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

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

טענה: יהי $m \in \mathbb{Z}$ עבורו $\sqrt{m} \notin \mathbb{Q}$ אזי $\{1, \sqrt{m}\}$ 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 $(a \sim b) \iff (\exists \varepsilon \in A^*. b = \varepsilon a)$.

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 $\forall b,c\in A.\,(a=bc)\Longrightarrow(b\in A^*)\vee(c\in A^*)$.

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

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 $a\in A\backslash\left(A^*\cup\{0\}\right)$ 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 הצמדה: יהי $\alpha\in\mathbb{Z}$ עבורו $\sqrt{\alpha}\notin\mathbb{Q}$ נגדיר $\sigma:\mathbb{Z}[\sqrt{\alpha}]\to\mathbb{Z}[\sqrt{\alpha}]$ כך $\sigma\left(a+b\sqrt{\alpha}\right)=a-b\sqrt{\alpha}$.

טענה: יהיו $z,w\in\mathbb{Z}[\sqrt{\alpha}]$ מתקיימים
- $\sigma(z+w)=\sigma(z)+\sigma(w)$.
- $\sigma(zw)=\sigma(z)\sigma(w)$.
- $\sigma(\sigma(z))=z$.
- 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 $z,w\in\mathbb{Z}[\sqrt{\alpha}]$ מתקיימים
- $N(zw)=N(z)N(w)$.
- $(N(z)=0)\Longleftrightarrow(z=0)$.

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 $a\in A\backslash\left(A^*\cup\{0\}\right)$ 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)$\Longleftrightarrow$(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 $a,b\in\mathbb{Z}$ כאשר $a>0$ אזי קיימים ויחידים $q,r\in\mathbb{Z}$ כאשר $0\le r<a$ המקיימים $b=qa+r$.

שארית חלוקה: יהיו $a,b\in\mathbb{Z}$ כאשר $a>0$ ויהיו $q,r\in\mathbb{Z}$ כאשר $0\le r<a$ 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 $a,b\in\mathbb{Z}$ כאשר $a>0$ אזי (שארית החלוקה של b ב־a היא 0)$\Longleftrightarrow(a\mid b)$.

מחלק משותף: יהיו $a,b\in\mathbb{Z}$ כאשר $(a,b)\neq0$ אזי $d\in\mathbb{Z}$ המקיים $(d\mid a)\wedge(d\mid b)$.

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

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

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

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

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

מחלק משותף מקסימלי (ממ"מ): יהיו $a_1\ldots a_n\in\mathbb{Z}$ כאשר $(a_1\ldots a_n)\neq0$ אזי $\max\{d\in\mathbb{Z}\mid\forall i\in[n].\,(d\mid a_i)\}$.

סימון: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי המחלק המשותף המקסימלי שלהם הינו $\gcd(a_1\ldots a_n)$.

משפט: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי $\exists u_1\ldots u_n\in\mathbb{Z}.\,\gcd(a_1\ldots a_n)=\sum_{i=1}^{n}u_ia_i$.

אלגוריתם אוקלידס: יהי $a\in\mathbb{Z}\backslash\{0\}$ 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 $\gcd\left(a,b\right)=\text{EuclideanAlgorithm}\left(a,b\right)$.

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: $\mathbb{P}=\left\{ p\in\mathbb{N}\mid p\text{ ראשוני}\right\}$.

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 $n\in\mathbb{N}\backslash\left\{ 0,1\right\}$ אזי

function SieveOfEratosthenesAlgorithm$\left(n\right)$

$|\ A\leftarrow\left[\underset{2}{\text{true}},\underset{3}{\text{true}},\ldots,\underset{n}{\text{true}}\right]$

$|$ **for** $i\leftarrow2\ldots n$

$|\quad|$ **if** $A\left[i\right]=\text{true}$

$|\quad|\quad|\ j\leftarrow1$

$|\quad|\quad|$ **while** $ij\le n$

$|\quad|\quad|\quad|\ A\left[ij\right]=\text{false}$

$|\quad|\quad|\quad|\ j\leftarrow j+1$

$|$ **return** A

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

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

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

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

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

משפט צ'בישב: $\exists a\in\left(0,1\right).\exists b\in\left(1,\infty\right).\forall x\ge2.\left(a\frac{x}{\log\left(x\right)}<\pi\left(x\right)<b\frac{x}{\log\left(x\right)}\right)$.

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

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

הגדרה: נגדיר $\text{Li}:\mathbb{R}\to\mathbb{R}$ כך $\text{Li}\left(x\right)=\int_{2}^{x}\frac{1}{\log\left(t\right)}dt$.

