xi-\frac{p_n}{q_n}\right|<q_n^m\cdot\frac{1}{q_n^n}=\frac{4}{q_n^{n-m}}$.

אבל $\lim_{n\to\infty}\frac{4}{q_n^{n-m}}=0$, כי $q_n>2$, ולכן לא ייתכן ש- $\forall n.\frac{4}{q_n^{n-m}}>c>0$. מש"ל.

למת הנזל (*Hensel*)

דוגמה: $2x^3+7x-4\equiv0(200)$, $200=2^3\cdot5^2$ $\Leftarrow$ $2x^3+7x-4\equiv0(2^3)$, $2x^3+7x-4\equiv0(5^2)$. נפתור רק את הקונגרואנציה השניה, וממנה נוכל לקבל רעיון. כל פתרון מודולו 5^2 הוא גם פתרון מודולו 5 , ולכן נפתור את $2x^2+7x-4\equiv0(5)$.

x	0	1	2	3	4
$f(x)$	1	0	1	1	2

למשל, 1 הוא פתרון. ננסה להרים (*Carry*) את הפתרון ל- $\mathbb{Z}/5^2\mathbb{Z}$. אזי $x=1+5t$. ניקח $t\in\{0,1,2,3,4\}$, ונקבל פתרונות ל- $\mathbb{Z}/5^2\mathbb{Z}$. אפשרות נוספת:

$2\cdot(1+5t)^3+7\cdot(1+5t)-4\equiv2+2\cdot3\cdot5t+7+7\cdot5t-4\equiv0(25)$ $\Leftarrow$ $5+(2\cdot3\cdot1+7)\cdot5t\equiv0(25)$ $\Leftarrow$ $1+(2\cdot3\cdot1+7)t\equiv0(5)$ (כי חילקנו הכל ב-5). נקבל: $1+13t\equiv0(5)$ $\Leftarrow$ $3t\equiv13t\equiv-1(5)$ $\Leftarrow$ $t\equiv3(5)$ $\Leftarrow$ $x=1+5\cdot3=16$ $\Leftarrow$ $x\equiv16(25)$. $f(x)=2x^3+7x-4$ $\Leftarrow$ $f'(x)=2\cdot3x^2+7$. נציב $x=1$: $f(1)=2\cdot3\cdot1+7=13$, $f'(1)=2\cdot3\cdot1+7=13$.

הגדרה: יהי R חוג. נגדיר **פולינומים על החוג** $\boldsymbol{R}$: $f\in R[X]$ אם $f=a_nx^n+\ldots+a_0$ כאשר $a_i\in R$.

הנגזרת: $f'(x)=n\cdot a_nx^{n-1}+\ldots+a_1$.

למה: יהיו $f,g\in R[X]$. אזי:

1. $(f+g)'=f'+g'$.
2. $\forall c\in R.(cf)'=cf'$.
3. $(f\cdot g)'=f'\cdot g+f\cdot g'$.

למה: אם $f(x)=x^m$ אז $f^{(k)}(x)=m\cdot(m-1)\cdot\ldots\cdot(m-k+1)x^{m-k}$.

למה: יהי $f\in\mathbb{Z}[X]$ ממעלה n . אם $b\in\mathbb{Z}$ אז $f(x+b)=f(x)+\frac{f'(x)}{1!}\cdot b+\frac{f''(x)}{2!}\cdot b^2+\ldots+\frac{f^{(n)}(x)}{n!}\cdot b^n$ (נוסחת טיילור), כאשר המקדם $\frac{f^{(k)}(x)}{k!}\in\mathbb{Z}[X]$.

הוכחה: מספיק להוכיח עבור $f_m(x)=x^m$ כאשר $m\leq n$. לפי משפט הבינום, $(x+b)^m=\sum_{j=0}^{m}\binom{m}{j}x^{m-j}b^j$. כמו כן, $f_m^{(j)}(x)=m\cdot(m-1)\cdot\ldots\cdot(m-j+1)x^{m-j}$ $\Leftarrow$ $\frac{1}{j!}\cdot f_m^{(j)}(x)=\binom{m}{j}x^{m-j}$ $\Leftarrow$ $f_m(x+b)=\sum_{j=0}^{m}\frac{1}{j!}\cdot f_m^{(j)}(x)b^j$. מש"ל.

