**פעולה בינארית**: תהא $A$ קבוצה אזי $*:A\times A\to A$.

**סימון**: תהא $*$ פעולה בינארית אזי $a*b=*\left(\langle a,b\rangle\right)$.

**חבורה**: תהא $G$ קבוצה ותהא $*$ פעולה בינארית אזי $\langle G,*\rangle$ המקיימת

- אסוציטיביות/קיבוציות: $\forall a,b,c\in A.a*\left(b*c\right)=\left(a*b\right)*c$.
- איבר יחידה: $\exists e\in A.\forall g\in G.e*g=g*e=g$.
- איבר הופכי/נגדי: $\forall g\in G.\exists h\in A.g*h=h*g=e_{G}$.

**סימון**: תהא $G$ חבורה אזי איבר היחידה של $G$ הינו $e_{G}$.

**סימון**: תהא $G$ חבורה ויהי $a\in G$ אזי האיבר ההופכי של $a$ הינו $a^{-1}$.

**חוג**: תהא $R$ קבוצה ויהיו $+,*:R^{2}\to R$ אזי $\langle R,*,+\rangle$ המקיימת

- $\langle R,+\rangle$ חבורה אבלית.
- אסוציטיביות/קיבוציות: $a*\left(b*c\right)=\left(a*b\right)*c$.
- איבר יחידה לכפל: $\exists e_{*}\in R.\forall g\in R.e_{*}*g=g*e_{*}=g$.
- חוק הפילוג: $\left(\left(b+c\right)*a=b*a+c*a\right)\wedge\left(a*\left(b+c\right)=a*b+a*c\right)$.

**שדה**: תהא $\mathbb{F}$ קבוצה ויהיו $+,*:\mathbb{F}^{2}\to\mathbb{F}$ אזי $\langle\mathbb{F},+,*\rangle$ המקיים

- $\langle\mathbb{F},+,*\rangle$ חוג.
- $\langle\mathbb{F}\backslash\left\{ e_{*}\right\} ,*\rangle$ חבורה אבלית.
- $e_{+}\neq e_{*}$.

**חזקה מושלמת**: $n\in\mathbb{N}$ עבורו קיימים $a\in\mathbb{N}_{+}$ וכן $b\in\mathbb{N}_{>1}$ המקיימים $n=a^{b}$.

**מקדם בינומי**: יהיו $k,n\in\mathbb{N}$ באשר $k\le n$ אזי $\binom{n}{k}=\frac{n!}{k!(n-k)!}$.

**סימון**: יהיו $k,n\in\mathbb{N}$ אזי $S_{n}^{(k)}=\sum_{i=1}^{n}i^{k}$.

**טענה**: $S_{n}^{(0)}=n$, $S_{n}^{(1)}=\frac{n(n+1)}{2}$, $S_{n}^{(2)}=\frac{n(n+1)(2n+1)}{6}$.

**הבינום של ניוטון**: יהיו $x,y\in\mathbb{R}$ וכן $n\in\mathbb{N}$ אזי $(x+y)^{n}=\sum_{k=0}^{n}\binom{n}{k}x^{k}y^{n-k}$.

**טענה**: $S_{n}^{(k)}=\frac{1}{k+1}\left(n^{k+1}-\sum_{t=0}^{k-1}\left(-1\right)^{k-t}\binom{k+1}{t}S_{n}^{(t)}\right)$.

**מסקנה**: $S_{n}^{(3)}=\frac{n^{4}+2n^{3}+n^{2}}{4}$.

**חוג חלקי ל־$\mathbb{C}$**: קבוצה $A\subseteq\mathbb{C}$ המקיימת

- $\langle A,+\rangle$ חבורה.
- סגירות לכפל: $\forall a,b\in A.ab\in A$.
- $1\in A$.

**טענה**: יהי $A$ חוג חלקי ל־$\mathbb{C}$ אזי $A$ חוג.

**טענה**: $\mathbb{Z}$ חוג חלקי ל־$\mathbb{C}$.

**הגדרה**: $\mathbb{Z}\left[\alpha\right]=\bigcup_{n=0}^{\infty}\left\{ \sum_{i=0}^{n}k_{i}\alpha^{i}\mid k\in\mathbb{Z}^{n}\right\}$.

