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

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

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

- אסוציטיביות/קיבוציות: $\forall a,b,c\in A.a*(b*c)=(a*b)*c$.
- 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: $a*(b*c)=(a*b)*c$.
- איבר יחידה לכפל: $\exists e_*\in R.\forall g\in R.e_**g=g*e_*=g$.
- חוק הפילוג: $((b+c)*a=b*a+c*a)\wedge(a*(b+c)=a*b+a*c)$.

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

- $\langle\mathbb{F},+,*\rangle$ חוג.
- $\langle\mathbb{F}\backslash\{e_*\},*\rangle$ 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 $(x+y)^n=\sum_{k=0}^n\binom{n}{k}x^ky^{n-k}$.

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

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: $\mathbb{Z}[\alpha]=\bigcup_{n=0}^\infty\{\sum_{i=0}^n k_i\alpha^i\mid k\in\mathbb{Z}^n\}$.

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

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

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

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

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

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 $(\exists\varepsilon\in A^{*}.b=\varepsilon a)\iff(a\sim b)$.

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 $(a,b)\neq 0$ 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 $(a_{1}\ldots a_{n})\neq 0$ אזי $\max\left\{ d\in\mathbb{Z}\mid\forall i\in[n].(d\mid a_{i})\right\}$.

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.

המשפט היסודי של האריתמטיקה : $\mathbb{Z}$ 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 : $\mathbb{P}=\left\{ p\in\mathbb{N}\mid\text{ראשוני } p\right\}$.

השערת התאומים הראשוניים : קיימים אינסוף $p\in\mathbb{P}$ עבורם $p+2\in\mathbb{P}$. השערה פתוחה

פונקציית ספירת ראשוניים : $\pi\left(x\right)=\left|\left\{ p\in\mathbb{P}\mid p\le x\right\} \right|$.

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

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

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

טענה: $\pi(x) > \log\log(x)$.

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: $\pi(x) \sim \frac{x}{\log(x)}$.

למה: יהי $x \in \mathbb{R}$ אזי $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0,1\}$.

למה: יהי $p \in \mathbb{P}$ ויהיו $n, r \in \mathbb{N}_+$ עבורם $p^r \le n < p^{r+1}$ אזי $\sum_{i=1}^{r} \left\lfloor \frac{n}{p^i} \right\rfloor = \max\{m \in \mathbb{N} \mid (p^m \mid n!)\}$.

משפט צ'בישב: $\exists a \in (0,1).\exists b \in (1,\infty).\forall x \ge 2.\left(a\frac{x}{\log(x)} < \pi(x) < b\frac{x}{\log(x)}\right)$.

מסקנה: $\exists \alpha, \beta > 0.\forall n \in \mathbb{N} \backslash \{0,1\}.(\alpha n \log(n) < p_n < \beta n \log(n))$.

משפט השערת ברטרנד: יהי $n \in \mathbb{N} \backslash \{0,1\}$ אזי $\exists p \in \mathbb{P}.n < p < 2n$.

הגדרה: נגדיר $\text{Li} : \mathbb{R} \to \mathbb{R}$ כך $\text{Li}(x) = \int_2^x \frac{1}{\log(t)} dt$.

טענה: $\text{Li}(x) \sim \frac{x}{\log(x)}$.

מסקנה: $\text{Li}(x) \sim \pi(x)$.

פונקציית זטא של רימן: נגדיר $\zeta : \mathbb{R} \to \mathbb{R}$ כך $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$.

השערת רימן: $\forall \beta > \frac{1}{2}.\exists x_0 \in \mathbb{R}_+.\forall x \ge x_0.|\pi(x) - \text{Li}(x)| \le x^\beta$. השערה פתוחה

משפט: (השערת רימן נכונה) $\iff \left(\text{sols}_{\mathbb{C}}(\zeta(s) = 0) \backslash \{-2n \mid n \in \mathbb{N}_+\} \subseteq \left\{z \in \mathbb{C} \mid \text{Re}(z) = \frac{1}{2}\right\}\right)$.

