

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־שוויון היסודי של תורת המספרים: קבוצה $S \subseteq \mathbb{R}$ המקיימת $S \cap (0, 1] = \{1\}$.
טענה: \mathbb{Z} מקיימת את אי־שוויון היסודי של תורת המספרים.

טענה: תהא $S \subseteq \mathbb{R}$ המקיימת את האי־שוויון 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 $S \neq \emptyset$ אזי $\min(S)$ קיים.

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

מסקנה: תהא $S \subseteq \mathbb{Z}$ חסומה מלעיל באשר $S \neq \emptyset$ 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 $P(n) \implies P(n+1)$ 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 $P(n+1) \implies (\forall m < n. P(m))$ 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 $a|1$ וכן $a|-1$.

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 $a|c$ 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 $((a|b) \wedge (b|a)) \iff (a \in \{\pm b\})$.

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 $d \in \mathbb{N}_+$ ויהי $a \in \mathbb{Z}$ חלוקה עם שארית של a ב־ d אזי q .

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

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

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

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

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 $\gcd(a, b) = \gcd(b, a)$.

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 $a_1 \dots a_n \in \mathbb{Z}$ אזי $d \in \mathbb{N}$ עבורו $d\mathbb{Z} = \sum_{i=1}^n a_i \mathbb{Z}$.

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

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

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

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

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

מספר פרמה: $F_k = 2^{2^k} + 1$ יהי $k \in \mathbb{N}$ אזי

טענה: יהי $k \in \mathbb{N}$ אזי $F_{k+1} - 2 = \prod_{i=0}^k F_i$

מסקנה: יהיו $k, n \in \mathbb{N}$ שונים אזי $(F_k, F_n) = 1$

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

ייצוג ספרתי בבסיס: יהי $b \in \mathbb{N}_{\geq 2}$ יהיו $n, k \in \mathbb{N}$ ויהי $d \in \{0, \dots, b-1\}^k$ 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 $\text{len}((n)_b) = \lfloor \log_b(n) \rfloor + 1$

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

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 $\mathcal{O}(n^2)$.

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

Function KaratsubaMult(a, b):

$\alpha \leftarrow (a_1 \dots a_{\frac{n}{2}}); \quad \beta \leftarrow (a_{\frac{n}{2}+1} \dots a_n)$

$\gamma \leftarrow (b_1 \dots b_{\frac{n}{2}}); \quad \delta \leftarrow (b_{\frac{n}{2}+1} \dots b_n)$

$A \leftarrow \text{KaratsubaMult}(\alpha, \gamma)$

$B \leftarrow \text{KaratsubaMult}(\beta, \delta)$

$C \leftarrow \text{KaratsubaMult}(\alpha + \beta, \gamma + \delta)$

return $B \cdot 2^n + (C - B - A) \cdot 2^{\frac{n}{2}} + A$

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

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

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 $(a < 0) \vee (b < 0) \vee (|a| < |b|)$ **then**

return EuclidGCD($\max\{|a|, |b|\}, \min\{|a|, |b|\}$)

if $b = 0$ **then return** a

$(q, r) \leftarrow \text{RemainderDiv}(a, b)$

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 $\mathcal{O}(n^2)$

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 $\mathcal{O}(n \log^2(n))$

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

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

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

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

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

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

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

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

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

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

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 $a_1 \dots a_n \in \mathbb{Z}$ אזי $[a_1 \dots a_n] = [[a_1 \dots a_{n-1}], a_n]$.

מספר ראשוני: מספר $p \in \mathbb{N}_{\geq 2}$ עבורו לכל $a, b \in \mathbb{N}_{\geq 2}$ מתקיים $ab \neq p$.

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

מספר פריק: מספר $m \in \mathbb{N}_{\geq 2}$ 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 $n \in \{0, \pm 1\} \cup (\pm \mathbb{P})$.

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

למה: יהי $n \in \mathbb{N}_{\geq 2}$ 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]⟩; A1 = False
for i ∈ [1, ..., N] do
  if Ai = True then
    j ← 1
    while i + 2j ≤ N do
      Ai+2j = False
      j ← j + 1
    end
  end
end
return {i ∈ [N] | Ai = 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 $(a_1 \dots a_n) = \prod_{p \in \mathbb{P}} p^{\min\{e_p(a_i) \mid i \in [n]\}}$.