**טענה**: יהי $m\in\mathbb{Z}$ עבורו $\sqrt{m}\notin\mathbb{Q}$ אזי $\left\{ 1,\sqrt{m}\right\}$ בת"ל מעל $\mathbb{Q}$.

**טענה**: יהי $m\in\mathbb{Z}$ עבורו $\sqrt{m}\notin\mathbb{Q}$ אזי $\mathbb{Z}\left[\sqrt{m}\right]$ חוג חלקי ל־$\mathbb{C}$.

**חוג השלמים של גאוס**: $\mathbb{Z}\left[i\right]=\left\{ a+bi\mid a,b\in\mathbb{Z}\right\}$.

**מסקנה**: $\mathbb{Z}\left[i\right]$ חוג חלקי ל־$\mathbb{C}$.

**חבורת ההפיכים**: יהי $A$ חוג חלקי ל־$\mathbb{C}$ אזי $A^{*}=\left\{ a\in A\mid\exists b\in A.ab=1\right\}$.

**טענה**: יהי $A$ חוג חלקי ל־$\mathbb{C}$ אזי $\langle A^{*},*\rangle$ חבורה.

**מחלק**: יהי $A$ חוג חלקי ל־$\mathbb{C}$ ויהי $b \in A$ אזי $a \in A\backslash\{0\}$ המקיים $\frac{b}{a} \in A$.

**סימון**: יהי $b \in A$ ויהי $a \in A\backslash\{0\}$ מחלק אזי $a \mid b$.

**טענה**: יהיו $a,b,c \in A$ עבורם $a \mid b$ וכן $b \mid c$ אזי $a \mid c$.

**טענה**: יהיו $a,b,c \in A$ עבורם $a \mid b$ וכן $a \mid c$ אזי $\forall v,u \in A.a \mid ub+vc$.

**יחס חברות**: $\sim$ יחס על $A$ המקיים $(a \sim b) \iff (\exists \varepsilon \in A^*.b = \varepsilon a)$.

**טענה**: יחס החברות הינו יחס שקילות.

**טענה**: יהיו $a,b \in A$ אזי ($a,b$ חברים) $\iff ((a \mid b) \wedge (b \mid a))$.

**טענה**: יהי $m \in \mathbb{Z}$ אזי חבריו של $m$ הם $\pm m$.

**טענה**: יהי $z \in \mathbb{Z}[i]$ אזי חבריו של $z$ הם $\{\pm z, \pm iz\}$.

**אי פריק (א"פ)**: $a \in A\backslash A^*$ המקיים $\forall b,c \in A.(a = bc) \implies (b \in A^*) \vee (c \in A^*)$.

**ראשוני**: $a \in A\backslash(A^* \cup \{0\})$ המקיים $\forall b,c \in A.(a \mid bc) \implies (a \mid b) \vee (a \mid c)$.

**טענה**: יהי $a \in A$ ראשוני אזי $a$ א"פ.

**טענה**: בחוג $\mathbb{Z}\left[\sqrt{-5}\right]$ מתקיים כי $2$ א"פ אך אינו ראשוני.

**תחום פריקות**: $A$ חוג חלקי של $\mathbb{C}$ המקיים לכל $a \in A\backslash(A^* \cup \{0\})$ קיימים $q_1 \ldots q_n \in A$ א"פ המקיימים $a = \prod_{i=1}^{n} q_i$.

**משפט פירוק לאי פריקים מעל $\mathbb{Z}$**: $\mathbb{Z}$ תחום פריקות.

**פונקציית הצמוד**: יהי $\alpha \in \mathbb{Z}$ עבורו $\sqrt{\alpha} \notin \mathbb{Q}$ נגדיר $\sigma : \mathbb{Z}[\sqrt{\alpha}] \to \mathbb{Z}[\sqrt{\alpha}]$ כך $\sigma(a + b\sqrt{\alpha}) = a - b\sqrt{\alpha}$.

**טענה**: יהיו $z,w \in \mathbb{Z}[\sqrt{\alpha}]$ מתקיים

- $\sigma(z+w) = \sigma(z) + \sigma(w)$.
- $\sigma(zw) = \sigma(z)\sigma(w)$.
- $\sigma(\sigma(z)) = z$.
- $\sigma$ חח"ע ועל.

