טענה: $\mathbb{Z}\subseteq\mathbb{R}$.

תת־קבוצה סגורה ביחס לחיבור חיסור וכפל: קבוצה $S\subseteq\mathbb{R}$ עבורה לכל $a,b\in S$ מתקיים $a+b\in S$ וכן $a-b\in S$ וכן $ab\in S$.

טענה: $\mathbb{Z}$ סגורה ביחס לחיבור חיסור וכפל.

קבוצה המקיימת את האי־שיוויון היסודי של תורת המספרים: קבוצה $S\subseteq\mathbb{R}$ המקיימת $S\cap(0,1]=\{1\}$.

טענה: $\mathbb{Z}$ מקיימת את אי־שיוויון היסודי של תורת המספרים.

טענה: תהא $S\subseteq\mathbb{R}$ המקיימת את האי־שיוויון היסודי של תורת המספרים וכן סגורה ביחס לחיבור חיסור וכפל אזי $S=\mathbb{Z}$.

מסקנה עיקרון הסדר הטוב על הטבעיים: תהא $S\subseteq\mathbb{N}$ באשר $S\neq\varnothing$ אזי $\min(S)$ קיים.

טענה: תהא $S\subseteq\mathbb{Z}$ חסומה מלרע באשר $S\neq\varnothing$ אזי $\min(S)$ קיים.

מסקנה: תהא $S\subseteq\mathbb{Z}$ חסומה מלעיל באשר $S\neq\varnothing$ אזי $\max(S)$ קיים.

מסקנה: $\mathbb{Z}$ אינה חסומה מלרע וכן אינה חסומה מלעיל.

מסקנה עיקרון האינדוקציה: יהי P פרידיקט מעל $\mathbb{N}$ באשר $P(0)$ וכן לכל $n\in\mathbb{N}$ מתקיים $P(n+1)\Longrightarrow P(n)$ אזי $P(m)$ לכל $m\in\mathbb{N}$.

טענה עיקרון האינדוקציה החזקה: יהי P פרידיקט מעל $\mathbb{N}$ באשר $P(0)$ וכן לכל $n\in\mathbb{N}$ מתקיים $(\forall m<n.P(m))\Longrightarrow P(n+1)$ אזי $P(k)$ לכל $k\in\mathbb{N}$.

מספר מתחלק במספר: יהי $b\in\mathbb{Z}$ אזי $a\in\mathbb{Z}$ עבורו קיים $c\in\mathbb{Z}$ המקיים $b=ac$.

סימון: יהיו $a,b\in\mathbb{Z}$ באשר b מתחלק ב־a אזי $a|b$.

סימון: יהיו $a,b\in\mathbb{Z}$ באשר b אינו מתחלק ב־a אזי $a\nmid b$.

טענה: יהי $a\in\mathbb{Z}$ אזי $a|0$.

טענה: יהי $a\in\mathbb{Z}$ אזי $1|a$ וכן $-1|a$.

טענה: יהיו $a,b,c\in\mathbb{Z}$ באשר $a|b$ וכן $a|c$ אזי לכל $c,d\in\mathbb{Z}$ מתקיים $a|(db+ec)$.

טענה: יהיו $a,b,c\in\mathbb{Z}$ באשר $a|b$ וכן $b|c$ אזי $a|c$.

טענה: יהיו $a,b\in\mathbb{N}$ באשר $a|b$ אזי $a\leq b$.

טענה: יהיו $a,b\in\mathbb{Z}$ אזי $(a\in\{\pm b\})\Longleftrightarrow((a|b)\wedge(b|a))$.

טענה חלוקה עם שארית: יהי $d\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}$ אזי קיימים ויחידים $q,r\in\mathbb{Z}$ באשר $0\leq r<d$ וכן $a=qd+r$.

מנה של חלוקה: יהי $d\in\mathbb{N}_+$ יהי $a\in\mathbb{Z}$ ויהיו $q,r\in\mathbb{Z}$ חלוקה עם שארית של a ב־d אזי q.

שארית של חלוקה: יהי $d\in\mathbb{N}_+$ יהי $a\in\mathbb{Z}$ ויהיו $q,r\in\mathbb{Z}$ חלוקה עם שארית של a ב־d אזי r.

מסקנה: יהי $d\in\mathbb{N}_+$ יהי $a\in\mathbb{Z}$ ויהיו $q,r\in\mathbb{Z}$ חלוקה עם שארית של a ב־d אזי $(d|a)\Longleftrightarrow(r=0)$.

