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

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

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

- $\left\langle R,+\right\rangle$ 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 $\left\langle \mathbb{F},+,*\right\rangle$ המקיים

- $\left\langle \mathbb{F},+,*\right\rangle$ חוג.
- $\left\langle \mathbb{F}\backslash\left\{ e_{*}\right\} ,*\right\rangle$ 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 $\binom{n}{k}=\frac{n!}{k!\left(n-k\right)!}$.

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

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

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

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

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

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

- $\left\langle A,+\right\rangle$ 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 $\left\langle A^{*},*\right\rangle$ 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 $(\exists\varepsilon\in A^{*}.b=\varepsilon a)\iff(a\sim b)$.

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
- $\sigma(z+w)=\sigma(z)+\sigma(w)$.
- $\sigma(zw)=\sigma(z)\sigma(w)$.
- $\sigma(\sigma(z))=z$.
- σ 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 $\mathbb{Z}[\sqrt{\alpha}]^{*}=\{z\in\mathbb{Z}[\sqrt{\alpha}]\mid N(z)\in\{\pm1\}\}$.

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 $(a,b)\neq0$ 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 $a\in\mathbb{Z}$ אזי a 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 $p_{n}\le2^{2^{n}}$.
סימון: $\mathbb{P}=\left\{ p\in\mathbb{N}\mid\text{ראשוני }p\right\}$.
פונקציית ספירת ראשוניים: $\pi\left(x\right)=\left|\left\{ p\in\mathbb{P}\mid p\le x\right\} \right|$.
סימון: יהיו $f,g\in\mathbb{R}\to\mathbb{N}$ המקיימות $\lim_{x\to\infty}\frac{f(x)}{g(x)}=1$ אזי $f\sim g$.
משפט: $\pi\left(x\right)\sim\frac{x}{\log(x)}$.
טענה: $\pi\left(x\right)>\log\log\left(x\right)$.

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

$$
\begin{array}{l}
\textbf{function } \mathrm{SieveOfEratosthenesAlgorithm}(n)\\
\quad| \ A\leftarrow\left[\underset{2}{\mathrm{true}},\underset{3}{\mathrm{true}},\ldots,\underset{n}{\mathrm{true}}\right]\\
\quad| \ \textbf{for } i\leftarrow 2\ldots n\\
\quad| \qquad | \ \textbf{if } A[i]=\mathrm{true}\\
\quad| \qquad | \qquad | \ j\leftarrow 1\\
\quad| \qquad | \qquad | \ \textbf{while } ij\le n\\
\quad| \qquad | \qquad | \qquad | \ A[ij]=\mathrm{false}\\
\quad| \qquad | \qquad | \qquad | \ j\leftarrow j+1\\
\quad| \ \textbf{return } A
\end{array}
$$

משפט: יהי $n\in\mathbb{N}\backslash\{0,1\}$ אזי כל אינדקס שמסומן כ־true בתשובת $\mathrm{SieveOfEratosthenesAlgorithm}(n)$ 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 $x^t-y^t=(x-y)\sum_{i=0}^{t-1}x^iy^{t-i-1}$.

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

מספרי מרסן: יהי $p\in\mathbb{P}$ 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 $n=\prod_{m=1}^kp_m^{r_m}$ אזי $f(n)=\prod_{i=1}^kf(p_i^{r_i})$.

טענה: σ פונקציה כפלית.

טענה: יהי $p\in\mathbb{P}$ 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 $n=\prod_{m=1}^kp_m^{r_m}$ 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 $\mu:\mathbb{N}\to\{0,\pm1\}$ כפלית יהי $p\in\mathbb{P}$ ויהי $r\in\mathbb{N}_+$ אזי $\mu(p^r)=\begin{cases}1 & r=0\\-1 & r=1\\0 & r\ge2\end{cases}$.

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 $M_p\in\mathbb{P}$ אזי $\frac{1}{2}M_p(M_p+1)$ מושלם.

משפט אוילר: יהי $n\in\mathbb{N}_{\mathrm{even}}$ מושלם אזי $\exists k\in\mathbb{N}.(M_k\in\mathbb{P})\wedge\left(n=\frac{1}{2}M_k(M_k+1)\right)$.

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.
   - פתור את מערכת המשוואות $\begin{cases}(t-b)x+a(y-t)=0\\ rx^2+sy^2=1\end{cases}$.
3. החזר את כל פתרונות החיתוך עבור $t\in\mathbb{Q}$.