**נורמה**: יהי $\alpha \in \mathbb{Z}$ עבורו $\sqrt{\alpha} \notin \mathbb{Q}$ נגדיר $N : \mathbb{Z}[\sqrt{\alpha}] \to \mathbb{Z}$ כך $N(z) = z\sigma(z)$.

**למה**: יהיו $z,w \in \mathbb{Z}[\sqrt{\alpha}]$ מתקיים

- $N(zw) = N(z)N(w)$.
- $(N(z) = 0) \iff (z = 0)$.

**טענה**: יהי $\alpha \in \mathbb{Z}$ עבורו $\sqrt{\alpha} \notin \mathbb{Q}$ אזי $\mathbb{Z}[\sqrt{\alpha}]^* = \{z \in \mathbb{Z}[\sqrt{\alpha}] \mid N(z) \in \{\pm 1\}\}$.

**משפט פירוק לאי פריקים מעל $\mathbb{Z}[\sqrt{\alpha}]$**: יהי $\alpha \in \mathbb{Z}$ עבורו $\sqrt{\alpha} \notin \mathbb{Q}$ אזי $\mathbb{Z}[\sqrt{\alpha}]$ תחום פריקות.

**תחום פריקות יחידה**: $A$ תחום פריקות המקיים לכל $a \in A\backslash(A^* \cup \{0\})$ קיימים $q_1 \ldots q_n$ א"פ יחידים המקיימים $a = \prod_{i=1}^{n} q_i$ עד כדי שינוי סדר הגורמים וחברות.

**משפט**: יהי $A$ תחום פריקות אזי ($A$ תחום פריקות יחידה) $\iff$ (כל $a \in A$ א"פ הינו ראשוני).

**מסקנה**: $\mathbb{Z}\left[\sqrt{-5}\right]$ אינו תחום פריקות יחידה.

**משפט חלוקה עם שארית ב־$\mathbb{Z}$**: יהיו $a,b \in \mathbb{Z}$ באשר $a > 0$ אזי קיימים ויחידים $q,r \in \mathbb{Z}$ באשר $0 \le r < a$ המקיימים $b = qa + r$.

**שארית חלוקה**: יהיו $a,b \in \mathbb{Z}$ באשר $a > 0$ ויהיו $q,r \in \mathbb{Z}$ באשר $0 \le r < a$ המקיימים $b = qa + r$ אזי $r$.

**סימון**: יהיו $a,b \in \mathbb{Z}$ ויהי $r \in \mathbb{Z}$ שארית החלוקה של $b$ ב־$a$ אזי $a \bmod b = r$.

**טענה**: יהיו $a,b \in \mathbb{Z}$ באשר $a > 0$ אזי (שארית החלוקה של $b$ ב־$a$ היא $0$) $\iff (a \mid b)$.

**מחלק משותף**: יהיו $a,b \in \mathbb{Z}$ באשר $(a,b) \neq 0$ אזי $d \in \mathbb{Z}$ המקיים $(d \mid a) \wedge (d \mid b)$.

**מחלק משותף מקסימלי (ממ"מ)**: יהיו $a,b\in\mathbb{Z}$ באשר $(a,b)\neq0$ אזי $\max\left\{ d\in\mathbb{Z}\mid(d\mid a)\wedge(d\mid b)\right\}$.

**סימון**: יהיו $a,b\in\mathbb{Z}$ אזי המחלק המשותף המקסימלי שלהם הינו $\gcd\left(a,b\right)$.

**משפט**: יהיו $a,b\in\mathbb{Z}$ אזי $\exists m,n\in\mathbb{Z}.\gcd\left(a,b\right)=ma+nb$.

**מסקנה**: יהיו $a,b\in\mathbb{Z}$ ויהי $d\in\mathbb{Z}$ מחלק משותף אזי $d\mid\gcd\left(a,b\right)$.

**טענה**: יהיו $a,b\in\mathbb{Z}$ ויהי $d\in\mathbb{Z}$ מחלק משותף אזי (לכל מחלק משותף $r\in\mathbb{Z}$ מתקיים $r\mid d$) $\Longleftarrow$ $(d=\gcd\left(a,b\right))$.