החלק השלם/ערך שלם תחתון: יהי $x\in\mathbb{R}$ אזי $\lfloor x\rfloor=\max((-\infty,x]\cap\mathbb{Z})$.

מסקנה: יהי $d\in\mathbb{N}_+$ יהי $a\in\mathbb{Z}$ ויהיו $q,r\in\mathbb{Z}$ חלוקה עם שארית של a ב־d אזי $q=\left\lfloor\frac{a}{d}\right\rfloor$.

טענה: תהא $H\leq\mathbb{Z}$ אזי קיים ויחיד $d\in\mathbb{N}$ עבורו $H=d\mathbb{Z}$.

טענה: יהיו $a,b\in\mathbb{Z}$ אזי $a\mathbb{Z}+b\mathbb{Z}\leq\mathbb{Z}$.

מחלק משותף מירבי: יהיו $a,b\in\mathbb{Z}$ אזי $d\in\mathbb{N}$ עבורו $d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z}$.

סימון: יהיו $a,b\in\mathbb{Z}$ ויהי $d\in\mathbb{N}$ המחלק המשותף המירבי של a,b אזי $\gcd(a,b)=d$.

סימון: יהיו $a,b\in\mathbb{Z}$ אזי $(a,b)=\gcd(a,b)$.

טענה: יהיו $a,b\in\mathbb{Z}$ אזי $\gcd(a,b)|a$ וכן $\gcd(a,b)|b$.

מסקנה: יהיו $a,b\in\mathbb{Z}$ אזי קיימים $n,m\in\mathbb{Z}$ עבורם $\gcd(a,b)=na+mb$.

טענה: יהיו $a,b,c\in\mathbb{Z}$ באשר $c|a$ וכן $c|b$ אזי $c|\gcd(a,b)$.

טענה: יהיו $a,b\in\mathbb{Z}$ באשר $\{a,b\}\neq\{0\}$ אזי $\gcd(a,b)=\max\{d\in\mathbb{Z}\mid(d|a)\wedge(d|b)\}$.

טענה: יהיו $a,b\in\mathbb{Z}$ ויהי $d\in\mathbb{N}$ באשר $d|a$ וכן $d|b$ וכן קיימים $n,m\in\mathbb{Z}$ עבורם $d=na+mb$ אזי $\gcd(a,b)=d$.

מחלק משותף מירבי: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי $d\in\mathbb{N}$ עבורו $d\mathbb{Z}=\sum_{i=1}^{n}a_i\mathbb{Z}$.

סימון: יהיו $a_1\ldots a_n\in\mathbb{Z}$ ויהי $d\in\mathbb{N}$ המחלק המשותף המירבי של $a_1\ldots a_n$ אזי $\gcd(a_1\ldots a_n)=d$.

טענה: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי $\gcd(a_1\ldots a_n)|a_i$ לכל $i\in[n]$.

מסקנה: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי קיים $m\in\mathbb{Z}^n$ עבורו $\gcd(a_1\ldots a_n)=\sum_{i=1}^{n}m_i\cdot a_i$.

טענה: יהיו $a_1\ldots a_n,d\in\mathbb{Z}$ באשר $d|a_i$ לכל $i\in[n]$ אזי $d|\gcd(a_1\ldots a_n)$.

מספרים זרים: מספרים $a_1\ldots a_n\in\mathbb{Z}$ המקיימים $(a_1\ldots a_n)=1$.

טענה: יהי $b \in \mathbb{N}_{\geq 2}$ ויהי $n \in \mathbb{N}$ אזי קיים ויחיד $k \in \mathbb{N}$ וקיים ויחיד $d \in \{0, \ldots, b-1\}^k$ באשר $d_k > 0$ המקיים $n = \sum_{i=1}^{k} d_i b^i$.

ייצוג ספרתי בבסיס: יהי $b \in \mathbb{N}_{\geq 2}$ ויהיו $n, k \in \mathbb{N}$ ויהי $d \in \{0, \ldots, b-1\}^k$ באשר $d_k > 0$ וכן $n = \sum_{i=1}^{k} d_i b^i$ אזי $(n)_b = d$.

הערה: כאשר לא כתוב בסיס בייצוג נתייחס לבסיס עשרוני.

טענה: יהי $b \in \mathbb{N}_{\geq 2}$ ויהי $n \in \mathbb{N}$ אזי $\text{len}\left((n)_b\right) = \lfloor \log_b(n) \rfloor + 1$.