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 $m \ne n$ 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 $n = \sum_{\substack{d \mid n \\ d < n}} d$.

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

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

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

טענה: תהא f פונקציה כופלית ויהי $n\in\mathbb{N}$ עם פירוק לראשוניים $n=\prod_{m=1}^{k}p_{m}^{r_{m}}$ אזי $f\left(n\right)=\prod_{i=1}^{k}f\left(p_{i}^{r_{i}}\right)$.

טענה: σ פונקציה כפלית.

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

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

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

פונקציית מביוס: נגדיר $\mu:\mathbb{N}\to\left\{ 0,\pm1\right\}$ כפלית יהי $p\in\mathbb{P}$ ויהי $r\in\mathbb{N}_{+}$ אזי $\mu\left(p^{r}\right)=\begin{cases} 1 & r=0\\ -1 & r=1\\ 0 & r\geq2 \end{cases}$.

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

משפט אוקלידס: יהי $M_{p}\in\mathbb{P}$ אזי $\frac{1}{2}M_{p}\left(M_{p}+1\right)$ מושלם.

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

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 $\left(a,b\right)$.
2. מצאו את נקודות החיתוך בין הישר העובר דרך $\left(a,b\right),\left(0,t\right)$ ובין העקומה.
   - פתור את מערכת המשוואות $\begin{cases} \left(t-b\right)x+a\left(y-t\right)=0\\ rx^{2}+sy^{2}=1 \end{cases}$.
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 $\left(t\in\mathbb{Q}\right)\iff\left(\left(\frac{t^{2}-1}{t^{2}+1}\in\mathbb{Q}\right)\wedge\left(\frac{2t}{t^{2}+1}\in\mathbb{Q}\right)\right)$.

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

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

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 $\gcd\left(u,v\right)=1$ 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 $\gcd\left(u,v\right)=1$ 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: $a+n\mathbb{Z}=\left\{ a+n\cdot m\mid m\in\mathbb{Z}\right\}$.

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

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

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

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

טענה: יהי $n,k\in\mathbb{N}_+$ 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: יהי $n,k\in\mathbb{N}_+$ 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: יהי $n\in\mathbb{N}$ עם פירוק לראשוניים $n=\prod_{m=1}^k p_m^{r_m}$ אזי $\phi(n)=n\prod_{p\mid n}\left(1-\frac{1}{p}\right)$.

מסקנה: ϕ פונקציה כפלית.

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

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 $(\gcd(a,n)\mid b)\iff(\mathrm{sols}_{\mathbb{Z}_n}(ax=b)\neq\varnothing)$.

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 $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv1\mod\frac{n}{\gcd(a,n)}$ אזי $\mathrm{sols}_{\mathbb{Z}_n}(ax=b)=\left\{\frac{cb+rn}{\gcd(a,n)}\mid r\in\mathbb{Z}\right\}$.

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 $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv1\mod\frac{n}{\gcd(a,n)}$ אזי $\mathrm{sols}_{\mathbb{Z}_n}(ax=b)=\left\{\frac{cb+kn}{\gcd(a,n)}\mid0\le k\le\gcd(a,n)\right\}$.

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 $|\mathrm{sols}_{\mathbb{Z}_n}(ax=b)|=\gcd(a,n)$.

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 $\left(\frac{a}{\gcd(a,n)}\right)\cdot c\equiv1\mod\frac{n}{\gcd(a,n)}$ וכן $\frac{ac}{\gcd(a,n)}=1+\frac{\alpha n}{\gcd(a,n)}$ אזי $\mathrm{sols}_{\mathbb{N}^2}(ax+ny=b)=\left\{\left(\frac{cb+rn}{\gcd(a,n)},-\frac{\alpha b+ra}{\gcd(a,n)}\right)\mid r\in\mathbb{Z}\right\}$.