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

מסקנה: $\text{Li}\left(x\right)\sim\pi\left(x\right)$.

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

השערת רימן: $\forall\beta>\frac{1}{2}.\exists x_{0}\in\mathbb{R}_{+}.\forall x\ge x_{0}.\left|\pi\left(x\right)-\text{Li}\left(x\right)\right|\le x^{\beta}$. השערה פתוחה

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

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 $x^{t}-y^{t}=\left(x-y\right)\sum_{i=0}^{t-1}x^{i}y^{t-i-1}$.

טענה: יהיו $m,n\in\mathbb{N}$ באשר $m\ne n$ אזי $\gcd\left(F_{n},F_{m}\right)=1$.

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 $n = \prod_{m=1}^{k} p_m^{r_m}$ אזי $f(n) = \prod_{i=1}^{k} f(p_i^{r_i})$.

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 $n = \prod_{m=1}^{k} p_m^{r_m}$ 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 $p \in \mathbb{P}$ ויהי $r \in \mathbb{N}_+$ 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 $M_p \in \mathbb{P}$ אזי $\frac{1}{2} M_p (M_p + 1)$ מושלם.

משפט אוילר: יהי $n \in \mathbb{N}_{\text{even}}$ 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 $(a, b), (0, t)$ 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: $f : \mathbb{Q} \to \left\{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\right\} \setminus \{(1, 0)\}$ 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: $\overline{a}=a+n\mathbb{Z}$.

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: 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: 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 $\frac{1}{2}n\phi(n)=\sum_{\substack{1\le k\le n\\ \gcd(k,n)=1}}k$.

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

משפט פתרון משוואות דיופנטיות לינאריות: יהי $a\in\mathbb{Z}\backslash\{0\}$ יהי $b,c,\alpha\in\mathbb{Z}$ 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 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 $a^{\phi(n)}\equiv 1 \mod n$.

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 $\left(\sum_{i=0}^m a_i x^i=\sum_{i=0}^m b_i x^i\right)\Longleftrightarrow(a_i=b_i)$.

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

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 $(\text{sols}_{\mathbb{Z}_m}(f(x)=0)\neq\varnothing)\Longleftrightarrow\left(\forall i\in[k].\text{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x)=0)\neq\varnothing\right)$.

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 $f\left(a_j+cp^j\right)\equiv 0 \mod p^{j+1}$.

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 $\forall k\in\mathbb{N}_+.\left(a^k\equiv 1 \mod n\right)\Longleftrightarrow(\text{ord}_n(a)\mid k)$.

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

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

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)$\Longleftrightarrow\left(n\in\{1,2,4\}\cup\left\{p^j \;\middle|\; \substack{p\in\mathbb{P}\\ j\in\mathbb{N}_+}\right\}\cup\left\{2p^j \;\middle|\; \substack{p\in\mathbb{P}\\ j\in\mathbb{N}_+}\right\}\right)$.

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

מסקנה: יהי $n\in\mathbb{N}$ בעל שורש פרימיטיבי ויהי $m\in\mathbb{N}_+$ נגדיר $\underset{f(x)\equiv x^m \mod n}{f:\mathbb{Z}_n^*\to\mathbb{Z}_n^*}$ 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 $\underset{f(x)\equiv x^m \mod n}{f:\mathbb{Z}_n^*\to\mathbb{Z}_n^*}$ 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 $N,\phi\left(N\right)$ 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 $p\in\mathbb{P}\backslash\left\{ 2\right\}$ 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 $p\in\mathbb{P}\backslash\left\{ 2\right\}$ 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 $p\in\mathbb{P}\backslash\left\{ 2\right\}$ אזי $a\in\mathbb{Z}_{p}^{*}$ המקיים $\text{sols}_{\mathbb{Z}_{p}}\left(x^{2}=a\right)\neq\varnothing$.

מסקנה: יהי $p\in\mathbb{P}\backslash\left\{ 2\right\}$ 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 $p\in\mathbb{P}\backslash\left\{ 2\right\}$ 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 $\mathbb{Z}_{p}^{*}=\left\{ a^{2}\mid a\in\mathbb{Z}_{p}^{*}\right\} \uplus\left\{ \alpha\cdot a^{2}\mid a\in\mathbb{Z}_{p}^{*}\right\}$.

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 $p\in\mathbb{P}\backslash\left\{ 2,3\right\}$ המקיים $p\equiv3\mod4$ וכן $2p+1\in\mathbb{P}$ אזי $2^{p}-1$ פריק.