מספר הביטים לייצוג מספר: יהי $n \in \mathbb{N}$ אזי $\text{len}\left((n)_2\right)$.

הערה: בסיבוכיות של אלגוריתמים מספריים נתייחס לסיבוכיות כפונקציה של אורך המספר בבינארי.

טענה: קיים אלגוריתם $\mathcal{A}$ המחשב חיבור מספרים בסיבוכיות ריצה $\mathcal{O}(n)$.

טענה: קיים אלגוריתם $\mathcal{A}$ המחשב כפל מספרים בסיבוכיות ריצה $\mathcal{O}\left(n^2\right)$.

אלגוריתם קרטסובה: יהי $n \in \mathbb{N}$ ויהיו $a, b \in \{0,1\}^n$ אזי

```
Function KaratsubaMult(a, b):
    α ← (a_1 ... a_{n/2});    β ← (a_{n/2+1} ... a_n)
    γ ← (b_1 ... b_{n/2});    δ ← (b_{n/2+1} ... b_n)
    A ← KaratsubaMult(α, γ)
    B ← KaratsubaMult(β, δ)
    C ← KaratsubaMult(α + β, γ + δ)
    return B · 2^n + (C − B − A) · 2^{n/2} + A
```

טענה: יהי $a, b \in \mathbb{N}$ אזי $\left(\text{KaratsubaMult}\left((a)_2, (b)_2\right)\right)_{10} = ab$.

טענה: יהיו $a, b \in \mathbb{N}$ באורך n ביטים אזי סיבוכיות הריצה של KaratsubaMult הינה $\mathcal{O}\left(n^{\log_2(3)}\right)$.

טענה קולי־טוקי: קיים אלגוריתם $\mathcal{A}$ המחשב כפל מספרים בסיבוכיות ריצה $\mathcal{O}(n \log(n) \log\log(n))$.

למה: יהיו $a, b, q \in \mathbb{Z}$ אזי $\gcd(a, b) = \gcd(a + qb, b)$.

אלגוריתם אוקלידס: יהיו $a, b \in \mathbb{Z}$ אזי

```
Function EuclidGCD(a, b):
    if (a < 0) ∨ (b < 0) ∨ (|a| < |b|) then
        return EuclidGCD(max{|a|, |b|}, min{|a|, |b|})
    if b = 0 then return a
    (q, r) ← RemainderDiv(a, b)
    return EuclidGCD(b, r)
```

טענה: יהיו $a, b \in \mathbb{Z}$ אזי $\text{EuclidGCD}(a, b) = \gcd(a, b)$.

טענה: יהיו $a, b \in \mathbb{Z}$ אזי סיבוכיות הריצה של EuclidGCD הינה $\mathcal{O}\left(n^2\right)$.

טענה: יהי $k \in \mathbb{N}_+$ אזי $(-1)^k F_{k-1} \cdot F_{k+1} + (-1)^{k+1} F_k F_k = 1$.

טענה: קיים אלגוריתם $\mathcal{A}$ המחשב gcd בסיבוכיות ריצה $\mathcal{O}\left(n \log^2(n)\right)$.

כפולה משותפת מזערית: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ אזי $d \in \mathbb{N}$ עבורו $d\mathbb{Z} = \bigcap_{i=1}^{n} a_i \mathbb{Z}$.

סימון: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ ויהי $d \in \mathbb{N}$ הכפולה המשותפת המזערית של $a_1 \ldots a_n$ אזי $\text{lcm}(a_1 \ldots a_n) = d$.

סימון: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ אזי $[a_1 \ldots a_n] = \text{lcm}(a_1 \ldots a_n)$.

טענה: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ אזי $a_i | \text{lcm}(a_1 \ldots a_n)$ לכל $i \in [n]$.

טענה: יהיו $a_1 \ldots a_n, m \in \mathbb{Z}$ באשר $a_i | m$ לכל $i \in [n]$ אזי $\text{lcm}(a_1 \ldots a_n) | m$.

טענה: יהיו $a_1 \ldots a_n \in \mathbb{Z} \backslash \{0\}$ אזי $\text{lcm}(a_1 \ldots a_n) = \min\left\{m \in \mathbb{N}_+ \mid \forall i \in [n] . (a_i | m)\right\}$.

למה: יהיו $a, b \in \mathbb{Z}$ באשר $a \neq 0$ אזי $\left(\frac{b}{a} \in \mathbb{Z}\right) \iff (a|b)$.