משפט השאריות הסיני: יהיו $n_1\ldots n_k\in\mathbb{N}_+$ זרים ויהיו $c_1\ldots c_k\in\mathbb{Z}$ אזי $\exists!x\in\mathbb{Z}_{\prod_{i=1}^{k}n_i}.\forall i\in[k].x\equiv c_i\mod n_i$.

משפט אוילר: יהי $n\in\mathbb{N}\backslash\{0,1\}$ ויהי $a\in\mathbb{Z}$ המקיים $\gcd(a,n)=1$ אזי $a^{\phi(n)}\equiv1\mod n$.

מסקנה: יהי $n\in\mathbb{N}\backslash\{0,1\}$ ויהי $a\in\mathbb{Z}$ המקיים $\gcd(a,n)=1$ אזי $a^{\phi(n)-1}\cdot a\equiv1\mod n$.

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 $a^{p-1}\equiv1\mod p$.

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

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

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 $\sum_{i=0}^{m}a_ix^i,\sum_{i=0}^{k}b_ix^i\in\mathbb{Z}_n[x]$ אזי

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

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 $|\mathrm{sols}_{\mathbb{Z}_m}(f(x)=0)|=\prod_{i=1}^{k}\left|\mathrm{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x)=0)\right|$.

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

משפט: יהי $f\in\mathbb{Z}[x]$ יהי $p\in\mathbb{P}$ ויהי $a_1\in\mathbb{Z}$ פתרון של $f(x)\equiv0\mod p$ וכן $f'(a_1)\not\equiv0\mod p$ יהי $j\in\mathbb{N}\backslash\{0,1\}$ אזי קיים ויחיד $a_j\in\mathbb{Z}_{p^j}$ המקיים $f(a_j)\equiv0\mod p^j$ 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 $f(a_j)\equiv0\mod p^j$ אזי $a_j+cp^j\in\mathbb{Z}_{p^{j+1}}$ המקיים $f(a_j+cp^j)\equiv0\mod p^{j+1}$.

סדר: יהי $n\in\mathbb{N}\backslash\{0,1\}$ ויהי $a\in\mathbb{Z}_n^*$ אזי $\mathrm{ord}_n(a)=\min\left\{d\in\mathbb{N}_+\mid a^d\equiv1\mod n\right\}$.

טענה: יהי $a\in\mathbb{Z}_n^*$ אזי $(\mathrm{ord}_n(a)\mid k)\iff\left(a^k\equiv1\mod n\right).\forall k\in\mathbb{N}_+$.

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

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

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

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

טענה: יהי $n\in\mathbb{N}\backslash\{0,1\}$ ויהי $a\in\mathbb{Z}_{n}^{*}$ אזי (a ש"פ) $\iff$ (a יוצר את $\mathbb{Z}_{n}^{*}$).

טענה: יהי $a\in\mathbb{Z}_{n}^{*}$ שורש פרימיטיבי אזי קיימים $\phi\left(\phi\left(n\right)\right)$ 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 $b^{2^{j-2}}\equiv1\mod 2^{j}$.

מסקנה: יהי $j\in\mathbb{N}\backslash\{0,1,2\}$ ויהי $b\in\mathbb{N}_{\text{odd}}$ אזי $\text{ord}_{2^{j}}\left(b\right)\mid2^{j-2}$.

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 $a^{\frac{1}{2}\phi(n_{1}n_{2})}\equiv1\mod n_{1}n_{2}$.

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 $\left(a^{\frac{\phi(n)}{\gcd(m,\phi(n))}}\equiv1\mod n\right)\iff\left(\text{sols}_{\mathbb{Z}_{n}}\left(x^{m}=a\right)\neq\varnothing\right)$.

מסקנה: יהי $n\in\mathbb{N}$ בעל שורש פרימיטיבי ויהי $m\in\mathbb{N}_{+}$ נגדיר $f:\mathbb{Z}_{n}^{*}\to\mathbb{Z}_{n}^{*}$ כך $f\left(x\right)\equiv x^{m}\mod n$ אזי $\text{Im}\left(f\right)=\left\{a\in\mathbb{Z}_{n}^{*}\mid a^{\frac{\phi(n)}{\gcd(m,\phi(n))}}\equiv1\mod n\right\}$.