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

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

- אם $a\equiv1\mod4$ אזי $\text{sols}_{\mathbb{Z}_{4}}\left(x^{2}=a\right)=\left\{ 1,3\right\}$.
- אם $a\not\equiv1\mod4$ אזי $\text{sols}_{\mathbb{Z}_{4}}\left(x^{2}=a\right)=\varnothing$.

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

- אם $a\equiv1\mod8$ אזי $\text{sols}_{\mathbb{Z}_{4}}\left(x^{2}=a\right)=\left\{ 1,3,5,7\right\}$.
- אם $a\not\equiv1\mod8$ אזי $\text{sols}_{\mathbb{Z}_{4}}\left(x^{2}=a\right)=\varnothing$.

טענה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}\backslash\left\{ 0,1,2\right\}$ אזי $\left(a\equiv1\mod8\right)\iff\left(\text{sols}_{\mathbb{Z}_{2^{k}}}\left(x^{2}=a\right)\neq\varnothing\right)$.

מסקנה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}_{+}$ אזי $\left(a\equiv1\mod\gcd\left(8,2^{k}\right)\right)\iff\left(\text{sols}_{\mathbb{Z}_{2^{k}}}\left(x^{2}=a\right)\neq\varnothing\right)$.

טענה: יהי $a\in\mathbb{Z}_{\text{odd}}$ ויהי $k\in\mathbb{N}_{+}$ עבורם $a\equiv1\mod\gcd\left(8,2^{k}\right)$ אזי $\left|\text{sols}_{\mathbb{Z}_{2^{k}}}\left(x^{2}=a\right)\right|=\begin{cases} 1 & k=1\\ 2 & k=2\\ 3 & k\geq3 \end{cases}$.

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

טענה: יהי $p\in\mathbb{P}\backslash\left\{ 2\right\}$ יהי $j\in\mathbb{N}_{+}$ ויהי $a\in\mathbb{Z}_{p}^{*}$ המקיים $a^{\frac{1}{2}\phi\left(p^{j}\right)}\equiv1\mod p^{j}$ 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
$\left(\left(a\equiv1\mod\gcd\left(8,2^{r_{0}}\right)\right)\wedge\left(\forall i\in\left[k\right].a^{\frac{1}{2}\phi\left(p_{i}^{r_{i}}\right)}\equiv1\mod p_{i}^{r_{i}}\right)\right)\iff\left(\text{sols}_{\mathbb{Z}_{n}}\left(x^{2}=a\right)\neq\varnothing\right)$.

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 $m=\begin{cases} 0, & r_{0}\in\left\{ 0,1\right\} \\ 1, & r_{0}=2\\ 2, & \text{else} \end{cases}$ אזי $\left|\text{sols}_{\mathbb{Z}_{n}}\left(x^{2}=a\right)\right|=2^{k}\cdot2^{m}$.

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

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

מסקנה: יהי $p\in\mathbb{P}\backslash\left\{ 2\right\}$ אזי $\left(\frac{2}{p}\right)=\begin{cases} 1 & p\equiv\pm1\mod8\\ -1 & p\equiv\pm3\mod8 \end{cases}$.

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

מסקנה: בסדרה $\left\{ 5n-1\right\}_{n=1}^{\infty}$ 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

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

למה: יהיו $n_{1}\ldots n_{k}\in\mathbb{N}_{\text{odd}}$ אזי

- $\frac{1}{2}\left(\left(\prod_{i=1}^{k}n_{i}\right)-1\right)\equiv\frac{1}{2}\sum_{i=1}^{k}\left(n_{i}-1\right)\mod2$.
- $\frac{1}{2}\left(\left(\prod_{i=1}^{k}n_{i}\right)^{2}-1\right)\equiv\frac{1}{2}\sum_{i=1}^{k}\left(n_{i}^{2}-1\right)\mod2$.

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 $n\neq1$ אזי $\left(\frac{-1}{n}\right)=\left(-1\right)^{\frac{n-1}{2}}$.
- $\left(\frac{2}{n}\right)=\left(-1\right)^{\frac{n^{2}-1}{8}}$.

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

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$\left(a,n\right)$

| $k\leftarrow0$

| $s\leftarrow a$

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

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

| | $k\leftarrow k+r$

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

| | $s\leftarrow s'$

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

עד פרמה: יהי $n\in\mathbb{N}_{+}$ אזי $a\in\mathbb{Z}_{n}^{*}$ המקיים $a^{n-1}\not\equiv1\mod n$.