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

מסקנה: יהיו $n, m \in \mathbb{N}_+$ אזי $(m, n) \iff$ (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: $|\mathbb{P}| = \aleph_0$.

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

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 $n \in \mathbb{N}_{\geq 2}$ אזי $\prod_{p \in \mathbb{P}_{\leq n}} p \leq 4^{n-1}$.

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: $|\{p \in \mathbb{P} \mid \exists n \in \mathbb{N}. p = 4n+3\}| = \aleph_0$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $(\mathbb{Z}/n\mathbb{Z})^\times \iff (n \in \mathbb{P})$.

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

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

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

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

פונקציית אויילר: נגדיר $\varphi: \mathbb{N}_+ \rightarrow \mathbb{N}$ כך $\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times|$.

טענה: יהיו $p_1 \dots p_k \in \mathbb{P}$ שונים ויהיו $e_1 \dots e_k \in \mathbb{N}_+$ אזי $\varphi(\prod_{i=1}^k p_i^{e_i}) = \prod_{i=1}^k (p_i^{e_i} - p_i^{e_i-1})$.

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

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

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

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

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

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

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

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

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

• קיים $s \in \mathbb{Z}$ המקיים $\mathbf{1}^n s \equiv a \pmod m$.

• לכל $y \in \mathbb{Z}$ המקיים $\mathbf{1}^n y \equiv a \pmod m$ מתקיים $\text{sols}_{\mathbb{Z}}(\mathbf{1}^n x \equiv a \pmod m) = \{y + k \prod_{i=1}^n m_i \mid k \in \mathbb{Z}\}$.

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

טענה: יהיו $m_1 \dots m_n \in \mathbb{N}_+$ ויהיו $a_1 \dots a_n \in \mathbb{Z}$ אזי (קיים $x \in \mathbb{Z}$ המקיים $\mathbf{1}^n x \equiv a \pmod m$) \iff (לכל $i, j \in [n]$ מתקיים

$(a_i \equiv a_j \pmod{(m_i, m_j)})$).

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

טענה: יהי $n \in \mathbb{N}_{\geq 2}$ אזי $\sum_{\substack{k \in [n] \\ \gcd(k, n) = 1}} k = \frac{1}{2}n \cdot \varphi(n)$.

טענה: יהיו $n, d \in \mathbb{N}_+$ תהא G חבורה ציקלית מסדר n ויהי $g \in G$ יוצר של G אזי $(n \mid d) \iff (g^d = 1)$.

טענה: יהיו $n, d \in \mathbb{N}_+$ תהא G חבורה ציקלית מסדר n ויהי $g \in G$ יוצר של G אזי $\text{ord}(g^d) = \frac{n}{(n, d)}$.

טענה: יהיו $d, n \in \mathbb{N}_+$ באשר $d|n$ ותהא G חבורה ציקלית מסדר n אזי $|\varphi(d)| = |\{a \in G \mid \text{ord}(a) = d\}|$.

טענה: יהי $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $\{a \in G \mid a \text{ יוצר של } G\} = \{g^d \mid (d, n) = 1\}$.

מסקנה: יהי $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $|\{g^d \mid (d, n) = 1\}| = \varphi(n)$.

מסקנה: יהיו $d, n \in \mathbb{N}_+$ באשר $d|n$ ותהא G חבורה ציקלית מסדר n אזי $|\{a \in G \mid a^d = 1\}| = d$.

מסקנה: יהיו $d, n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $|\{a \in G \mid a^d = 1\}| = (n, d)$.

מסקנה: יהי $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $(G \text{ ציקלית}) \iff |G| \mid d \mid \text{מתקיים } d \leq |\{a \in \mathbb{Z}_n \mid a^d = 1\}|$.

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

מסקנה: יהי \mathbb{F} שדה ותהא $G \leq \mathbb{F}^\times$ סופית אזי G ציקלית.

שורש פרימיטיבי: יהי $n \in \mathbb{N}_+$ אזי $g \in \mathbb{Z}$ עבורו $\langle g \bmod n \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$.

מסקנה: יהי $n \in \mathbb{N}_+$ אזי (קיים שורש פרימיטיבי מודולו n) $\iff (\mathbb{Z}/n\mathbb{Z})^\times$ חבורה ציקלית.