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

אלגוריתם RSA:

- נבחר $p,q\in\mathbb{P}$ גדולים, ונסמן $n=pq$.
- נבחר $m\in\mathbb{Z}_{\phi(n)}^{*}$, ונחשב $s\equiv m^{-1}\mod\phi\left(n\right)$.
- נפרסם את $\left(n,m\right)$ 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 $N,\phi\left(N\right)$ אזי אנו יודעים את p,q ב־$\mathcal{O}\left(1\right)$.

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: יהי $p\in\mathbb{P}\backslash\{2\}$ ויהי $a\in\mathbb{Z}_{p}^{*}$ אזי $\left(a^{\frac{p-1}{2}}\equiv1\mod p\right)\vee\left(a^{\frac{p-1}{2}}\equiv-1\mod p\right)$.

מסקנה: יהי $p\in\mathbb{P}\backslash\{2\}$ ויהי $a\in\mathbb{Z}_{p}^{*}$ אזי $\left(a^{\frac{p-1}{2}}\equiv1\mod p\right)\iff\left(\text{sols}_{\mathbb{Z}_{p}}\left(x^{2}=a\right)\neq\varnothing\right)$.

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

מסקנה: יהי $p\in\mathbb{P}\backslash\{2\}$ ויהי $a\in\mathbb{Z}_{p}^{*}$ אזי

- (a שארית ריבועית מודולו p) $\iff$ $\left(a^{\frac{p-1}{2}}\equiv1\mod p\right)$.
- (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 $\left(\frac{a}{p}\right)=\begin{cases}1 & a\text{ שארית ריבועית }p\\ -1 & \text{else}\end{cases}$.

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

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 $\text{sols}_{\mathbb{Z}_4}\left(x^2=a\right)=\varnothing$.

טענה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}\backslash\{0,1,2\}$ אזי $\left(a\equiv 1 \mod 8\right)\iff\left(\text{sols}_{\mathbb{Z}_{2^k}}\left(x^2=a\right)\neq\varnothing\right)$.

מסקנה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}_+$ אזי $\left(a\equiv 1 \mod \gcd\left(8,2^k\right)\right)\iff\left(\text{sols}_{\mathbb{Z}_{2^k}}\left(x^2=a\right)\neq\varnothing\right)$.

טענה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}_+$ עבורם $a\equiv 1 \mod \gcd\left(8,2^k\right)$ אזי $\left|\text{sols}_{\mathbb{Z}_{2^k}}\left(x^2=a\right)\right|=\begin{cases}1 & k=1\\ 2 & k=2\\ 3 & k\geq 3\end{cases}$.

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

טענה: יהי $p\in\mathbb{P}\backslash\{2\}$ יהי $j\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}_p^*$ המקיים $a^{\frac{1}{2}\phi\left(p^j\right)}\equiv 1 \mod p^j$ אזי $\left|\text{sols}_{\mathbb{Z}_{p^j}}\left(x^2=a\right)\right|=2$.

טענה: יהי $n\in\mathbb{N}_+$ עם פירוק $n=2^{r_0}\prod_{i=1}^{k}p_i^{r_i}$ ויהי $a\in\mathbb{Z}_n^*$ אזי

$$\left(\left(a\equiv 1 \mod \gcd\left(8,2^{r_0}\right)\right)\wedge\left(\forall i\in[k].a^{\frac{1}{2}\phi\left(p_i^{r_i}\right)}\equiv 1 \mod p_i^{r_i}\right)\right)\iff\left(\text{sols}_{\mathbb{Z}_n}\left(x^2=a\right)\neq\varnothing\right).$$

מסקנה: יהי $n\in\mathbb{N}_+$ עם פירוק $n=2^{r_0}\prod_{i=1}^{k}p_i^{r_i}$ ויהי $a\in\mathbb{Z}_n^*$ המקיים $\text{sols}_{\mathbb{Z}_n}\left(x^2=a\right)\neq\varnothing$ נסמן $m=\begin{cases}0, & r_0\in\{0,1\}\\ 1, & r_0=2\\ 2, & \text{else}\end{cases}$ אזי $\left|\text{sols}_{\mathbb{Z}_n}\left(x^2=a\right)\right|=2^k\cdot 2^m$.