טענה: יהיו $r,s\in\mathbb{Q}$ אזי (אלגוריתם מציאת כל הנקודות הרציונליות על חתך חרוט)$=\text{sols}_{\mathbb{Q}}\left(rx^2+sy^2=1\right)$.

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

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

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

- קיימים $u,v\in\mathbb{N}_{\text{odd}}$ 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 $u+v\in\mathbb{N}_{\text{odd}}$ 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 $[a]_{\text{mod}n}=a+n\mathbb{Z}$.

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

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

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 $\exists b\in\mathbb{Z}.a\cdot b\equiv 1 \mod n$.

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: $\bar{a}=a+n\mathbb{Z}$.

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

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

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

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

מסקנה: יהי $p\in\mathbb{P}$ אזי $\mathbb{Z}_p$ שדה.

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

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 $p\in\mathbb{P}$ ויהי $m\in\mathbb{N}_+$ עבורו $p\mid m$ אזי $\phi(pm)=p\phi(m)$.

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

מסקנה: יהיו $s,\ell\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ 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: ϕ פונקציה כפלית.

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

ראשוני סופי ז'רמן: $q\in\mathbb{P}$ עבורו $2q+1\in\mathbb{P}$.

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

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

משפט: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהי $b\in\mathbb{Z}$ ויהי $n\in\mathbb{N}_+$ אזי $(\gcd(a,n)\mid b) \iff (\text{sols}_{\mathbb{Z}_n}(ax=b)\neq\varnothing)$.

למה: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהיו $b,c\in\mathbb{Z}$ ויהי $n\in\mathbb{N}_+$ המקיימים $\gcd(a,n)\mid b$ וכן $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv 1 \mod \frac{n}{\gcd(a,n)}$ אזי $\text{sols}_{\mathbb{Z}_n}(ax=b)=\left\{\frac{cb+rn}{\gcd(a,n)}\mid r\in\mathbb{Z}\right\}$.

משפט: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהיו $b,c\in\mathbb{Z}$ ויהי $n\in\mathbb{N}_+$ המקיימים $\gcd(a,n)\mid b$ וכן $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv 1 \mod \frac{n}{\gcd(a,n)}$ אזי $\text{sols}_{\mathbb{Z}_n}(ax=b)=\left\{\frac{cb+kn}{\gcd(a,n)}\mid 0\le k\le\gcd(a,n)\right\}$.

מסקנה: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהיו $b,c\in\mathbb{Z}$ ויהי $n\in\mathbb{N}_+$ המקיימים $\gcd(a,n)\mid b$ אזי $|\text{sols}_{\mathbb{Z}_n}(ax=b)|=\gcd(a,n)$.

משפט פתרון משוואות דיופנטיות לינאריות: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהיו $b,c,\alpha\in\mathbb{Z}$ ויהי $n\in\mathbb{N}_+$ המקיימים $\gcd(a,n)\mid b$ וגם $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv 1 \mod \frac{n}{\gcd(a,n)}$ וכן $\frac{ac}{\gcd(a,n)}=1+\frac{\alpha n}{\gcd(a,n)}$ אזי $\text{sols}_{\mathbb{N}^2}(ax+ny=b)=\left\{\left(\frac{cb+rn}{\gcd(a,n)},-\frac{\alpha b+ra}{\gcd(a,n)}\right)\mid r\in\mathbb{Z}\right\}$.

משפט השאריות הסיני: יהיו $n_1\ldots n_k\in\mathbb{N}_+$ זרים בזוגות ויהיו $c_1\ldots c_k\in\mathbb{Z}$ אזי $\exists! x\in\mathbb{Z}_{\prod_{i=1}^k n_i}.\begin{cases}x\equiv c_1 & \mod n_1\\ \vdots & \\ x\equiv c_k & \mod n_k\end{cases}$.

משפט אוילר: יהי $n \in \mathbb{N}\backslash\{0,1\}$ ויהי $a \in \mathbb{Z}$ המקיים $\gcd(a,n)=1$ אזי $a^{\phi(n)} \equiv 1 \mod n$.

מסקנה: יהי $n \in \mathbb{N}\backslash\{0,1\}$ ויהי $a \in \mathbb{Z}$ המקיים $\gcd(a,n)=1$ אזי $a^{\phi(n)-1} \cdot a \equiv 1 \mod n$.