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

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

כפולה משותפת מינימלית: יהיו $a_{1}\ldots a_{n}\in\mathbb{Z}$ באשר $\left(a_{1}\ldots a_{n}\right)\neq0$ אזי $\min\left\{ d\in\mathbb{Z}\mid\forall i\in\left[n\right].\left(a_{i}\mid d\right)\right\}$.

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

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

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

משפט: יהי $n \in \mathbb{N}_+$ אזי

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

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

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) ≢ 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 $(n \notin \mathbb{P}) \iff (\text{RabinMillerPrimalityTest}(n,b) = \text{false})$.

תבנית ריבועית: יהיו $a,b,c \in \mathbb{Z}$ אזי $f \in \mathbb{Z}[x,y]$ המוגדר $f(x,y) = ax^2 + bxy + cy^2$.

מטריצה מייצגת של תבנית ריבועית: תהא $f(x,y) = ax^2 + bxy + cy^2$ תבנית ריבועית אזי $A_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$.

קבוצת התבניות הריבועיות: $\text{sym}_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid A = A^t\}$.

טענה: תהא $f \in \text{sym}_2(\mathbb{Z})$ אזי $f(v) = vA_f v^t$.

דיסקרימיננטה של תבנית ריבועית: תהא $f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$ תבנית ריבועית אזי $\Delta_f = b^2 - 4ac$.

טענה: תהא $f \in \text{sym}_2(\mathbb{Z})$ אזי $(\Delta_f \equiv 0 \mod 4) \vee (\Delta_f \equiv 1 \mod 4)$.

טענה: יהי $\delta \in \mathbb{Z}$ המקיים $(\delta \equiv 0 \mod 4) \vee (\delta \equiv 1 \mod 4)$ אזי $\exists f \in \text{sym}_2(\mathbb{Z}). \Delta_f = \delta$.

פירוק תבנית ריבועית לגורמים ליניאריים: $f \in \text{sym}_2(\mathbb{Z})$ עבורה $\exists m, \ell, r, s \in \mathbb{Q}. (f(x,y) = (mx + \ell y)(rx + sy))$.

משפט גאוס: תהא $f \in \text{sym}_2(\mathbb{Z})$ אזי (f פריקה לגורמים ליניאריים מעל $\mathbb{Q}$)$\iff$(f פריקה לגורמים ליניאריים מעל $\mathbb{Z}$).

טענה: תהא $f \in \text{sym}_2(\mathbb{Z})$ אזי (f פריקה לגורמים ליניאריים מעל $\mathbb{Z}$)$\iff \left(\exists k \in \mathbb{Z}. \Delta = k^2\right)$.

ייצוג על ידי תבנית: תהא $f \in \text{sym}_2(\mathbb{Z})$ אזי $n \in \mathbb{N}$ המקיים $\exists u \in \mathbb{Z}. \exists v \in \mathbb{Z}_u^*. f(v,u) = n$.

משפט: יהי $\delta \in \mathbb{Z} \backslash \left\{k^2 \mid k \in \mathbb{Z}\right\}$ המקיים $(\delta \equiv 0 \mod 4) \vee (\delta \equiv 1 \mod 4)$ ויהי $n \in \mathbb{Z}$ אזי (קיימת $f \in \text{sym}_2(\mathbb{Z})$ המקיימת $\Delta = \delta$ וכן n מיוצג על ידי f)$\iff \left(\text{sols}_{\mathbb{Z}_{4n}}(x^2 = \delta) \neq \varnothing\right)$.

סימון: $\text{SL}_2(\mathbb{Z}) = \{U \in M_2(\mathbb{Z}) \mid \det(U) = 1\}$.

טענה: $\text{SL}_2(\mathbb{Z})$ חבורה ביחס לכפל מטריצות.

תבניות ריבועיות שקולות: $f,g\in\mathrm{sym}_2(\mathbb{Z})$ המקיימות $\exists U\in\mathrm{SL}_2(\mathbb{Z}).f((x,y))=g((x,y)U)$.

טענה: שקילות תבניות ריבועיות הינו יחס שקילות.

סימון: יהיו $f,g\in\mathrm{sym}_2(\mathbb{Z})$ שקולות אזי $f\sim g$.

טענה: יהיו $f,g\in\mathrm{sym}_2(\mathbb{Z})$ אזי $(f\sim g)\Longleftrightarrow(\exists U\in\mathrm{SL}_2(\mathbb{Z}).A_g=UA_fU^t)$.

טענה: תהא $U\in\mathrm{SL}_2(\mathbb{Z})$ ונגדיר $\substack{T_U:\mathbb{Z}^2\to\mathbb{Z}^2\\ T_U(m,n)=(m,n)\cdot U}$ אזי

- T_u חח"ע ועל.
- יהיו $m,n\in\mathbb{Z}$ אזי $(\gcd(T_U(m,n))=1)\Longleftrightarrow(\gcd(m,n)=1)$.