למה: יהיו $a, b, c \in \mathbb{Z}$ אזי $(ac|bc) \iff (a|b)$.

טענה: יהיו $a, b \in \mathbb{N}_+$ אזי $[a, b] = \frac{ab}{(a,b)}$.

טענה: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ אזי $[a_1, \ldots, a_n] = [|a_1|, \ldots, |a_n|]$.

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

מסקנה: יהיו $a, b \in \mathbb{Z}$ זרים אזי $[a, b] = |ab|$.

טענה: יהיו $a_1 \ldots a_n \in \mathbb{Z}$ אזי $[a_1 \ldots a_n] = [[a_1 \ldots a_{n-1}], a_n]$.

מספר ראשוני: מספר $p\in\mathbb{N}_{\geq2}$ עבורו לכל $a,b\in\mathbb{N}_{\geq2}$ מתקיים $ab\neq p$.

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

מספר פריק: מספר $m\in\mathbb{N}_{\geq2}$ באשר $m\notin\mathbb{P}$.

טענה: יהי $p\in\mathbb{P}$ ויהיו $a,b\in\mathbb{Z}$ באשר $p|ab$ אזי $(p|a)\vee(p|b)$.

טענה: יהי $n\in\mathbb{N}$ עבורו לכל $a,b\in\mathbb{Z}$ אם $n|ab$ אז $(n|a)\vee(n|b)$ אזי $n\in\{0,\pm1\}\cup(\pm\mathbb{P})$.

מסקנה: יהי $p\in\mathbb{P}$ ויהיו $a_1\dots a_n\in\mathbb{Z}$ באשר $p|\prod_{i=1}^{n}a_i$ אזי קיים $i\in[n]$ המקיים $p|a_i$.

למה: יהי $n\in\mathbb{N}_{\geq2}$ אזי קיים $p\in\mathbb{P}$ המקיים $p|n$.

אלגוריתם הנפה של ארטוסתנס: יהי $N\in\mathbb{N}_+$ אזי

```
Function EratosthenesSieve(N):
    A ← ⟨True | n ∈ [1,...,N]⟩ ;    A_1 = False
    for i ∈ [1,...,N] do
        if A_i = True then
            j ← 1
            while i + 2j ≤ N do
                A_{i+2j} = False
                j ← j + 1
            end
        end
    end
    return {i ∈ [N] | A_i = True}
```

טענה: יהי $N\in\mathbb{N}_+$ אזי $\text{EratosthenesSieve}(N)=\{p\in\mathbb{P}\mid p\leq N\}$.

טענה: יהי $N\in\mathbb{N}_+$ אזי סיבוכיות הריצה של $\text{EratosthenesSieve}(N)$ הינה $\mathcal{O}\left(\left(\sum_{p\in\mathbb{P}_{\leq N}}\frac{1}{p}\right)\cdot N\right)$.

טענה אטקין־ברנסטיין: קיים אלגוריתם $\mathcal{A}$ עבורו $\mathcal{A}(N)=\mathbb{P}_{\leq N}$ לכל $N\in\mathbb{N}_+$ וכן $\mathcal{A}$ רץ בסיבוכיות ריצה $\mathcal{O}(N)$.

משפט היסודי של האריתמטיקה: יהי $n\in\mathbb{N}_+$ אזי קיימים ויחידים $p_1\dots p_k\in\mathbb{P}$ באשר $p_i<p_{i+1}$ לכל $i\in[k-1]$ המקיימים $n=\prod_{i=1}^{k}p_i$.

סימון: יהי $n\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ אזי $e_p(n)=\max\{m\in\mathbb{N}\mid(p^m|n)\}$.

סימון: יהי $n\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ אזי $p^{e_p(n)}\|n$.

מסקנה: יהי $n\in\mathbb{N}_+$ אזי $n=\prod_{p\in\mathbb{P}}p^{e_p(n)}$.

מסקנה: יהיו $n,m\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ אזי $e_p(mn)=e_p(m)+e_p(n)$.

מסקנה: יהיו $n,m\in\mathbb{N}_+$ אזי $(m|n)\iff(\forall p\in\mathbb{P}.e_p(m)\leq e_p(n))$.

מסקנה: יהיו $a_1\dots a_n\in\mathbb{N}_+$ אזי $(a_1\dots a_n)=\prod_{p\in\mathbb{P}}p^{\min\{e_p(a_i)|i\in[n]\}}$.