מסקנה: יהי $n \in \mathbb{N}\backslash\{0,1\}$ ויהיו $a,x \in \mathbb{Z}$ המקיימים $\gcd(a,n)=1$ אזי $a^x \equiv a^{x \mod \phi(n)} \mod n$.

המשפט הקטן של פרמה: יהי $p \in \mathbb{P}$ ויהי $a \in \mathbb{Z}$ המקיים $\gcd(a,p)=1$ אזי $a^{p-1} \equiv 1 \mod p$.

הגדרה: $\mathbb{Z}_n[x] = \bigcup_{m=0}^{\infty}\left\{\sum_{i=0}^{m} a_i x^i \mid \forall i \in [m] . a_i \in \mathbb{Z}_n\right\}$.

הגדרה: יהיו $\sum_{i=0}^{m} a_i x^i, \sum_{i=0}^{m} b_i x^i \in \mathbb{Z}_n[x]$ אזי $(a_i = b_i) \iff \left(\sum_{i=0}^{m} a_i x^i = \sum_{i=0}^{m} b_i x^i\right)$.

סימון: יהיו $f,g \in \mathbb{Z}_n[x]$ אזי $(f=g) \iff (f \equiv g \mod n)$.

אריתמטיקה ב־$\mathbb{Z}_n[x]$: יהיו $\sum_{i=0}^{m} a_i x^i, \sum_{i=0}^{k} b_i x^i \in \mathbb{Z}_n[x]$ אזי

- $\left(\sum_{i=0}^{m} a_i x^i\right) + \left(\sum_{i=0}^{k} b_i x^i\right) = \sum_{i=0}^{\max\{m,k\}} (a_i + b_i) x^i$.
- $\left(\sum_{i=0}^{m} a_i x^i\right) \cdot \left(\sum_{i=0}^{k} b_i x^i\right) = \sum_{i=0}^{m+k} \left(\sum_{\ell=0}^{i} a_\ell b_{i-\ell}\right) x^i$.

משפט וילסון: יהי $p \in \mathbb{P}$ אזי $(p-1)! \equiv -1 \mod p$.

טענה: יהי $f \in \mathbb{Z}[x]$ ויהי $m \in \mathbb{N}$ עם פירוק $m = \prod_{i=1}^{k} p_i^{r_i}$ אזי $\left|\text{sols}_{\mathbb{Z}_m}(f(x)=0)\right| = \prod_{i=1}^{k}\left|\text{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x)=0)\right|$.

מסקנה: יהי $f \in \mathbb{Z}[x]$ ויהי $m \in \mathbb{N}$ עם פירוק $m = \prod_{i=1}^{k} p_i^{r_i}$ אזי $\left(\forall i \in [k] . \text{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x)=0) \neq \varnothing\right) \iff (\text{sols}_{\mathbb{Z}_m}(f(x)=0) \neq \varnothing)$.

משפט: יהי $f \in \mathbb{Z}[x]$ יהי $p \in \mathbb{P}$ ויהי $a_1 \in \mathbb{Z}$ פתרון של $f(x) \equiv 0 \mod p$ וכן $f'(a_1) \not\equiv 0 \mod p$ יהי $j \in \mathbb{N}\backslash\{0,1\}$ אזי קיים ויחיד $a_j \in \mathbb{Z}_{p^j}$ המקיים $f(a_j) \equiv 0 \mod p^j$ וכן $a_j \equiv a_{j-1} \mod p^{j-1}$.

הרמת פתרון: יהי $f \in \mathbb{Z}[x]$ יהי $p \in \mathbb{P}$ יהי $j \in \mathbb{N}_+$ ויהיו $a_j, c \in \mathbb{Z}$ עבורם $f(a_j) \equiv 0 \mod p^j$ אזי $a_j + cp^j \in \mathbb{Z}_{p^{j+1}}$ המקיים $f(a_j + cp^j) \equiv 0 \mod p^{j+1}$.

סדר: יהי $n \in \mathbb{N}\backslash\{0,1\}$ ויהי $a \in \mathbb{Z}_n^*$ אזי $\text{ord}_n(a) = \min\left\{d \in \mathbb{N}_+ \mid a^d \equiv 1 \mod n\right\}$.

טענה: יהי $a \in \mathbb{Z}_n^*$ אזי $(\text{ord}_n(a) \mid k) \iff (a^k \equiv 1 \mod n) . \forall k \in \mathbb{N}_+$.

