

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 $1|a$ 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 $d|\gcd(a_1 \dots a_n)$.

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

Algorithm 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: סיבוכיות הריצה של KaratsubaMult הינה $\mathcal{O}(n^{\log_2(3)})$

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

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

Algorithm 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: 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

Algorithm 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) זרים \iff (לא קיים $p \in \mathbb{P}$ המקיים $p|m$ וכן $p|n$).

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 $2p+1 \in \mathbb{P}$.

טענה: $|\mathbb{P} \cap (4\mathbb{N}+3)| = \aleph_0$.

טענה: $|\mathbb{P} \cap (4\mathbb{N}+1)| = \aleph_0$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

אלגוריתם הופכי בחבורת שאריות החלוקה: יהי $n \in \mathbb{N}_+$ ויהי $a \in \mathbb{Z}$ באשר $(a, n) = 1$ ואי

Algorithm InverseMod(n, a):

```

     $(b, c) \leftarrow \text{ExtendedEuclidGCD}(a, n)$  //  $ba + cn = \text{gcd}(a, n)$ 
     $(q, r) \leftarrow \text{RemainderDiv}(b, n)$ 
    return  $r$ 

```

טענה: יהי $n \in \mathbb{N}_+$ ויהי $a \in \mathbb{Z}$ באשר $(a, n) = 1$ ואי $\text{InverseMod}(n, a) = (a \bmod n)^{-1}$.

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

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 $e_1 \dots e_k \in \mathbb{N}_+$ ואי $\varphi\left(\prod_{i=1}^k p_i^{e_i}\right) = \prod_{i=1}^k (p_i^{e_i} - p_i^{e_i-1})$.

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

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

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

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

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

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

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

הגדרה: יהי $n \in \mathbb{N}_+$ ואי נגדיר $\mathbb{1}^n \in \mathbb{N}^n$ כך $\mathbb{1}^n_i = 1$ לכל $i \in [n]$.

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

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

• לכל $y \in \mathbb{Z}$ המקיים $\mathbb{1}^n y \equiv a \bmod m$ מתקיים $y = \mathbb{1}^n x + k \prod_{i=1}^n m_i$ $\mathbb{1}^n x \equiv a \bmod m$.

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

Algorithm ModEquationSys($m_1 \dots m_n, a_1 \dots a_n$):

```

for  $i \in [n]$  do
     $M_i \leftarrow \prod_{j \in [n] \setminus \{i\}} m_j$ 
     $N_i \leftarrow \text{InverseMod}(m_i, M_i)$ 
end
return  $\sum_{i=1}^n a_i M_i N_i$ 

```

טענה: יהיו $m_1 \dots m_n \in \mathbb{N}_+$ זרים בזוגות ויהיו $a_1 \dots a_n \in \mathbb{Z}$ אזי $a \equiv a_1 \dots a_n \pmod{m}$ $\mathbb{1}^n \cdot \text{ModEquationSys} \equiv a \pmod{m}$

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 $x \equiv a \pmod{m}$) $\iff (1^n x \equiv a \pmod{m})$ (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 $\sum_{\substack{k \in [n] \\ \gcd(k, n) = 1}} k = \frac{1}{2} n \cdot \varphi(n)$

פונקציה כפלית: פונקציה $f: \mathbb{N} \rightarrow \mathbb{R}$ עברה לכל $n, m \in \mathbb{N}$ באשר $(n, m) = 1$ מתקיים $f(nm) = f(n)f(m)$ **טענה:** φ פונקציה כפלית.

טענה: תהא $f: \mathbb{N} \rightarrow \mathbb{R}$ כפלית באשר $f \neq 0$ אזי $f(1) = 1$

טענה: תהייה $f, g: \mathbb{N} \rightarrow \mathbb{R}$ כפוליות באשר לכל $p \in \mathbb{P}$ ולכל $k \in \mathbb{N}$ מתקיים $f(p^k) = g(p^k)$ אזי $f = g$

טענה: יהי $k \in \mathbb{N}_+$ נגדיר $f: \mathbb{N} \rightarrow \mathbb{R}$ כך $f(n) = \gcd(n, k)$ אזי f כפלית.

טענה: תהא $f: \mathbb{N} \rightarrow \mathbb{R}$ כפלית אזי $F: \mathbb{N} \rightarrow \mathbb{R}$ המוגדרת $F(n) = \sum_{d|n} f(d)$ הינה כפלית.