**מחלק משותף מקסימלי (ממ"מ)**: יהיו $a_{1}\ldots a_{n}\in\mathbb{Z}$ באשר $(a_{1}\ldots a_{n})\neq0$ אזי $\max\left\{ d\in\mathbb{Z}\mid\forall i\in\left[n\right].\left(d\mid a_{i}\right)\right\}$.

**סימון**: יהיו $a_{1}\ldots a_{n}\in\mathbb{Z}$ אזי המחלק המשותף המקסימלי שלהם הינו $\gcd\left(a_{1}\ldots a_{n}\right)$.

**משפט**: יהיו $a_{1}\ldots a_{n}\in\mathbb{Z}$ אזי $\exists u_{1}\ldots u_{n}\in\mathbb{Z}.\gcd\left(a_{1}\ldots a_{n}\right)=\sum_{i=1}^{n}u_{i}a_{i}$.

**אלגוריתם אוקלידס**: יהי $a\in\mathbb{Z}\backslash\left\{ 0\right\}$ ויהי $b\in\mathbb{N}$ אזי

```
function EuclideanAlgorithm(a, b)
    if b = 0
        return a
    else
        return EuclideanAlgorithm(b, a mod b)
```

**משפט**: יהי $a\in\mathbb{Z}\backslash\left\{ 0\right\}$ ויהי $b\in\mathbb{N}$ אזי $\text{EuclideanAlgorithm}\left(a,b\right)=\gcd\left(a,b\right)$.

**מספרים זרים**: $a,b\in\mathbb{Z}$ המקיימים $\gcd\left(a,b\right)=1$.

**מסקנה**: יהיו $a,b\in\mathbb{Z}$ זרים אזי $\exists m,n\in\mathbb{Z}.ma+nb=1$.

**משפט**: יהי $a\in\mathbb{Z}$ א"פ אזי $a$ ראשוני.

**מסקנה**: $\mathbb{Z}$ תחום פריקות יחידה.

**משפט אוקלידס**: קיימים אינסוף ראשוניים ב־$\mathbb{Z}$.

**טענה**: בסדרה $\left\{ 4n+3\right\} _{n=0}^{\infty}$ ישנם אינסוף ראשוניים.

**משפט דיריכלה**: יהיו $a,b\in\mathbb{N}_{+}$ זרים אזי בסדרה $\left\{ bn+a\right\} _{n=0}^{\infty}$ ישנם אינסוף ראשוניים.

**טענה**: תהא $\left\{ p_{n}\right\} _{n=1}^{\infty}$ סדרת הראשוניים אזי $p_{n}\leq2^{2^{n}}$.

**פונקציית ספירת ראשוניים**: $\pi\left(x\right)=\left|\left\{ p\leq x\mid\text{ראשוני }p\right\} \right|$.

**סימון**: יהיו $f,g\in\mathbb{R}\to\mathbb{N}$ המקיימות $\lim_{x\to\infty}\frac{f\left(x\right)}{g\left(x\right)}=1$ אזי $f\sim g$.

**משפט**: $\pi\left(x\right)\sim\frac{x}{\log\left(x\right)}$.

**טענה**: $\pi\left(x\right)>\log\log\left(x\right)$.

**אלגוריתם הנפה של ארטוסטנס**: יהי $n \in \mathbb{N} \setminus \{0,1\}$ אזי

$$
\begin{aligned}
&\textbf{function } \text{SieveOfEratosthenesAlgorithm}(n) \\
&\quad A \leftarrow \Big[\underset{2}{\text{true}}, \underset{3}{\text{true}}, \ldots, \underset{n}{\text{true}}\Big] \\
&\quad \textbf{for } i \leftarrow 2 \ldots n \\
&\quad\quad \textbf{if } A[i] = \text{true} \\
&\quad\quad\quad j \leftarrow 1 \\
&\quad\quad\quad \textbf{while } ij \le n \\
&\quad\quad\quad\quad A[ij] = \text{false} \\
&\quad\quad\quad\quad j \leftarrow j+1 \\
&\quad \textbf{return } A
\end{aligned}
$$

**משפט**: יהי $n \in \mathbb{N} \setminus \{0,1\}$ אזי כל אינדקס שמסומן כ־true בתשובת $\text{SieveOfEratosthenesAlgorithm}(n)$ הינו ראשוני.