טענה: תהיינה $f,g\in\mathrm{sym}_2(\mathbb{Z})$ שקולות אזי

- $\Delta_f=\Delta_g$.
- $f(\mathbb{Z}\times\mathbb{Z})=g(\mathbb{Z}\times\mathbb{Z})$.
- יהי $n\in\mathbb{Z}$ אזי (n מיוצג על ידי f)$\Longleftrightarrow$(n מיוצג על ידי g).

משפט: תהא $f\in\mathrm{sym}_2(\mathbb{Z})$ אזי קיימת $f\sim\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}$ המקיימת $|b|\le|a|\le|c|$.

אלגוריתם חפיפת תבנית לצורה קנונית: תהא $\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\in\mathrm{sym}_2(\mathbb{Z})$ אזי

function CanonicalFormMatrixCongruence$\left(\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\right)$

| $M\leftarrow\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}$

| **while** $\neg(|b|\le|a|\le|c|)$

| | **if** $|c|<|a|$

| | $M\leftarrow\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)M\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)^t$

| | **if** $|a|<|b|$

| | | $k\leftarrow\{k\in\mathbb{Z}\mid|-b+2ck|\le|c|\}$

| | | $M\leftarrow\left(\begin{smallmatrix}1&0\\k&1\end{smallmatrix}\right)M\left(\begin{smallmatrix}1&0\\k&1\end{smallmatrix}\right)^t$

| **return** M

משפט: נסמן $\begin{pmatrix}d&\frac{e}{2}\\\frac{e}{2}&f\end{pmatrix}=\left(\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\right)$CanonicalFormMatrixCongruence אזי $\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\sim\begin{pmatrix}d&\frac{e}{2}\\\frac{e}{2}&f\end{pmatrix}$ וכן $|e|\le|d|\le|f|$.

סימון: תהא $A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}$ ותהא $f\in A$ אזי $\Delta_A=\Delta_f$.

מסקנה: יהי $\delta\in\mathbb{Z}\backslash\left\{k^2\mid k\in\mathbb{Z}\right\}$ המקיים $(\delta\equiv0\mod4)\vee(\delta\equiv1\mod4)$ אזי $|\{A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}\mid\Delta_A=\delta\}|\in\mathbb{N}$.

תבנית חיובית לחלוטין: $\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\in\mathrm{sym}_2(\mathbb{Z})$ המקיימת $(\Delta<0)\wedge(a>0)$.

מחלקה חיובית לחלוטין: $A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}$ עבורה כל $f\in A$ הינה חיובית לחלוטין.

תבנית שלילית לחלוטין: $\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\in\mathrm{sym}_2(\mathbb{Z})$ המקיימת $(\Delta<0)\wedge(a<0)$.

מחלקה שלילית לחלוטין: $A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}$ עבורה כל $f\in A$ הינה שלילית לחלוטין.

תבנית בצורה מצומצמת: $\begin{pmatrix}a&\frac{b}{2}\\\frac{b}{2}&c\end{pmatrix}\in\mathrm{sym}_2(\mathbb{Z})$ המקיימת $(-a<b\le a<c)\vee(0\le b\le a=c)$.

טענה: תהא $A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}$ חיובית לחלוטין אזי קיימת $f\in A$ מצומצמת.

טענה: תהא $f\in\mathrm{sym}_2(\mathbb{Z})$ מצומצמת אזי $\min_{x,y\in\mathbb{Z}\backslash\{0\}}f(x,y)=a-|b|+c$.

מסקנה: תהא $f\in\mathrm{sym}_2(\mathbb{Z})$ מצומצמת אזי $\min_{(x,y)\in\mathbb{Z}^2\backslash\{(0,0)\}}f(x,y)=a$.

מסקנה: תהא $f\in\mathrm{sym}_2(\mathbb{Z})$ מצומצמת אזי $\min_{\gcd(x,y)=1}f(x,y)=a$.

משפט: יהיו $f,g\in\mathrm{sym}_2(\mathbb{Z})$ מצומצמות אזי $(f\sim g)\Longleftrightarrow(f=g)$.

סימון: יהי $\delta\in\mathbb{Z}\backslash\mathbb{N}$ אזי $h(\delta)=|\{A\in{}^{\mathrm{sym}_2(\mathbb{Z})}/_{\sim}\mid(\Delta_A=\delta)\wedge(A\text{ חיובית לחלוטין})\}|$.

