

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

טענה: תהא  $S \subseteq \mathbb{R}$  המקיימת את האי־שיויון 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  $a|b$ .

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  $d \in \{0, \dots, b-1\}^k$  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  $\text{len}((n)_2)$ .

**טענה:** קיים אלגוריתם  $A$  עבורו לכל  $a, b \in \mathbb{N}$  מתקיים  $A(a, b) = a + b$  וכן  $A$  רץ בסיבוכיות  $\mathcal{O}(n)$ .

**טענה:** קיים אלגוריתם  $A$  עבורו לכל  $a, b \in \mathbb{N}$  מתקיים  $A(a, b) = ab$  וכן  $A$  רץ בסיבוכיות  $\mathcal{O}(n^2)$ .

**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  $A$  עבורו לכל  $a, b \in \mathbb{N}$  מתקיים  $A(a, b) = ab$  וכן  $A$  רץ בסיבוכיות  $\mathcal{O}(n \log(n) \log \log(n))$ .

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

**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  $\text{EuclidGCD}(a, b) = \text{gcd}(a, b)$ .

**טענה:** יהיו  $a, b \in \mathbb{Z}$  אזי סיבוכיות הריצה של EuclidGCD הוא לכל היותר  $2 \log_2(\min\{|a|, |b|\})$ .