**מספרי פרמה**: יהי $n \in \mathbb{N}$ אזי $F_n = 2^{2^n} + 1$.

**טענה**: יהיו $x, y \in \mathbb{R}$ ויהי $t \in \mathbb{N}_+$ אזי $x^t - y^t = (x-y)\sum_{i=0}^{t-1} x^i y^{t-i-1}$.

**טענה**: יהיו $m, n \in \mathbb{N}$ באשר $m \neq n$ אזי $\gcd(F_n, F_m) = 1$.

**מספרי מרסן**: יהי $p$ ראשוני אזי $M_p = 2^p - 1$.

**מספר מושלם**: $n \in \mathbb{N}_+$ המקיים $n = \sum_{\substack{d|n \\ d<n}} d$.

**פונקציית סכום המחלקים**: יהי $n \in \mathbb{N}_+$ אזי $\sigma(n) = \sum_{d|n} d$.

**טענה**: יהי $n \in \mathbb{N}_+$ אזי ($n$ מושלם) $\iff (\sigma(n) = 2n)$.

**פונקציה כפלית**: $f : \mathbb{N} \to \mathbb{C}$ המקיימת לכל $n, m \in \mathbb{N}$ זרים מתקיים $f(nm) = f(n) f(m)$.

**טענה**: תהא $f$ פונקציה כופלית ויהי $n \in \mathbb{N}$ עם פירוק לראשוניים $n = \prod_{m=1}^{k} p_m^{r_m}$ אזי $f(n) = \prod_{i=1}^{k} f(p_i^{r_i})$.

**טענה**: $\sigma$ פונקציה כפלית.

**טענה**: יהי $p \in \mathbb{N}$ ראשוני ויהי $n \in \mathbb{N}$ אזי $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$.

**מסקנה**: יהי $n \in \mathbb{N}$ עם פירוק לראשוניים $n = \prod_{m=1}^{k} p_m^{r_m}$ אזי $\sigma(n) = \prod_{m=1}^{k} \frac{p_m^{r_m+1}-1}{p_m - 1}$.

**טענה**: תהא $f$ פונקציה כפלית אזי $F(n) = \sum_{d|n} f(d)$ כפלית.

**פונקציית מביוס**: נגדיר $\mu : \mathbb{N} \to \{0, \pm 1\}$ כפלית יהי $p$ ראשוני אזי
$$\mu(p^r) = \begin{cases} 1 & r = 0 \\ -1 & r = 1 \\ 0 & r \geq 2 \end{cases}.$$

**משפט נוסחת ההיפוך של מביוס**: תהא $f : \mathbb{N} \to \mathbb{C}$ אזי $\left(f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right)\right) \iff \left(F(n) = \sum_{d|n} f(d)\right)$.

**משפט אוקלידס**: יהי $M_p$ ראשוני אזי $\frac{1}{2} M_p (M_p + 1)$ מושלם.

**משפט אוילר**: יהי $n \in \mathbb{N}_{\text{even}}$ מושלם אזי קיים $M_p$ ראשוני עבורו $n = \frac{1}{2} M_p (M_p + 1)$.

**שלשה פיתגורית**: $x,y,z\in\mathbb{N}_+$ המקיימים $x^2+y^2=z^2$.

**אלגוריתם מציאת כל הנקודות הרציונליות על חתך חרוט**: יהיו $r,s\in\mathbb{Q}$ ותהא עקומה $rx^2+sy^2=1$

1. מצא פתרון רציונלי $(a,b)$.
2. מצאו את נקודות החיתוך בין הישר העובר דרך $(0,t),(a,b)$ ובין העקומה.

**משפט**: יהי $t\in\mathbb{R}$ אזי $(t\in\mathbb{Q})\iff\left(\left(\frac{t^2-1}{t^2+1}\in\mathbb{Q}\right)\wedge\left(\frac{2t}{t^2+1}\in\mathbb{Q}\right)\right)$.

**משפט**: $f:\mathbb{Q}\to\{(x,y)\in\mathbb{Q}^2\mid x^2+y^2=1\}\backslash\{(1,0)\}$ המוגדרת $f(t)=\left(\frac{t^2-1}{t^2+1},\frac{2t}{t^2+1}\right)$ הינה חח"ע ועל.