טענה: יהיו $n, k \in \mathbb{N}_+$ ויהי a שורש פרימיטיבי מודולו p אזי (a^k) שורש פרימיטיבי מודולו p $\iff (k, \varphi(n)) = 1$.

מסקנה: יהי $n \in \mathbb{N}_+$ באשר קיים שורש פרימיטיבי מודולו n אזי $|\{g \in [n-1] \mid \langle g \bmod n \rangle = (\mathbb{Z}/n\mathbb{Z})^\times\}| = \varphi(\varphi(n))$.

למה: יהי $p \in \mathbb{P}$ אזי $|\{g \in [p-1] \mid \langle g \bmod p \rangle = (\mathbb{Z}/p\mathbb{Z})^\times\}| = \varphi(p-1)$.

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

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

טענה: יהי $n \in \mathbb{N}_{\geq 2}$ באשר $(n-1)! \equiv -1 \pmod{n}$ אזי $n \in \mathbb{P}$.

למה: יהי $n \in \mathbb{N}$ תהא G חבורה ציקלית מסדר n ויהי $g \in G$ אזי $(g \text{ יוצר של } G) \iff (q|n \text{ באשר } q \in \mathbb{P} \text{ מתקיים } g^{\frac{n}{q}} \neq 1)$.

למה: יהי $p \in \mathbb{P}$ ויהי $m \in [p-1]$ אזי $p \mid \binom{p}{m}$.

למה: יהי $p \in \mathbb{P}_{>2}$ ראשוני ויהי $k \in \mathbb{N}_{\geq 2}$ ויהי $a \in \mathbb{Z}$ אזי $(1+ap)^{p^{k-2}} \equiv 1 + ap^{k-1} \pmod{p^k}$.

טענה: יהי $p \in \mathbb{P}_{>2}$ ראשוני ויהי $k \in \mathbb{N}_+$ אזי $(\mathbb{Z}/p^k\mathbb{Z})^\times \simeq C_{p^{k-1}(p-1)}$.

מסקנה: יהי $p \in \mathbb{P}_{>2}$ ראשוני ויהי $k \in \mathbb{N}_+$ אזי $(\mathbb{Z}/p^k\mathbb{Z})^\times$ ציקלית.

טענה: יהי $k \in \mathbb{N}_{\geq 2}$ ויהי $a \in \mathbb{Z}_{\text{odd}}$ אזי קיימים ויחידים $\alpha \in \{0, 1\}$ וכן $\beta \in \{0, \dots, 2^{k-2}\}$ עבורם $a \equiv (-1)^\alpha 5^\beta \pmod{2^k}$.

מסקנה: יהי $k \in \mathbb{N}_{\geq 2}$ ויהי $a \in \mathbb{Z}_{\text{odd}}$ אזי $(\mathbb{Z}/2^k\mathbb{Z})^\times \simeq C_2 \times C_{2^{k-2}}$.

משפט: יהי $n \in \mathbb{N}_+$ יהיו $k, m \in \mathbb{N}$ יהיו $e_1, \dots, e_m \in \mathbb{N}_+$ ויהיו $p_1 \dots p_m \in \mathbb{P}$ שונים באשר $n = 2^k \cdot \prod_{i=1}^m p_i^{e_i}$ אזי

• אם $k \leq 1$ אז $(\mathbb{Z}/n\mathbb{Z})^\times \simeq \prod_{i=1}^m C_{p_i^{e_i-1}(p_i-1)}$.

• אם $k \geq 2$ אז $(\mathbb{Z}/n\mathbb{Z})^\times \simeq C_2 \times C_{2^{k-2}} \times \prod_{i=1}^m C_{p_i^{e_i-1}(p_i-1)}$.

מסקנה: יהי $n \in \mathbb{N}_+$ אזי $(\mathbb{Z}/n\mathbb{Z})^\times$ ציקלית $\iff (n \in \{2, 4\}) \vee (n \in \mathbb{P}_{>2} \text{ וקיים } p \in \mathbb{P}_{>2} \text{ וקיים } k \in \mathbb{N}_+ \text{ עבורו } n \in \{p^k, 2p^k\})$.

טענה: יהי $p \in \mathbb{P}_{>2}$ ויהי a שורש פרימיטיבי מודולו p אזי

• אם $a^{p-1} \not\equiv 1 \pmod{p^2}$ אז לכל $k \in \mathbb{N}_+$ מתקיים כי a פרימיטיבי מודולו p^k .