משפט (למת *Hensel*): יהי $f\in\mathbb{Z}[X]$ ו- $2\leq k\in\mathbb{Z}$. יהי r פתרון של הקונגרואנציה $f(x)\equiv0(p^{k-1})$. אזי:

1. אם $f'(r)\neq0(p)$ אז קיים ויחיד $0\leq t<p$ כך ש- $f(r+tp^{k-1})\equiv0(p)$, כאשר $t\equiv\widetilde{f'(r)}\cdot\left(-\frac{f(r)}{p^{k-1}}\right)(mod\,p)$ כאשר $\widetilde{f'(r)}\cdot f'(r)\equiv1(p)$.
2. אם $f'(r)\equiv0(p)$ וגם $f(r)\equiv0(p^k)$, אזי גם $f(r+tp^{k-1})\equiv0(p^k)$ לכל $t\in\mathbb{Z}$.
3. אם $f'(r)\equiv0(p)$ וגם $f(r)\not\equiv0(p^k)$ אזי לקונגרואנציה $f(x)\equiv0(p^k)$ אין פתרון עבור $x\equiv r(p^{k-1})$.

הוכחה: יהי $r'\in\mathbb{Z}$ כך ש- $r'\equiv r(p^{k-1})$. אזי $r'=r+tp^{k-1}$ עבור $t\in\mathbb{Z}$. נניח $f(r')\equiv0(p^k)$. אזי: $f(r+tp^{k-1})=f(r)+f'(r)tp^{k-1}+\frac{1}{2!}\cdot f''(r)(tp^{k-1})^2+\ldots$. יהי $j\geq2$. אזי $\frac{f^{(j)}(r)}{j!}\cdot t^jp^{(k-1)^j}\equiv0(p^k)$ כי $\frac{f^{(j)}(r)}{j!}\in\mathbb{Z}$, ומכיון ש- $k,j\geq2$ אז $(k-1)(j-1)\geq1$ $\Leftarrow$ $(k-1)j-k+1\geq1$ $\Leftarrow$ $k\leq(k-1)j$ $\Leftarrow$

$f(r')\equiv f(r)+f'(r)\,t\,p^{k-1}\equiv 0\left(p^k\right)$. $f(r)\equiv 0\left(p^{k-1}\right)$ $\Leftarrow$ $p^{k-1}|f(r)$ $\Leftarrow$ $\frac{f(r)}{p^{k-1}}\overset{(*)}{\equiv}-f'(r)\,t(p)$.

1. אם $f'(r)\not\equiv 0(p)$ אז יש פתרון יחיד: אם $\widetilde{f'(r)}\cdot f'(r)\equiv 1(p)$ אז $t\equiv-\frac{f(r)}{p^{k-1}}\cdot\widetilde{f'(r)}(p)$.
2. אם $f'(r)\equiv 0(p)$ וגם $\frac{f(r)}{p^{k+1}}\equiv 0(p)$ אז יש אינסוף פתרונות, כי ב- $(*)$ נקבל $0\equiv 0\left(p^k\right)$.
3. אם $f'(r)\equiv 0(p)$ וגם $\frac{f(r)}{p^{k-1}}\not\equiv 0(p)$ אז אין פתרונות, כי ב- $(*)$ נקבל $\frac{f(r)}{p^{k+1}}\equiv 0(p)$, בסתירה להנחה.

מש"ל.

<u>מסקנה</u>: נניח ש- $r_1\in\mathbb{Z}$ הוא פתרון של הקונגרואנציה $f(x)\equiv 0(p)$. אם $f'(r_1)\neq 0(p)$ אז לכל k קיים ויחיד פתרון r_k של $f(x)\equiv 0\left(p^k\right)$.

<u>דוגמה</u>: $x^2+x+7\equiv 0(27)$. $27=3^3$. נסתכל מודולו 3 : $x\equiv 1(3)$ הוא הפתרון היחיד. $f'(x)=2x+1$ $\Leftarrow$ $f'(1)=3\equiv 0(3)$. $f(1)=9$ $\Leftarrow$ $\frac{f(1)}{3}\equiv 0(3)$ $\Leftarrow$ $x\equiv 1+3t(9)$ עבור t כלשהו, ולכן $x\equiv 1,4,7(9)$. $f(1)=9\not\equiv 0(27)$, ולכן $x=1+9\cdot t$ לא ניתן להרמה. $f(4)=27\equiv 0(27)$ $\Leftarrow$ $x=4+9\cdot t$ עבור t כלשהו, ולכן $x\equiv 4,13,22(27)$ פתרונות. $f(7)\not\equiv 0(27)$ $\Leftarrow$ אי אפשר להרים.

<u>טענה</u>: אם p ראשוני אי זוגי, אז הקונגרואנציה $x^2\overset{(*_k)}{\equiv}a\left(p^k\right)$ (עבור $p\nmid a$) ניתנת לפתרון אם ורק אם $x^2\overset{(*_1)}{\equiv}a(p)$ ניתנת לפתרון. $\Leftrightarrow$ $\left(\frac{a}{p}\right)=1$

הצפנה במפתח פומבי

$13=(1101)_2$ (ארבעה ביטים).

