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

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

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

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

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

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

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

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 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: $\mathbb{Z}$ 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 $A^{*}=\{a\in A\mid a^{-1}\in A\}$.

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

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

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

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

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

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

טענה: יחס החברות הינו יחס שקילות.

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

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

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

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

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

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

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

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

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

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

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

טענה: יהי $\alpha\in\mathbb{Z}$ עבורו $\sqrt{\alpha}\notin\mathbb{Q}$ אזי $\mathbb{Z}\left[\sqrt{\alpha}\right]^{*}=\left\{z\in\mathbb{Z}\left[\sqrt{\alpha}\right]\mid N\left(z\right)\in\{\pm1\}\right\}$.

משפט פירוק לאי פריקים מעל $\mathbb{Z}\left[\sqrt{\alpha}\right]$: יהי $\alpha\in\mathbb{Z}$ עבורו $\sqrt{\alpha}\notin\mathbb{Q}$ אזי $\mathbb{Z}\left[\sqrt{\alpha}\right]$ 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) $\iff$ (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) $\iff\left(a\mid b\right)$.

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

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

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 $r\mid d$) $\Longleftarrow\left(d=\gcd\left(a,b\right)\right)$.

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

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 $a \in \mathbb{Z} \backslash \{0\}$ ויהי $b \in \mathbb{N}$ אזי

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

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

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

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

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

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

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

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

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

טענה: תהא $\{p_n\}_{n=1}^{\infty}$ סדרת הראשוניים אזי $p_n \le 2^{2^n}$.

פונקציית ספירת ראשוניים: $\pi(x) = |\{p \le x \mid p \text{ ראשוני}\}|$.

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

טענה: $\pi(x) > \log\log(x)$.

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

```
function SieveOfEratosthenesAlgorithm(n)
    A ← [true_2, true_3, ..., true_n]
    for i ← 2...n
        if A[i] = true
            j ← 1
            while ij ≤ n
                A[ij] = false
                j ← j + 1
    return A
```

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

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

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

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

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

מספר מושלם: $n\in\mathbb{N}_+$ המקיים $n=\sum\limits_{\substack{d\mid n\\ 1\le d<n}}d$.

פונקציית סכום המחלקים: יהי $n\in\mathbb{N}_+$ אזי $\sigma\left(n\right)=\sum\limits_{\substack{d\mid n\\ 1\le d}}d$.

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 $p\in\mathbb{N}$ ראשוני 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 $F\left(n\right)=\sum_{d\mid n}f\left(d\right)$ כפלית.

פונקציית מביוס: נגדיר $\mu:\mathbb{N}\to\{0,\pm1\}$ כפלית יהי p ראשוני אזי $\mu\left(p^r\right)=\begin{cases}1 & r=0\\ -1 & r=1\\ 0 & r\ge2\end{cases}$.

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

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

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

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.

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

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

מסקנה: תהא $\begin{pmatrix}x\\y\\z\end{pmatrix}$ 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 $\begin{pmatrix}x\\y\\z\end{pmatrix}=\begin{pmatrix}u^2-v^2\\ 2uv\\ u^2+v^2\end{pmatrix}$.