משפט: יהי $n\in\mathbb{N}_+$ אזי $\left(\exists k,m\in\mathbb{N}.k^2+m^2=n\right)\Longleftrightarrow(\forall p\in\mathbb{P}.(p|n)\wedge(p\equiv3\mod4)\Longrightarrow\max\{r\in\mathbb{N}|(p^r|n)\}\in\mathbb{N}_{\mathrm{even}})$.

מסקנה משפט פרמה: יהי $p\in\mathbb{P}\backslash\{2\}$ אזי $(p\equiv1\mod4)\Longleftrightarrow\left(\exists k,m\in\mathbb{N}.k^2+m^2=p\right)$.

טענה: יהי $\theta\in\mathbb{R}$ אזי (קיים ל־θ יצוג עשרוני סופי)$\Longleftrightarrow\left(\exists z\in\mathbb{Z}.\exists n,k\in\mathbb{N}.\theta=\frac{z}{2^n5^k}\right)$.

טענה: יהי $\theta\in\mathbb{R}$ אזי (קיים ל־θ יצוג עשרוני סופי)$\Longleftrightarrow$(קיימים ל־θ יצוגים עשרוניים שונים).

טענה: יהי $\theta\in\mathbb{R}$ אזי (קיים ל־θ יצוג מחזורי החל ממקום מסויים)$\iff(\theta\in\mathbb{Q})$.

סימון: יהיו $x_0\dots x_n\in\mathbb{R}$ אזי $[x_0,\dots,x_n]=x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{\ddots+\frac{1}{x_n}}}}}$.

שבר משולב: יהיו $a_0\dots a_n\in\mathbb{Z}$ אזי $[a_0,\dots,a_n]$.

טענה: יהי $\theta\in\mathbb{R}$ אזי $(\theta\in\mathbb{Q})\iff(\exists a_0\dots a_n\in\mathbb{Z}.\theta=[a_0,\dots,a_n])$.

סימון: תהא $x\in\mathbb{R}^{\mathbb{N}}$ אזי $[x_0,x_1,\dots]=x_0+\cfrac{1}{x_1+\cfrac{1}{x_2+\cfrac{1}{x_3+\cfrac{1}{\ddots}}}}$.

שבר משולב: תהא $a\in\mathbb{Z}^{\mathbb{N}}$ אזי $[a_0,a_1,\dots]$.

טענה: יהי $\theta\in\mathbb{R}$ אזי $(\theta\notin\mathbb{Q})\iff\left(\exists a\in\mathbb{Z}^{\mathbb{N}}.\theta=[a_0,a_1,\dots]\right)$.

אלגוריתם פיתוח מספר ממשי לשבר משולב: יהי $\theta\in\mathbb{R}$ אזי

function ContinuedFractionConverter (θ)

| **if** $\theta\in\mathbb{Z}$

| **return** θ

| $a\leftarrow\lfloor\theta\rfloor$

| $\theta'\leftarrow\dfrac{1}{\theta-a}$

| **return** $a+\dfrac{1}{\text{ContinuedFractionConverter}(\theta')}$

משפט: יהי $\theta\in\mathbb{R}$ אזי ContinuedFractionConverter (θ) הינו שבר משולב של θ. אם רץ לנצח השבר אינסופי

מנות חלקיות: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ אזי $a\in\mathbb{Z}^{\mathbb{N}}$ עבורה $\theta=[a_0,a_1,\dots]$.

הגורמים המתכנסים: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ ותהא $\theta=[a_0,a_1,\dots]$ אזי $\{[a_0,\dots,a_k]\}_{k=0}^{\infty}$.

הגדרה: תהא $a\in\mathbb{Z}^{\mathbb{N}}$ אזי נגדיר $p,q\in\mathbb{Z}^{\mathbb{N}\uplus\{-1,-2\}}$ כך

- $\binom{p_{-2}=0}{p_{-1}=1}\wedge(\forall k\in\mathbb{N}.p_k=a_kp_{k-1}+p_{k-2})$.
- $\binom{q_{-2}=1}{q_{-1}=0}\wedge(\forall k\in\mathbb{N}.q_k=a_kq_{k-1}+q_{k-2})$.

טענה: תהא $a\in\mathbb{R}^{\mathbb{N}}$ אזי $\forall n\in\mathbb{N}.[a_0\dots a_n]=\frac{p_n}{q_n}$.

טענה: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ ותהא $\theta=[a_0,a_1,\dots]$ אזי $\{q_n\}_{n=1}^{\infty}$ עולה ממש.

טענה: $\forall n\in\mathbb{N}\uplus\{-1\}.p_nq_{n-1}-p_{n-1}q_n=(-1)^{n-1}$.