למספר n יש סדר גודל של $\log_2 n$ ביטים.

<u>חיבור</u>: לחיבור של שני מספרים עם 8 ביטים כל אחד עשינו 8 פעולות.

$$\begin{array}{ccccccccc} & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0\\ + & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0\\ \hline 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0\end{array}$$

לשני מספרים עם k ביטים כל אחד נעשה k פעולות.

<u>כפל</u>: בכפל שני מספרים עם k,l ביטים עשינו l חיבורים של $k+l$ ביטים (אורך המספר המחובר), כלומר $l\cdot(k+l)$ פעולות, כלומר לכל היותר $2kl$ פעולות. אזי: $Time(m\cdot n)\leq 2\log_2 m\cdot\log_2 n$, כלומר $c\cdot\log m\cdot\log n$. אם $m<2^k$ אזי $\log_2 m<k$.

$$\begin{array}{ccccccccc} & & & & & 1 & 1 & 1 & 0 & 1\\ & & & & & \cdot & 1 & 1 & 0 & 1\\ \hline & & & & & 1 & 1 & 1 & 0 & 1\\ + & & & 1 & 1 & 1 & 0 & 1 & & \\ + & 1 & 1 & 1 & 0 & 1 & & & & \\ \hline & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1\end{array}$$

<u>סימון</u>: אם $f,g:\mathbb{N}\to\mathbb{R}$ אז $f(n)=O(g(n))$ אם ורק אם קיימים $B,C>0$ כך שאם $n>B$ אז $f(n)$ ו- $g(n)$ מוגדרים, ו- $f(n)\leq C\cdot g(n)$.

<u>דוגמה</u>: נגדיר: $f(n)$ - מספר הביטים של n . אזי $f(n)=O(\log n)$.

<u>חילוק</u>: לחילוק מספר עם k ביטים במספר עם l ביטים, דרוש זמן $O(kl)$.

<u>הגדרה</u>: אם $n_1,\dots,n_r\in\mathbb{Z}$ ו- $k_1,\dots,k_r$ מספר הביטים של כל אחד מהם בהתאמה, נאמר שאלגוריתם רץ בזמן פולינומיאלי אם קיימים $d_1,\dots,d_r$ כך ש- $Time=O\left(k_1^{d_1}\cdot\ldots\cdot k_r^{d_r}\right)$.

<u>הקדמה לאלגוריתם הצפנה</u>: אם p,q שני ראשוניים גדולים ו- $n=p\cdot q$. לדעת את p,q זה כמו לדעת את $\varphi(n)$. כיוון אחד: מכיוון ש- $p,q\neq 2$, n אי זוגי. $\varphi(n)=(p-1)(q-1)=n+1-(p+q)$. בכיוון ההפוך: אם יודעים את n ואת $\varphi(n)$ אז יודעים את $p\cdot q$ ואת $p+q$. אזי p,q הם שורשים של x^2-ax+b כאשר $b=pq=n$ ו- $a=p+q=n+1-\varphi(n)$.

מערכות הצפנה פשוטות

אם A רוצה לשלוח הודעה ל-B בלי ש-C (שנמצאת באמצע) תשמע, A מצפינה את הטקסט. במקום לשלוח את הטקסט המקורי (*plaintext*) היא שולחת טקסט מוצפן (*ciphertext*). בדרך כלל, הטקסט המוצפן והטקסט המקורי נכתבים באותו א"ב. למשל, A-Z,0-9, או ביחידות הודעה. באופן יותר פורמלי, A מחפשת $f:P\to C$ שתהיה חח"ע להפצנה, ואז $f^{-1}:C\to P$ לפענוח.