מסקנה: יהי $a \in \mathbb{Z}_n^*$ אזי $\text{ord}_n(a) \mid \phi(n)$.

טענה: יהי $a \in \mathbb{Z}_n^*$ אזי $\left\{1, a, a^2, \ldots, a^{\text{ord}_n(a)-1}\right\}$ תת חבורה של $\mathbb{Z}_n^*$.

טענה: יהי $a \in \mathbb{Z}_n^*$ ויהי $m \in \mathbb{Z}$ אזי $\text{ord}_n(a^m) = \frac{\text{ord}_n(a)}{\gcd(m, \text{ord}_n(a))}$.

שורש פרימיטיבי: יהי $n \in \mathbb{N}\backslash\{0,1\}$ אזי $a \in \mathbb{Z}_n^*$ המקיים $\text{ord}_n(a) = \phi(n)$.

טענה: יהי $a \in \mathbb{Z}_n^*$ שורש פרימיטיבי אזי קיימים $\phi(\phi(n))$ שורשים פרימיטיביים מודולו n.

משפט: יהי $p \in \mathbb{P}$ אזי קיים שורש פרימיטיבי מודולו p.

משפט: יהי $p \in \mathbb{P}\backslash\{2\}$ ויהי $j \in \mathbb{N}_+$ אזי קיים שורש פרימיטיבי מודולו p^j.

מסקנה: יהי $p \in \mathbb{P}\backslash\{2\}$ ויהי $j \in \mathbb{N}_+$ אזי קיים שורש פרימיטיבי מודולו $2p^j$.

למה: יהי $j \in \mathbb{N}\backslash\{0,1,2\}$ ויהי $b \in \mathbb{N}_{\text{odd}}$ אזי $b^{2^{j-2}} \equiv 1 \mod 2^j$.

מסקנה: יהי $j \in \mathbb{N}\backslash\{0,1,2\}$ ויהי $b \in \mathbb{N}_{\text{odd}}$ אזי $\text{ord}_{2^j}(b) \mid 2^{j-2}$.

טענה: יהי $j \in \mathbb{N}\backslash\{0,1,2\}$ אזי לא קיים שורש פרימיטיבי מודולו 2^j.

למה: יהיו $n_1, n_2 \in \mathbb{N}\backslash\{0,1,2\}$ זרים ויהי $a \in \mathbb{Z}_{n_1 n_2}^*$ אזי $a^{\frac{1}{2}\phi(n_1 n_2)} \equiv 1 \mod n_1 n_2$.

משפט: יהי $n \in \mathbb{N}_+$ אזי (קיים שורש פרימיטיבי מודולו n) $\iff \left(n \in \{1,2,4\} \cup \left\{p^j \mid \substack{p \in \mathbb{P} \\ j \in \mathbb{N}_+}\right\} \cup \left\{2p^j \mid \substack{p \in \mathbb{P} \\ j \in \mathbb{N}_+}\right\}\right)$.

משפט: יהי $n \in \mathbb{N}$ בעל שורש פרימיטיבי יהי $a \in \mathbb{Z}_n^*$ ויהי $m \in \mathbb{N}_+$ אזי $\left(a^{\frac{\phi(n)}{\gcd(m,\phi(n))}} \equiv 1 \mod n\right) \iff (\text{sols}_{\mathbb{Z}_n}(x^m = a) \neq \varnothing)$.

מסקנה: יהי $n \in \mathbb{N}$ בעל שורש פרימיטיבי ויהי $m \in \mathbb{N}_+$ נגדיר $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ כך $f(x) \equiv x^m \mod n$ אזי $\text{Im}(f) = \left\{a \in \mathbb{Z}_n^* \;\middle|\; a^{\frac{\phi(n)}{\gcd(m,\phi(n))}} \equiv 1 \mod n\right\}$.

טענה: יהיו $n,m \in \mathbb{N}_+$ באשר $\gcd(m,\phi(n)) = 1$ אזי $f : \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ המוגדרת $f(x) \equiv x^m \mod n$ חח"ע ועל.

אלגוריתם RSA:

- נבחר $p,q\in\mathbb{P}$ גדולים, ונסמן $n=pq$.
- נבחר $m\in\mathbb{Z}_{\phi(n)}^{*}$, ונחשב $s\equiv m^{-1}\mod\phi(n)$.
- נפרסם את (n,m) ונשמור בסוד על s.
- כאשר מישהו שולח לנו את ההודעה A הוא יחשב $B\equiv A^{m}\mod n$ וישלח את B, רק מי שיודע את s יוכל לפצח את B כך $A\equiv B^{s}\mod n$.