הלמה של גאוס: יהי $p\in\mathbb{P}\backslash\{2\}$ יהי $a\in\mathbb{Z}_p^*$ אזי $\left(\frac{a}{p}\right)=(-1)^{\left|\left\{j\in\left\{1\ldots\frac{p-1}{2}\right\}\ \middle|\ \substack{aj\in\left[-\frac{p-1}{2},\frac{p-1}{2}\right]\\ aj<0}\right\}\right|}$.

טענה: יהי $p\in\mathbb{P}\backslash\{2\}$ אזי $\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$.

מסקנה: יהי $p\in\mathbb{P}\backslash\{2\}$ אזי $\left(\frac{2}{p}\right)=\begin{cases}1 & p\equiv\pm 1 \mod 8\\ -1 & p\equiv\pm 3 \mod 8\end{cases}$.

משפט ההדדיות הריבועית של גאוס: יהיו $p,q\in\mathbb{P}\backslash\{2\}$ באשר $p\neq q$ אזי $\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\frac{1}{4}(p-1)(q-1)}$.

מסקנה: בסדרה $\{5n-1\}_{n=1}^{\infty}$ ישנם אינסוף ראשוניים.

סמל יעקובי: יהי $n\in\mathbb{N}_{\text{odd}}$ עם פירוק $n=\prod_{i=1}^{k}p_i^{r_i}$ ויהי $a\in\mathbb{Z}_n^*$ אזי $\left(\frac{a}{n}\right)=\prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{r_i}$.

טענה: יהי $n\in\mathbb{N}_{\text{odd}}$ ויהיו $a,b\in\mathbb{Z}_n^*$ אזי

- $\left(\left(\frac{a}{n}\right)=\left(\frac{b}{n}\right)\right)\impliedby\left(a\equiv b \mod n\right)$.
- $\left(\left(\frac{a}{n}\right)=-1\right)\implies$ (a לא שארית ריבועית מודולו n).

למה: יהיו $n_1\ldots n_k\in\mathbb{N}_{\text{odd}}$ אזי

- $\frac{1}{2}\left(\left(\prod_{i=1}^{k}n_i\right)-1\right)\equiv\frac{1}{2}\sum_{i=1}^{k}\left(n_i-1\right) \mod 2$.
- $\frac{1}{2}\left(\left(\prod_{i=1}^{k}n_i\right)^2-1\right)\equiv\frac{1}{2}\sum_{i=1}^{k}\left(n_i^2-1\right) \mod 2$.

משפט: יהיו $n,m\in\mathbb{N}_{\text{odd}}$ ויהיו $a,b\in\mathbb{N}_+$ אזי

- נניח כי $a,b\in\mathbb{Z}_n^*$ אזי $\left(\frac{a\cdot b}{n}\right)=\left(\frac{a}{n}\right)\cdot\left(\frac{b}{n}\right)$.
- נניח כי $a\in\mathbb{Z}_n^*\cap\mathbb{Z}_m^*$ אזי $\left(\frac{a}{n\cdot m}\right)=\left(\frac{a}{n}\right)\cdot\left(\frac{a}{m}\right)$.
- נניח כי $n\neq 1$ אזי $\left(\frac{-1}{n}\right)=(-1)^{\frac{n-1}{2}}$.
- $\left(\frac{2}{n}\right)=(-1)^{\frac{n^2-1}{8}}$.