מסקנה: $\forall n\in\mathbb{N}\uplus\{-1\}.\gcd(p_n,q_n)=1$.

טענה: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ אזי $\lim_{n\to\infty}\frac{p_n}{q_n}=\theta$.

מסקנה: תהא $a\in\mathbb{Z}^{\mathbb{N}}$ אזי $\lim_{n\to\infty}[a_0\dots a_n]=[a_0,a_1\dots]$.

למה: יהי $a\in\mathbb{Z}$ יהי $b\in\mathbb{N}$ ויהי $x\in\mathbb{R}$ אזי $\left\lfloor\frac{a+x}{b}\right\rfloor=\left\lfloor\frac{a+\lfloor x\rfloor}{b}\right\rfloor$.

סימון: יהיו $a_0\dots a_n,b_0\dots b_m\in\mathbb{Z}$ אזי $[a_1\dots a_n,\overline{b_1\dots b_m}]=[a_1\dots a_n,b_1\dots b_m,b_1\dots b_m\dots]$.

טרינום: יהיו $a,b,c\in\mathbb{R}$ אזי $f\in\mathbb{R}[x]$ המוגדר $f(x)=ax^2+bx+c$.

דסקרימיננטה: יהי $ax^2+bx+c\in\mathbb{R}[x]$ טרינום אזי $\Delta=b^2-4ac$.

משפט לגראנז': יהי $\alpha\in\mathbb{R}$ אזי $\left(\exists a_0\dots a_k,b_1\dots b_m\in\mathbb{Z}.\alpha=[a_0\dots a_k,\overline{b_1\dots b_m}]\right)\iff$(קיים טרינום $f\in\mathbb{Z}[x]$ המקיים $\Delta\in\mathbb{N}\backslash\{k^2\mid k\in\mathbb{N}\}$ עבורו $f(\alpha)=0$).

מספר ניתן לקירוב דיופנטי מסדר r: $\alpha\in\mathbb{R}$ המקיים $\exists c\in\mathbb{R}_+.\left|\left\{\frac{n}{m}\mid\binom{n\in\mathbb{Z}}{m\in\mathbb{Z}}\wedge\left(\left|\alpha-\frac{n}{m}\right|<\frac{1}{cm^r}\right)\right\}\right|\geq\aleph_0$.

טענה: יהי $\theta\in\mathbb{R}$ אזי $\exists p,q\in\mathbb{Z}.\left|\theta-\frac{p}{q}\right|\leq\frac{1}{2q}$.

מסקנה: יהי $\theta\in\mathbb{R}$ אזי θ ניתן לקירוב דיופנטי מסדר ראשון.

טענה: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ אזי $\forall n\in\mathbb{N}.\left|\theta-\frac{p_n}{q_n}\right|<\frac{1}{q_n^2}$.

מסקנה: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ אזי θ ניתן לקירוב דיופנטי מסדר שני.

משפט: יהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ אזי $\frac{p_n}{q_n}$ הינו הקירוב הדיופנטי הטוב ביותר כלומר

- במובן החלש: יהיו $a,b\in\mathbb{Z}$ באשר $1\le b<q_n$ אזי $\left|\theta-\frac{a}{b}\right|<\left|\theta-\frac{p_n}{q_n}\right|$.
- במובן החזק: יהיו $a,b\in\mathbb{Z}$ באשר $1\le b<q_{n+1}$ אזי $|b\theta-a|<|q_n\theta-p_n|$.

מספר אלגברי: $\alpha\in\mathbb{R}$ המקיים $\exists f\in\mathbb{Z}[x].f(\alpha)=0$.

מספר טרנסצנדנטי: $\alpha\in\mathbb{R}$ שאינו אלגברי.

מעלה של מספר אלגברי: יהי $\alpha\in\mathbb{R}$ אלגברי אזי $\min\left\{\deg(f)\mid(f\in\mathbb{Z}[x])\wedge(f(\alpha)=0)\right\}$.

משפט ליוביל: יהי $\alpha\in\mathbb{R}$ אלגברי ממעלה d אזי $\exists c\in\mathbb{R}_+.\forall\frac{p}{q}\in\mathbb{Q}\backslash\{\alpha\}.\left|\alpha-\frac{p}{q}\right|\ge\frac{c}{q^d}$.

מספר ליוביל: $\alpha\in\mathbb{R}$ המקיים $\forall d\in\mathbb{N}.\exists\frac{p}{q}\in\mathbb{Q}\backslash\{\alpha\}.\left|\alpha-\frac{p}{q}\right|<\frac{1}{q^d}$.