טענה: יהיו $p,q\in\mathbb{P}$ נסמן $N=pq$ נניח כי אנו יודעים את $N,\phi(N)$ אזי אנו יודעים את p,q ב־$\mathcal{O}(1)$.

טענה: מציאת פתרון למשוואה $x^{m}\equiv B\mod n$ באלגוריתם RSA שקול למציאת p,q.

טענה: מציאת p,q באלגוריתם RSA זוהי בעיה לא פתירה בזמן סביר. לא ניכנס כאן פורמלית לסיבוכיות פירוק לראשוניים

טענה תנאי הכרחי לראשוניות: יהי $n\in\mathbb{N}_{+}$ ויהי $a\in\mathbb{Z}_{n}^{*}$ המקיים $a^{n-1}\not\equiv1\mod n$ אזי $n\notin\mathbb{P}$.

מספרי קרמייקל: $n\in\mathbb{N}_{+}\backslash\mathbb{P}$ עבורו $\forall a\in\mathbb{Z}_{n}^{*}.a^{n-1}\equiv1\mod n$.

טענה: יהי $k\in\mathbb{N}\backslash\{0,1\}$ ויהי $n\in\mathbb{N}_{+}$ עם פירוק לראשוניים זרים $n=\prod_{i=1}^{k}p_{i}$ המקיימים $(n-1)\,|\,(p_{i}-1)\,.\,\forall i\in[k]$ אזי n מספר קרמייקל.

הגדרה: נגדיר $\lambda:\mathbb{N}_{+}\to\mathbb{N}_{+}$ כך

- $\lambda(1)=1$.
- $\lambda(2)=\phi(2)=1$.
- $\lambda(4)=\phi(4)=2$.
- יהי $j\in\mathbb{N}\backslash\{0,1,2\}$ אזי $\lambda(2^{j})=2^{j-2}$.
- יהי $p\in\mathbb{P}\backslash\{2\}$ ויהי $j\in\mathbb{N}_{+}$ אזי $\lambda(p^{j})=\phi(p^{j})=p^{j-1}(p-1)$.
- יהי $n\in\mathbb{N}_{+}$ עם פירוק לראשוניים $n=2^{j_{0}}\prod_{i=1}^{k}p_{i}^{j_{i}}$ אזי $\lambda(n)=\text{lcm}\left(\lambda(2^{j_{0}}),\lambda(p_{1}^{j_{1}})\ldots(p_{k}^{j_{k}})\right)$.

למה: יהי $j\in\mathbb{N}\backslash\{0,1,2\}$ אזי $\text{ord}_{2^{j}}(5)=2^{j-2}$.

משפט: יהי $n\in\mathbb{N}_{+}$ אזי

- $\forall a\in\mathbb{Z}_{n}^{*}.a^{\lambda(n)}\equiv1\mod n$.
- $\exists c\in\mathbb{Z}_{n}^{*}.\text{ord}_{n}(c)=\lambda(n)$.

למה: יהי $n\in\mathbb{N}\backslash\{0,1,2\}$ אזי $\lambda(n)\in\mathbb{N}_{\text{even}}$.

משפט: יהי $n\in\mathbb{N}$ מספר קרמייקל אזי קיים $k\in\mathbb{N}\backslash\{0,1\}$ וקיימים $p_{1}\ldots p_{k}\in\mathbb{P}$ שונים עבורם $n=\prod_{i=1}^{k}p_{i}$ וכן $\forall i\in[k]\,.\,(p_{i}-1)\,|\,(n-1)$.

אלגוריתם מבחן רבין־מילר לבדיקת ראשוניות: יהי $n \in \mathbb{N}_{\text{odd}} \backslash \{1\}$ ויהי $b \in \mathbb{Z}_n^*$ אזי

```
function RabinMillerPrimalityTest(n, b)
| if b^(n-1) ≢ 1 mod n
|     return false
| if b^((n-1)/2) ≡ ±1 mod n
|     | if (n-1)/2 ∈ N_even
|     |     | if b^((n-1)/2) ≡ 1 mod n
|     |     |     return RabinMillerPrimalityTest(n, b^(1/2))
|     |     | if b^((n-1)/2) ≡ -1 mod n
|     |     |     return maybe
|     | if (n-1)/2 ∈ N_odd
|     |     return maybe
| if b^((n-1)/2) ≢ ±1 mod n
|     return false
```

משפט: יהי $n \in \mathbb{N}_{\text{odd}} \backslash \{1\}$ ויהי $b \in \mathbb{Z}_n^*$ אזי $(n \notin \mathbb{P}) \iff (\text{RabinMillerPrimalityTest}(n,b) = \text{false})$.