מסקנה: יהיו $a_1\dots a_n\in\mathbb{N}_+$ אזי $[a_1\dots a_n]=\prod_{p\in\mathbb{P}}p^{\max\{e_p(a_i)|i\in[n]\}}$.

מסקנה: יהיו $n,m\in\mathbb{N}_+$ אזי (m,n זרים)$\iff$(לא קיים $p\in\mathbb{P}$ המקיים $p|m$ וכן $p|n$).

טענה: יהי $n\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ אזי $e_p(n!)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$.

משפט אוקלידס: $|\mathbb{P}|\geq\aleph_0$.

טענה: יהי $n\in\mathbb{N}$ אזי קיים $b\in\mathbb{N}$ עבורו $\{b+i\mid i\in\{0,\dots,n\}\}\cap\mathbb{P}=\varnothing$.

השערה הראשוניים התאומים: יהי $N\in\mathbb{N}$ אזי קיים $p\in\mathbb{P}$ באשר $p\geq N$ וכן $p+2\in\mathbb{P}$. השערה פתוחה

טענה: יהי $n\in\mathbb{N}_{\geq2}$ אזי $\prod_{p\in\mathbb{P}_{\leq n}}p\leq4^{n-1}$.

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

ראשוני מרסן: ראשוני $p\in\mathbb{P}$ עבורו קיימים $a,n\in\mathbb{N}_+$ המקיימים $p=a^n-1$.

טענה: יהי $p\in\mathbb{P}$ ראשוני מרסן אזי קיים $q\in\mathbb{P}$ עבורו $p=2^q-1$.

טענה: יהי $n\in\mathbb{N}_+$ אזי $|\mathbb{Z}/n\mathbb{Z}|=n$.

טענה: יהי $n\in\mathbb{N}_+$ יהי $a\in\mathbb{Z}$ תהא $\pi:\mathbb{Z}\to\mathbb{Z}/n\mathbb{Z}$ העתקת המנה ויהי $r\in\mathbb{N}$ שארית החלוקה של a ב־n אזי $\pi(a)=r+n\mathbb{Z}$.

מודלו: יהי $n\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}$ אזי $(a\mod n)=a+n\mathbb{Z}$.

מספרים שקולים תחת מודולו: יהי $n\in\mathbb{N}_+$ אזי $a,b\in\mathbb{Z}$ עבורם $(a\mod n)=(b\mod n)$.

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

טענה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b\in\mathbb{Z}$ אזי $(a\equiv b \mod n)\iff(n|(a-b))$.

טענה: יהיו $n,r\in\mathbb{N}_+$ באשר $r|n$ ויהיו $\alpha,\beta\in\mathbb{Z}$ באשר $r|\alpha,\beta$ אזי $\left(\frac{\alpha}{r}\equiv\frac{\beta}{r} \mod \frac{n}{r}\right)\iff(\alpha\equiv\beta \mod n)$.

למה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b,c,d\in\mathbb{Z}$ באשר $a\equiv c \mod n$ וכן $b\equiv d \mod n$ אזי $a+b\equiv c+d \mod n$.

הגדרה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b\in\mathbb{Z}$ אזי $(a \mod n)+(b \mod n)=((a+b) \mod n)$.

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathbb{Z}/n\mathbb{Z}$ חבורה אבלית.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $(2|a_0)\iff(2|a)$.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $\left(3|\left(\sum_{i=0}^{k}a_i\right)\right)\iff(3|a)$.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $(5|a_0)\iff(5|a)$.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $\left(7|\left(5a_0+\sum_{i=1}^{k}10^{i-1}a_i\right)\right)\iff(7|a)$.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $\left(9|\left(\sum_{i=0}^{k}a_i\right)\right)\iff(9|a)$.

טענה: יהי $k\in\mathbb{N}$ ויהיו $a_0\ldots a_k\in\{0,\ldots,9\}$ אזי $\left(11|\sum_{i=0}^{k}(-1)^i a_i\right)\iff(11|a)$.

למה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b,c,d\in\mathbb{Z}$ באשר $a\equiv c \mod n$ וכן $b\equiv d \mod n$ אזי $ab\equiv cd \mod n$.

הגדרה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b\in\mathbb{Z}$ אזי $(a \mod n)\cdot(b \mod n)=((a\cdot b) \mod n)$.

הערה: אלא אם כן נאמר אחרת חוג הינו חוג חילופי בעל יחידה.