פונקציית סכום המחלקים: נגדיר $\sigma: \mathbb{N} \rightarrow \mathbb{N}$ כך $\sigma(n) = \sum_{d|n} d$

מספר מושלם: מספר $n \in \mathbb{N}$ המקיים $\sigma(n) = 2n$

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

טענה: יהיו $n, d \in \mathbb{N}_+$ תהא G חבורה ציקלית מסדר n והי $g \in G$ 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 מסדר n אזי $(G \text{ ציקלית}) \iff (|G| \mid d \text{ מתקיים } |\{a \in \mathbb{Z}_n \mid a^d = 1\}| \leq d)$

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 $\langle g \pmod{n} \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$

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

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

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

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

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 מסדר n והי $g \in G$ 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 $p \in \mathbb{P}$ והי $m \in [p-1]$ אזי $p \mid \binom{p}{m}$

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

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

מסקנה: יהי $p \in \mathbb{P}_{>2}$ ראשוני והי $k \in \mathbb{N}_+$ 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 $n = 2^k \cdot \prod_{i=1}^m p_i^{e_i}$

• 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 $n \in \mathbb{N}$ אזי $a \in \mathbb{Z}$ המקיים $a \not\equiv n$ וכן קיים $x \in \mathbb{Z}$ עבורו $x^2 \equiv a \pmod{n}$

סימון: יהי $n \in \mathbb{N}$ אזי $\text{QR}_n = \{a \in \mathbb{Z} \mid a \text{ שארית ריבועית מודולו } n\}$

אי־שארית ריבועית: יהי $n \in \mathbb{N}$ אזי $a \in \mathbb{Z}$ המקיים $a \not\equiv n$ וכן a אינו שארית ריבועית מודולו n .

סימון: יהי $n \in \mathbb{P}$ אזי a אי־שארית ריבועית מודולו n $\text{QNR}_n = \{a \in \mathbb{Z} \mid a \text{ אי־שארית ריבועית מודולו } n\}$

טענה: יהי $p \in \mathbb{P}_{>2}$ יהי g שורש פרימיטיבי מודולו p ויהיו $a, r \in \mathbb{Z}$ באשר $a, r \in \mathbb{Z}$ 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 לז'נדר: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \in \text{QR}_p \\ -1 & a \in \text{QNR}_p \\ 0 & p \mid a \end{cases}$

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 $\left(\frac{a \pmod{p}}{p}\right) = \left(\frac{a}{p}\right)$

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

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

$\left(\frac{a}{p}\right) = (-1)^{|aS \cap (-S)|}$

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 $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \pmod{8} \in \{1, 7\} \\ -1 & p \pmod{8} \in \{3, 5\} \end{cases}$

טענה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{3}{p}\right) = \begin{cases} 0 & p=3 \\ 1 & p \pmod{12} \in \{1, 11\} \\ -1 & p \pmod{12} \in \{5, 7\} \end{cases}$

למה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{N}_+$ באשר $a \not\equiv p$ אזי $\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\lfloor \frac{a}{2} \rfloor} (\lfloor \frac{ip}{a} \rfloor - \lfloor \frac{(2i-1)p}{2a} \rfloor)}$

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

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

מסקנה: יהיו $p, q \in \mathbb{P}_{>2}$ אזי $\left(\frac{p}{q}\right) = \left(\frac{-q}{p}\right)$

מסקנה: יהי $p \in \mathbb{P}_{>2}$ אזי $\left(\frac{5}{p}\right) = \begin{cases} 0 & p=5 \\ 1 & p \pmod{5} \in \{1, 4\} \\ -1 & p \pmod{5} \in \{2, 3\} \end{cases}$

מספר חסר ריבועים: מספר $N \in \mathbb{Z}$ עבורו לכל $p \in \mathbb{P}$ מתקיים $p^2 \nmid N$

טענה: יהי $k \in \mathbb{N}_+$ ויהיו $p_1 \dots p_k \in \mathbb{P}_{>2}$ שונים אזי $|\text{QR}_{\prod_{i=1}^k p_i}| = \frac{1}{2^k} \varphi\left(\prod_{i=1}^k p_i\right)$

סמל יעקובי: יהי $k \in \mathbb{N}$ יהיו $p_1 \dots p_k \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a}{\prod_{i=1}^k p_i}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)$