טענה: יהי $p \in \mathbb{P} \backslash \{2\}$ ויהי $a \in \mathbb{Z}_p^*$ אזי $\left(a^{\frac{p-1}{2}} \equiv 1 \mod p\right) \vee \left(a^{\frac{p-1}{2}} \equiv -1 \mod p\right)$.

מסקנה: יהי $p \in \mathbb{P} \backslash \{2\}$ ויהי $a \in \mathbb{Z}_p^*$ אזי $\left(a^{\frac{p-1}{2}} \equiv 1 \mod p\right) \iff \left(\text{sols}_{\mathbb{Z}_p}(x^2 = a) \neq \varnothing\right)$.

שארית ריבועית: יהי $p \in \mathbb{P} \backslash \{2\}$ אזי $a \in \mathbb{Z}_p^*$ המקיים $\text{sols}_{\mathbb{Z}_p}(x^2 = a) \neq \varnothing$.

מסקנה: יהי $p \in \mathbb{P} \backslash \{2\}$ ויהי $a \in \mathbb{Z}_p^*$ אזי
- (a שארית ריבועית מודולו p) $\iff \left(a^{\frac{p-1}{2}} \equiv 1 \mod p\right)$.
- (a לא שארית ריבועית מודולו p) $\iff \left(a^{\frac{p-1}{2}} \equiv -1 \mod p\right)$.

סימן לז'נדר: יהי $p \in \mathbb{P} \backslash \{2\}$ ויהי $a \in \mathbb{Z}_p^*$ אזי $\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{שארית ריבועית } p \ a \\ -1 & \text{else} \end{cases}$.

מסקנה: $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \mod p$.

טענה: $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$.

טענה: $\left|\left\{a \in \mathbb{Z}_p^* \mid \left(\frac{a}{p}\right) = 1\right\}\right| = \frac{p-1}{2} = \left|\left\{a \in \mathbb{Z}_p^* \mid \left(\frac{a}{p}\right) = -1\right\}\right|$.

טענה: יהי $\alpha \in \mathbb{Z}_p^*$ שארית לא ריבועית ויהי $\beta \in \alpha \left(\mathbb{Z}_p^*\right)^2$ אזי β לא שארית ריבועית.

משפט: יהי $\alpha \in \mathbb{Z}_p^*$ שארית לא ריבועית אזי $\mathbb{Z}_p^* = \left(\mathbb{Z}_p^*\right)^2 \uplus \left(\alpha \left(\mathbb{Z}_p^*\right)^2\right)$

טענה : יהיו $a,b\in\mathbb{Z}_p^*$ אזי $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)$.

משפט אוילר : יהי $p\in\mathbb{P}\backslash\{2,3\}$ המקיים $p\equiv 3 \mod 4$ וכן $2p+1\in\mathbb{P}$ אזי 2^p-1 פריק.

טענה : יהי $a\in\mathbb{Z}_{\text{odd}}$ אזי $\text{sols}_{\mathbb{Z}_2}\left(x^2=a\right)=\{1\}$.

טענה : יהי $a\in\mathbb{Z}_{\text{odd}}$ אזי

- אם $a\equiv 1 \mod 4$ אזי $\text{sols}_{\mathbb{Z}_4}\left(x^2=a\right)=\{1,3\}$.
- אם $a\not\equiv 1 \mod 4$ אזי $\text{sols}_{\mathbb{Z}_4}\left(x^2=a\right)=\varnothing$.

טענה : יהי $a\in\mathbb{Z}_{\text{odd}}$ אזי

- אם $a\equiv 1 \mod 8$ אזי $\text{sols}_{\mathbb{Z}_4}\left(x^2=a\right)=\{1,3,5,7\}$.
- אם $a\not\equiv 1 \mod 8$ אזי $\text{sols}_{\mathbb{Z}_4}\left(x^2=a\right)=\varnothing$.