**משפט**: $\mathrm{sols}_{\mathbb{Q}}(x^2+y^2=1)=\{(1,0)\}\cup\left\{\left(\frac{t^2-1}{t^2+1},\frac{2t}{t^2+1}\right)\;\middle|\;t\in\mathbb{Q}\right\}$.

**מסקנה**: תהא $\begin{pmatrix}x\\y\\z\end{pmatrix}\in\mathbb{N}_+^3$ שלשה פתגורית אזי מתקיים אחד מהבאים

- קיימים $u,v\in\mathbb{N}_{\mathrm{odd}}$ המקיימים $\gcd(u,v)=1$ עבורם $\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}\frac{u^2-v^2}{2}\\\frac{u^2+v^2}{2}\\uv\end{pmatrix}$.
- קיימים $u,v\in\mathbb{N}_+$ המקיימים $u+v\in\mathbb{N}_{\mathrm{odd}}$ וכן $\gcd(u,v)=1$ עבורם $\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}u^2-v^2\\2uv\\u^2+v^2\end{pmatrix}$.

**מספרים קונגרואנטים**: יהי $n\in\mathbb{N}_+$ אזי $a,b\in\mathbb{Z}$ המקיימים $n\mid a-b$.

**סימון**: יהי $n\in\mathbb{N}_+$ ויהיו $a,b\in\mathbb{Z}$ קונגרואנטים מודולו $n$ אזי $a\equiv b\mod n$.

**טענה**: יהי $n\in\mathbb{N}_+$ אזי יחס הקונגרואציה מודלו $n$ הינו יחס שקילות על $\mathbb{Z}$.

**סימון**: $a+n\mathbb{Z}=\{a+n\cdot m\mid m\in\mathbb{Z}\}$.

**טענה**: יהי $n\in\mathbb{N}_+$ אזי $[a]_{\mathrm{mod}n}=a+n\mathbb{Z}$.

**מסקנה**: $\mathbb{Z}/_{\mathrm{mod}n}=\{a+n\mathbb{Z}\mid a\in\{0\ldots n-1\}\}$.

**סימון**: $\mathbb{Z}_n=\mathbb{Z}/_{\mathrm{mod}n}$.

**טענה**: יהי $n\in\mathbb{N}_+$ ויהיו $a,a',b,b'\in\mathbb{Z}$ המקיימים $a\equiv a'\mod n$ וכן $b\equiv b'\mod n$ אזי

- $a+b\equiv a'+b'\mod n$.
- $ab\equiv a'b'\mod n$.

**מסקנה**: יהי $f\in\mathbb{Z}[x]$ ויהיו $b,c\in\mathbb{Z}$ המקיימים $b\equiv c\mod n$ אזי $f(b)\equiv f(c)\mod n$.

**משפט סימן החלוקה**: יהי $n\in\mathbb{Z}$ מתקיים

- סימן חלוקה ב־2: (ספרת האחדות של $n$ היא זוגית) $\iff(2\mid n)$.
- סימן חלוקה ב־5: (ספרת האחדות של $n$ היא $\{0,5\}$) $\iff(5\mid n)$.
- סימן חלוקה ב־10: (ספרת האחדות של $n$ היא 0) $\iff(10\mid n)$.
- סימן חלוקה ב־3: (סכום הספרות של $n$ מתחלק ב־3) $\iff(3\mid n)$.

**אריתמטיקה של מחלקות קונגרואציה**: יהי $n\in\mathbb{N}_+$ ויהיו $(a+n\mathbb{Z}),(b+n\mathbb{Z})\in\mathbb{Z}_n$ אזי

- חיבור: $(a+n\mathbb{Z})+(b+n\mathbb{Z})=(a+b)+n\mathbb{Z}$.
- כפל: $(a+n\mathbb{Z})\cdot(b+n\mathbb{Z})=ab+n\mathbb{Z}$.