טענה: יהי $n\in\mathbb{N}_+$ אזי $\mathbb{Z}/n\mathbb{Z}$ חוג.

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

למה: יהי $n\in\mathbb{N}_+$ ויהיו $a,b\in\mathbb{Z}$ באשר $a\equiv b \mod n$ אזי $(a,n)=(b,n)$.

טענה: יהי $n\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}$ אזי $\left((a \mod n)\in(\mathbb{Z}/n\mathbb{Z})^\times\right)\iff((a,n)=1)$.

אלגוריתם הופכי בחבורת שאריות החלוקה: יהי $n\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}$ אזי ...

טענה: יהי $p\in\mathbb{P}$ אזי $(\mathbb{Z}/p\mathbb{Z})^\times=\{(i \mod p)\mid i\in\{0,\ldots,p-1\}\}$.

פונקציית אוילר: נגדיר $\varphi:\mathbb{N}_+\to\mathbb{N}$ כך $\varphi(n)=\left|(\mathbb{Z}/n\mathbb{Z})^\times\right|$.

טענה: יהיו $p_1\ldots p_k\in\mathbb{P}$ שונים ויהיו $e_1\ldots e_k\in\mathbb{N}_+$ אזי $\varphi\left(\prod_{i=1}^{k}p_i^{k_i}\right)=n\cdot\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)$.

טענה: יהי $p\in\mathbb{P}$ ראשוני עבורו קיים $n\in\mathbb{N}_+$ המקיים $\varphi(n)=2p$ אזי p ראשוני סופי ז'רמן.

משפט אוילר: יהי $n\in\mathbb{N}_+$ ויהי $a\in\mathbb{Z}$ באשר $(a,m)=1$ אזי $a^{\varphi(n)}\equiv 1 \mod n$.

משפט הקטן של פרמה: יהי $p\in\mathbb{P}$ ויהי $a\in\mathbb{Z}$ באשר $p\nmid a$ אזי $a^{p-1}\equiv 1 \mod p$.

מסקנה: יהי $p\in\mathbb{P}$ ויהי $a\in\mathbb{Z}$ אזי $a^p\equiv a \mod p$.

מספרים זרים בזוגות: מספרים $a_1\ldots a_n\in\mathbb{Z}$ המקיימים $(a_i,a_j)=1$ לכל $i,j\in[n]$.

טענה: יהיו $a_1\ldots a_n\in\mathbb{Z}$ זרים בזוגות אזי $[a_1,\ldots,a_n]=\prod_{i=1}^{n}a_i$.

הגדרה: יהי $m\in\mathbb{N}_+^n$ ויהיו $a,v\in\mathbb{Z}^n$ באשר $v_i\equiv a_i \mod m_i$ לכל $i\in[n]$ אזי $v\equiv a \mod m$.

הגדרה: יהי $n\in\mathbb{N}_+$ אזי נגדיר $\mathbb{1}^n\in\mathbb{N}^n$ כך $\left(\mathbb{1}^n\right)_i=1$ לכל $i\in[n]$.

משפט השאריות הסיני: יהיו $m_1\ldots m_n\in\mathbb{N}_+$ זרים בזוגות ויהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי

- קיים $s\in\mathbb{Z}$ המקיים $\mathbb{1}^n s\equiv a \mod m$.
- לכל $y\in\mathbb{Z}$ המקיים $\mathbb{1}^n y\equiv a \mod m$ מתקיים $\text{sols}_{\mathbb{Z}}\left(\mathbb{1}^n x\equiv a \mod m\right)=\{y+k\prod_{i=1}^{n}m_i\mid k\in\mathbb{Z}\}$.

אלגוריתם פתרון למערכת משוואות מודולרית: יהיו $m_1\ldots m_n\in\mathbb{N}_+$ זרים בזוגות ויהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי ...

טענה: יהיו $m_1\ldots m_n\in\mathbb{N}_+$ ויהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי (קיים $x\in\mathbb{Z}$ המקיים $\mathbb{1}^n x\equiv a \mod m$)$\iff$(לכל $i,j\in[n]$ מתקיים $a_i\equiv a_j \mod (m_i,m_j)$).

משפט השאריות הסיני: יהיו $m_1\ldots m_n\in\mathbb{N}_+$ זרים בזוגות אזי $\mathbb{Z}/(\prod_{i=1}^{n}m_i)\mathbb{Z}\simeq\prod_{i=1}^{n}\mathbb{Z}/m_i\mathbb{Z}$.