מסקנה: יהי $\alpha\in\mathbb{R}$ מספר ליוביל אזי α הינו טרנסצנדנטי.

קבוע ליוביל: $\sum_{n=1}^{\infty}\frac{1}{10^{n!}}$.

טענה: קבוע ליוביל הינו מספר ליוביל.

שדה ריבועי: יהי $d\in\mathbb{Z}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\mathbb{Q}\left[\sqrt{d}\right]=\left\{a+b\sqrt{d}\mid a,b\in\mathbb{Q}\right\}$.

טענה: יהי $d\in\mathbb{Z}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי

- $\mathbb{Q}\left[\sqrt{d}\right]$ מ"ו מעל $\mathbb{Q}$ ממימד 2 עם בסיס $\left\{1,\sqrt{d}\right\}$.
- $\mathbb{Q}\left[\sqrt{d}\right]$ שדה.

מספר אי־רציונלי ממעלה שנייה: $\theta\in\mathbb{R}\backslash\mathbb{Q}$ עבורו קיים $f\in\mathbb{Z}[x]$ טרינום המקיים $(f(\theta)=0)\wedge(\Delta=0)$.

משפט: יהי $f\in\mathbb{Z}[x]$ טרינום באשר $\Delta\notin\left\{k^2\mid k\in\mathbb{N}\right\}$ ויהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ פתרון אזי $\sigma(\theta)$ פתרון מעל $\mathbb{Q}\left[\sqrt{\Delta}\right]$.

טענה: יהיו $f,g\in\mathbb{Q}[x]$ טרינומים מתוקנים ויהי $\theta\in\mathbb{R}\backslash\mathbb{Q}$ פתרון של שניהם אזי $f=g$.

מספר אי־רציונלי ממעלה שנייה בעל מחזוריות טהורה: $\theta\in\mathbb{R}$ אי־רציונלי ממעלה שנייה המקיים $\exists a_0\ldots a_n\in\mathbb{Z}.\theta=\left[\overline{a_0\ldots a_n}\right]$.

משפט: יהי $\theta\in\mathbb{R}$ אי־רציונלי ממעלה שנייה אזי (θ בעל מחזוריות טהורה)$\Longleftrightarrow\left(\left(-1<\sigma(\theta)<0\text{ מעל }\mathbb{Q}\left[\sqrt{\Delta}\right]\right)\wedge(\theta>1)\right)$.

מסקנה: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\frac{1}{\sqrt{d}-\left\lfloor\sqrt{d}\right\rfloor},\left\lfloor\sqrt{d}\right\rfloor+\sqrt{d}$ בעלי מחזוריות טהורה.

משוואת פל: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $x^2-dy^2=1$.

פתרון משוואת פל: יהי $\substack{d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}\\ \sqrt{d}=\left[a_0,\overline{a_1\ldots a_m}\right]}$ אזי $\mathrm{sols}_{\mathbb{Z}^2}\left(x^2-dy^2=1\right)=\left\{\pm(p_n,q_n)\mid\substack{n\in\mathbb{N}_{\text{odd}}\\ \exists k\in\mathbb{Z}.n=mk-1}\right\}$.

סימון: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\mathcal{O}_d^*=\left\{x+y\sqrt{d}\;\middle|\;\substack{x,y\in\mathbb{Z}\\ x^2-dy^2=1}\right\}$.

טענה: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\mathcal{O}_d^*=\left\{x+y\sqrt{d}\;\middle|\;\substack{x,y\in\mathbb{Z}\\ N\left(x+y\sqrt{d}\right)=1}\right\}$.

מסקנה: $\mathcal{O}_d^*$ תת חבורה של $\mathbb{Q}\left[\sqrt{d}\right]$ ביחס לכפל.

מסקנה: יהי $z\in\mathbb{Q}\left[\sqrt{d}\right]$ אזי $\left(-z\in\mathcal{O}_d^*\right)\Longleftrightarrow\left(\frac{1}{z}\in\mathcal{O}_d^*\right)\Longleftrightarrow\left(z\in\mathcal{O}_d^*\right)$.

טענה: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\left|\mathcal{O}_d^*\right|\ge\aleph_0$.

טענה: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\varepsilon=\min\left\{x\in\mathcal{O}_d^*\mid x>1\right\}$ קיים.

משפט: יהי $d\in\mathbb{N}\backslash\left\{k^2\mid k\in\mathbb{N}\right\}$ אזי $\mathcal{O}_d^*=\left\{\pm\varepsilon^n\mid n\in\mathbb{Z}\right\}$.