**טענה**: $\mathbb{Z}_n$ חוג עם אריתמטיקה של מחלקות קונגרואציה.

**איבר הפיך ב־$\mathbb{Z}_n$**: $a\in\mathbb{Z}_n$ המקיים $\exists b\in\mathbb{Z}_n.a\cdot b=1$.

**איבר הפיך מודולו $n$**: $a\in\mathbb{Z}$ המקיים $\exists b\in\mathbb{Z}.a\cdot b\equiv1\mod n$.

**טענה**: יהי $a\in\mathbb{Z}$ אזי ($a$ הפיך מודולו $n$) $\iff$ ($a+n\mathbb{Z}$ הפיך ב־$\mathbb{Z}_n$).

**טענה**: יהי $a$ הפיך ב־$\mathbb{Z}_n$ אזי $\exists!b\in\mathbb{Z}_n.a\cdot b=1$.

**טענה**: יהי $a\in\mathbb{Z}$ אזי ($a$ הפיך מודולו $n$) $\iff(\gcd(a,n)=1)$.

**סימון:** $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z}_n . a \cdot b = 1\}$.

**סימון:** $\overline{a} = a + n\mathbb{Z}$.

**סימון:** יהי $\overline{a} \in \mathbb{Z}_n$ הפיך ויהי $\overline{b} \in \mathbb{Z}_n$ המקיים $\overline{a}\overline{b} = \overline{1}$ אזי $(\overline{a})^{-1} = \overline{b}$.

**טענה:** $\left(\overline{a} \cdot \overline{b}\right)^{-1} = \overline{a}^{-1} \cdot \overline{b}^{-1}$.

**פונקציית אוילר:** $\phi(n) = |\mathbb{Z}_n^*|$.

**טענה:** יהי $p \in \mathbb{N}$ ראשוני אזי $\phi(p) = p - 1$.

**מסקנה:** יהי $p \in \mathbb{N}$ ראשוני אזי $\mathbb{Z}_p$ שדה.

**טענה:** יהי $n \in \mathbb{N}_+$ אזי ($\mathbb{Z}_n$ שדה) $\iff$ ($n$ ראשוני).

**טענה:** יהיו $n, k \in \mathbb{N}_+$ זרים אזי $(a \equiv b \mod n) \iff \forall a, b \in \mathbb{Z}. (ka \equiv kb \mod n)$.

**טענה:** יהיו $n, k \in \mathbb{N}_+$ ויהי $r \in \mathbb{N}$ מחלק משותף אזי $\left(\frac{k}{r}a \equiv \frac{k}{r}b \mod \frac{n}{r}\right) \iff \forall a, b \in \mathbb{Z}. (ka \equiv kb \mod n)$.

**מסקנה:** יהיו $n, k \in \mathbb{N}_+$ אזי $\left(a \equiv b \mod \frac{n}{\gcd(k,n)}\right) \iff \forall a, b \in \mathbb{Z}. (ka \equiv kb \mod n)$.

**טענה:** יהי $p \in \mathbb{N}$ ראשוני ויהי $m \in \mathbb{N}_+$ המקיימים $p \mid m$ אזי $\phi(pm) = p\phi(m)$.

**טענה:** יהי $p \in \mathbb{N}$ ראשוני ויהי $m \in \mathbb{N}_+$ המקיימים $p \nmid m$ אזי $\phi(pm) = (p-1)\phi(m)$.

**מסקנה:** יהיו $s, \ell \in \mathbb{N}_+$ ויהי $p \in \mathbb{N}$ ראשוני המקיים $p \nmid s$ אזי $\phi\left(p^\ell \cdot s\right) = \begin{cases} p^{\ell-1}(p-1) & s = 1 \\ p^{\ell-1}(p-1)\phi(s) & \text{else} \end{cases}$.

**מסקנה:** יהי $n \in \mathbb{N}$ עם פירוק לראשוניים $n = \prod_{m=1}^k p_m^{r_m}$ אזי $\phi(n) = \prod_{i=1}^k p_i^{r_i - 1}(p_i - 1)$.

**מסקנה:** $\phi$ פונקציה כפלית.

**טענה:** יהי $n \in \mathbb{N}_+$ אזי $\sum_{d \mid n} \phi(d) = n$.

**ראשוני סופי ז'רמן:** $q \in \mathbb{N}$ ראשוני המקיים $2q + 1$ ראשוני.

**משפט:** יהי $n \in \mathbb{N}$ ויהי $q \in \mathbb{N} \setminus \{2\}$ ראשוני עבורם $\phi(n) = 2q$ אזי $q$ ראשוני סופי ז'רמן.

**טענה:** יהי $n \in \mathbb{N}_+$ אזי $\sum_{\substack{\gcd(k,n)=1 \\ 1 \le k \le n}} k = \frac{1}{2} n\phi(n)$.