<u>הגדרה:</u> f,f^{-1} נקראים **מערכת הצפנה**.
<u>מערכת ההצפנה של יוליוס קיסר:</u> נעביר כל אות ב-A-Z למספרה הסידורי. ואז: $P=\{0,\ldots,25\}$. אזי: $f(p)=(p+3)\,mod\,26$. למשל, אם רוצים לכתוב YES, כלומר $24,4,28$ מקבלים $1,7,21$, כלומר BHV. ואז: $f^{-1}(c)=(c-3)\,mod\,26$. באופן כללי, למערכת עם N אותיות, $f(p)=(p+b)\,mod\,N$ כאשר b הוא מפתח הצפנה. איך יודעים למצוא את b? באמצעות ניתוח שכיחויות של אותיות בשפה המתאימה. אם יודעים את מפתח ההצפנה, יודעים גם את $-b$ שהוא מפתח הפענוח.
<u>הצפנה אופיינית:</u> אם ביחידת הודעה יש k אותיות ובא"ב יש N אותיות, אזי $p\in(\mathbb{Z}/N\mathbb{Z})^k$ ו- $A\in Mat_{k\times k}(\mathbb{Z}/N\mathbb{Z})$ ו- $b\in(\mathbb{Z}/N\mathbb{Z})^k$, אזי $c=Ap+b$. ואז, מפתח ההצפנה הוא (A,b). ואז: $p=A^{-1}(c-b)=A^{-1}c-A^{-1}b$, ולכן מפתח הפענוח הוא $(A^{-1},-A^{-1}b)$. המערכת היא סימטרית.
<u>RSA:</u> מערכת הצפנה לא סיטמרית על שם *Rivest, Shamir, Adelman* משנת 1987. *Shamir* ו-*Adelman* הם ישראלים. כל משתמש בוחר שני מספרים ראשוניים גדולים מאוד, בערך עם 200 ספרות עשרוניות. נסמן אותם ב-p,q. המשתמש יחשב את $n=pq$. אזי $\varphi(n)=(p-1)(q-1)=n+1-(p+q)$. כל אחד יבחר $1\le e\le\varphi(n)$ זר ל-$\varphi(n)$. כלומר, A תבחר את p_A,q_A. אז היא תבחר e_A זר ל-$\varphi(n_A)$ כאשר $n_A=p_A\cdot q_A$. נסמן: d_A – ההפוך של e_A מודולו $\varphi(n_A)$, כלומר $d_A\equiv e_A^{-1}(\varphi(n_A))$. כעת, A תפרסם את מפתח ההצפנה $K_{E,A}=(n_A,e_A)$, ותסתיר את מפתח הפענוח $K_{D,A}=(n_A,d_A)$. ההצפנה תעבוד בצורה הבאה: $f:\mathbb{Z}/n_A\mathbb{Z}\to\mathbb{Z}/n_A\mathbb{Z}$, כאשר $f(p)=p^{e_A}mod\,n_A$. הפענוח יעבוד בצורה הבאה: $f^{-1}(x)=c^{d_A}mod\,n_A$. למה זה אכן פענוח? $(f^{-1}\circ f)(p)=p^{e_Ad_A}mod\,n_A$ אבל $e_Ad_A\equiv1(\varphi(n_A))$ $\Leftarrow$ $p^{e_Ad_A}\equiv p^1\cdot\left(p^{\varphi(n_A)}\right)^k\equiv p(n_A)$ $\Leftarrow$ $f^{-1}\circ f=id$.

בדיקת ראשוניות

<u>אלגוריתם קל:</u> כדי לבדוק אם n ראשוני, לוקחים $m<n$ ומנסים לחלק. אפשרות אחרת: $m<\sqrt{n}$ אי זוגי, ובודקים שאכן $m\nmid n$. יש $0.5\sqrt{n}$ מספרים לחלק. יעילות האלגוריתם: $O\left(e^{0.5\log n}\right)$. לכן, הזמן הוא אקספוננציאלי ב-$\log n$.
אלגוריתם אחר: אם n ראשוני, אז לכל b המקיים $\gcd(b,n)=1$ מתקיים $b^{n-1}\equiv1(n)$.
<u>הגדרה:</u> אם $n\in\mathbb{Z}$, אומרים ש-n הוא **פסאודו ראשוני** לבסיס b אם $b^{n-1}\equiv1(n)$.
<u>דוגמה:</u> $n=91$, $b=3$: $3^{90}\equiv1(91)$, ולכן 91 הוא פסאודו ראשוני לבסיס 3. אבל $2^{90}\equiv64(91)$, ולכן 91 אינו ראשוני.
<u>הגדרה:</u> מספר מורכב n כך ש-$\forall b\in(\mathbb{Z}/n\mathbb{Z})^X.\, b^{n-1}\equiv1(n)$ נקרא **מספר קרמייקל** (*Carmichel*).
<u>דוגמה:</u> 561.
<u>טענה:</u>

1. אם n זוגי אז n אינו מספר קרמייקל.
2. אם n מתחלק בריבוע אז n אינו מספר קרמייקל.
3. אם n אי זוגי בלי ריבועים, אז n מספר קרמייקל $\Leftrightarrow$ לכל מחלק ראשוני $p|n$ מתקיים $(p-1)|(n-1)$.
4. אם n מספר קרמייקל, אז n הוא מכפלה של לפחות שלושה ראשוניים.

הסיכום נכתב לפי ההרצאות של פרופ' מיכאל בורובוי.