חוק ההדדיות של גאוס: יהיו $n,m\in\mathbb{N}_{\text{odd}}\backslash\{1\}$ אזי $\left(\frac{m}{n}\right)\cdot\left(\frac{n}{m}\right)=(-1)^{\frac{1}{4}(n-1)(m-1)}$.

אלגוריתם חישוב סמל יעקובי: יהי $n\in\mathbb{N}_{\text{odd}}$ עם פירוק $n=\prod_{i=1}^k p_i^{r_i}$ ויהי $a\in\mathbb{Z}_n^*$ אזי

function JacobiSymbolCalculator (a,n)

| $k\leftarrow 0$

| $s\leftarrow a$

| **while** $s\in\mathbb{Z}_{\text{even}}$

| | $r\leftarrow\max\left\{\ell\in\mathbb{N}\mid\left(2^\ell\mid s\right)\right\}$

| | $k\leftarrow k+r$

| | $s'\leftarrow(0\le s'\le n-1)\wedge\left(s'\equiv\frac{s}{r}\mod n\right)$

| | $s\leftarrow s'$

| **return** $(-1)^{\frac{1}{8}k\left(n^2-1\right)+\frac{1}{4}(n-1)(s-1)}\cdot$ JacobiSymbolCalculator (n,s)

עד פרמה: יהי $n\in\mathbb{N}_+$ אזי $a\in\mathbb{Z}_n^*$ המקיים $a^{n-1}\not\equiv 1\mod n$.

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

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 $\forall i\in[k].(p_i-1)\mid(n-1)$ אזי n מספר קרמייקל.

כפולה משותפת מינימלית: יהיו $a_1\ldots a_n\in\mathbb{Z}$ באשר $(a_1\ldots a_n)\neq 0$ אזי $\min\{d\in\mathbb{Z}\mid\forall i\in[n].(a_i\mid d)\}$.

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 $\lambda\left(2^j\right)=2^{j-2}$.
- יהי $p\in\mathbb{P}\backslash\{2\}$ ויהי $j\in\mathbb{N}_+$ אזי $\lambda\left(p^j\right)=\phi\left(p^j\right)=p^{j-1}(p-1)$.
- יהי $n\in\mathbb{N}_+$ עם פירוק לראשוניים $n=2^{j_0}\prod_{i=1}^k p_i^{j_i}$ אזי $\lambda(n)=\operatorname{lcm}\left(\lambda\left(2^{j_0}\right),\lambda\left(p_1^{j_1}\right)\ldots\left(p_k^{j_k}\right)\right)$.

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

משפט: יהי $n\in\mathbb{N}_+$ אזי

- $\forall a\in\mathbb{Z}_n^*.a^{\lambda(n)}\equiv 1\mod n$.
- $\exists c\in\mathbb{Z}_n^*.\operatorname{ord}_n(c)=\lambda(n)$.

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 $\forall i\in[k].(p_i-1)\mid(n-1)$.

עד אוילר־יעקובי: יהי $n\in\mathbb{N}_{\text{odd}}$ אזי $a\in\mathbb{Z}_n^*$ המקיים $a^{\frac{n-1}{2}}\not\equiv\left(\frac{a}{n}\right)\mod n$.

משפט: יהי $n\in\mathbb{N}_{\text{odd}}$ פריק אזי קיים עד אוילר־יעקובי.

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** $b^{n-1}\not\equiv 1\mod n$
  - **return** false
- **if** $b^{\frac{n-1}{2}}\equiv\pm1\mod n$
  - **if** $\frac{n-1}{2}\in\mathbb{N}_{\text{even}}$
    - **if** $b^{\frac{n-1}{2}}\equiv 1\mod n$
      - **return** RabinMillerPrimalityTest$\left(n,b^{\frac{1}{2}}\right)$
    - **if** $b^{\frac{n-1}{2}}\equiv -1\mod n$
      - **return** maybe
  - **if** $\frac{n-1}{2}\in\mathbb{N}_{\text{odd}}$
    - **return** maybe
- **if** $b^{\frac{n-1}{2}}\not\equiv\pm1\mod n$
  - **return** false

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