• אם $a^{p-1} \equiv 1 \pmod{p^2}$ אז לכל $k \in \mathbb{N}_+$ מתקיים כי $a+p$ פרימיטיבי מודולו p^k .

שארית ריבועית: יהי $p \in \mathbb{P}$ אזי $a \in \mathbb{Z}$ המקיים $a \not\equiv 0 \pmod{p}$ וכן קיים $x \in \mathbb{Z}$ עבורו $x^2 \equiv a \pmod{p}$.

סימון: יהי $p \in \mathbb{P}$ אזי $\text{QR}_p = \{a \in \mathbb{Z} \mid a \text{ שארית ריבועית מודולו } p\}$.

אי-שארית ריבועית: יהי $p \in \mathbb{P}$ אזי $a \in \mathbb{Z}$ המקיים $a \not\equiv 0 \pmod{p}$ וכן a אינו שארית ריבועית מודולו p .

סימון: יהי $p \in \mathbb{P}$ אזי $\text{QNR}_p = \{a \in \mathbb{Z} \mid a \text{ אי-שארית ריבועית מודולו } p\}$.

טענה: יהי $p \in \mathbb{P}_{>2}$ יהי g שורש פרימיטיבי מודולו p ויהיו $a, r \in \mathbb{Z}$ באשר $a \not\equiv 0 \pmod{p}$ וכן $a \equiv g^r \pmod{p}$ אזי $(r \in \mathbb{Z}_{\text{even}}) \iff (a \in \text{QR}_p)$.

מסקנה: יהי $p \in \mathbb{P}_{>2}$ אזי $|\text{QR}_p| = |\text{QNR}_p| = \frac{p-1}{2}$.

סמל לזנדר: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in \text{QR}_p \\ -1 & a \in \text{QNR}_p \\ 0 & p|a \end{cases}$.

טענה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

מסקנה: יהי $p \in \mathbb{P}_{>2}$ ויהיו $a, b \in \mathbb{Z}$ אזי $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$.

מסקנה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{-1}{p}\right) = \begin{cases} 1 & p \equiv 1 \pmod{4} \\ -1 & p \equiv 3 \pmod{4} \end{cases}$.

הגדרה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a \bmod p}{p}\right) = \left(\frac{a}{p}\right)$.

מסקנה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}/p\mathbb{Z}$ אזי $\left| \text{sols} \left(x^2 = a \right) \right| = 1 + \left(\frac{a}{p} \right)$

למה גאוס: יהי $p \in \mathbb{P}_{>2}$ תהא $S \subseteq (\mathbb{Z}/p\mathbb{Z})^\times$ באשר $S \cap (-S) = \emptyset$ וכן $S \cup (-S) = (\mathbb{Z}/p\mathbb{Z})^\times$ ויהי $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ אזי $\left(\frac{a}{p} \right) = (-1)^{|a \cap (-S)|}$

מסקנה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{2}{p} \right) = (-1)^{\frac{p^2-1}{8}}$

טענה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{2}{p} \right) = \begin{cases} 1 & p \bmod 8 \in \{1,7\} \\ -1 & p \bmod 8 \in \{3,5\} \end{cases}$

טענה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{3}{p} \right) = \begin{cases} 1 & p \bmod 12 \in \{1,11\} \\ -1 & p \bmod 12 \in \{5,7\} \end{cases}$

למה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{N}_+$ באשר $p \nmid a$ אזי $\left(\frac{a}{p} \right) = (-1)^{\sum_{i=1}^{\lfloor \frac{p}{2} \rfloor} \left(\lfloor \frac{ip}{a} \rfloor - \lfloor \frac{(2i-1)p}{2a} \rfloor \right)}$

למה: יהי $a \in \mathbb{N}_+$ ויהיו $p, q \in \mathbb{P}_{>2}$ באשר $p \equiv \pm q \bmod 4a$ אזי $\left(\frac{a}{p} \right) = \left(\frac{a}{q} \right)$

משפט חוק ההדדיות הריבועית: יהיו $p, q \in \mathbb{P}_{>2}$ אזי $\left(\frac{p}{q} \right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \cdot \left(\frac{q}{p} \right)$