

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 האי־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 $S \neq \emptyset$ 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 $1|a$ 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 $a|c$ אזי $a|b$.

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 $\lfloor x \rfloor = \max((-\infty, x] \cap \mathbb{Z})$.

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 $d|\gcd(a_1 \dots a_n)$.

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 $d \in \{0, \dots, b-1\}^k$ וכך $d_k > 0$ ואז $n = \sum_{i=1}^k d_i b^i$.

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

טענה: קיים אלגוריתם 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 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 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 $a_1 \dots a_n, m \in \mathbb{Z}$ כאשר $a_i | m$ 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 $a, b \in \mathbb{Z}$ כאשר $a \neq 0$ 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 $p \mid ab$ אזי $(p \mid a) \vee (p \mid b)$.

טענה: יהי $n \in \mathbb{N}$ עבורו לכל $a, b \in \mathbb{Z}$ אם $n \mid ab$ אז $(n \mid a) \vee (n \mid b)$ אזי $(n \mid a) \vee (n \mid b)$ $n \in \{0, \pm 1\} \cup (\pm \mathbb{P})$.

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 $p \mid a_i$.

למה: יהי $n \in \mathbb{N}_{\geq 2}$ אזי קיים $p \in \mathbb{P}$ המקיים $p \mid n$.

אלגוריתם הנפה של ארטוסתנס: ...

טענה: יהי $N \in \mathbb{N}$ אזי אלגוריתם ארטוסתנס מחשב את הראשוניים עד N בסיבוכיות $\mathcal{O}\left(\left(\sum_{p \in \mathbb{P}_{\leq N}} \frac{1}{p}\right) \cdot N\right)$.

טענה אטקין-ברנסטיין: קיים אלגוריתם $\mathcal{O}(N)$ שעושה אותו דבר. ...

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 $e_p(n) = \max\{m \in \mathbb{N} \mid (p^m \mid n)\}$.

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

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 $(m \mid n) \iff (\forall p \in \mathbb{P}. e_p(m) \leq e_p(n))$.

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 $(m, n) \iff (n \mid m)$ (לא קיים $p \in \mathbb{P}$ המקיים $p \mid m$ וכן $p \mid n$).