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהיו $m, k \in \mathbb{Z}$ באשר $m, k \equiv k \pmod{n}$ אזי $\left(\frac{m}{n}\right) = \left(\frac{k}{n}\right)$

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהי $m \in \mathbb{Z}$ אזי $\left(\frac{m}{n}\right) = 0 \iff ((m, n) > 1)$

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהיו $a, b \in \mathbb{Z}$ אזי $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$

טענה: יהיו $n, m \in \mathbb{N}_{\text{odd}}$ ויהי $a \in \mathbb{Z}$ אזי $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{a}{m}\right)$

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהי $m \in \mathbb{Z}$ עבורו $(m, n) = 1$ וכן קיים $a \in \mathbb{Z}$ המקיים $m \equiv a^2 \pmod n$ אזי $\left(\frac{m}{n}\right) = 1$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהי $m \in \mathbb{Z}$ באשר $(m, n) = 1$ אזי קיים $a \in \mathbb{Z}$ עבורו $m \equiv a^2 \pmod n$ \iff (לכל $p \mid n$ המקיים $p \in \mathbb{P}$) מתקיים $\left(\frac{m}{p}\right) = 1$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ אזי $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

מסקנה: יהי $n \in \mathbb{N}_{\text{odd}}$ אזי $\left(\frac{-1}{n}\right) = \begin{cases} 1 & n \equiv 1 \pmod 4 \\ -1 & n \equiv 3 \pmod 4 \end{cases}$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ אזי $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

מסקנה: יהי $n \in \mathbb{N}_{\text{odd}}$ אזי $\left(\frac{2}{n}\right) = \begin{cases} 1 & n \pmod 8 \in \{1, 7\} \\ -1 & n \pmod 8 \in \{3, 5\} \end{cases}$.

טענה חוק ההדדיות: יהיו $n, m \in \mathbb{N}_{\text{odd}}$ אזי $\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \cdot \left(\frac{n}{m}\right)$.

אלגוריתם לחישוב סמל יעקובי: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהי $m \in \mathbb{Z}$ אזי

Algorithm JacobiSymbol(m, n):

```

if  $m = 0$  then return 0
if  $n = 1$  then return 1
if  $m < 0$  then return  $(-1)^{\frac{n-1}{2}} \cdot \text{JacobiSymbol}(-m, n)$ 
if  $m \in \mathbb{N}_{\text{even}}$  then return  $(-1)^{\frac{n^2-1}{8} \cdot e_2(m)} \cdot \text{JacobiSymbol}(\frac{m}{2^{e_2(m)}}, n)$ 
if  $m < n$  then return  $(-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} \cdot \text{JacobiSymbol}(n, m)$ 
 $(q, r) \leftarrow \text{RemainderDiv}(m, n)$ 
return JacobiSymbol( $r, n$ )

```

טענה: יהי $n \in \mathbb{N}_{\text{odd}}$ ויהי $m \in \mathbb{Z}$ אזי $\text{JacobiSymbol}(m, n) = \left(\frac{m}{n}\right)$.

טענה: סיבוכיות הריצה של JacobiSymbol הינה $\mathcal{O}(n^3)$.

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

טענה: יהי $p \in \mathbb{P}_{>2}$ ויהי $a \in \mathbb{Z}$ באשר $p \nmid a$ אזי קיימים $x, y \in \mathbb{Z}$ זרים עבורם $p \mid x^2 + ay^2 \iff \left(\frac{-a}{p}\right) = 1$.

טענה: $|\mathbb{P} \cap (3\mathbb{N} + 1)| = \aleph_0$.

מספר ריבוע שלם: מספר $n \in \mathbb{Z}$ עבורו קיים $m \in \mathbb{Z}$ המקיים $n = m^2$.

סימון: יהי $n \in \mathbb{Z}$ ריבוע שלם אזי $n = \square$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}} \setminus \{1\}$ באשר $n = \square$ ויהי $a \in \mathbb{Z}$ באשר $(a, n) = 1$ אזי $\left(\frac{a}{n}\right) = 1$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}} \setminus \{1\}$ באשר $n \neq \square$ אזי קיים $a \in \mathbb{Z}$ עבורו $\left(\frac{a}{n}\right) = -1$.

טענה: יהי $n \in \mathbb{N}_{\text{odd}} \setminus \{1\}$ באשר $n \neq \square$ אזי $\frac{1}{2}\varphi(n) = \left| \left\{ x \in (\mathbb{Z}/n\mathbb{Z})^\times \mid \left(\frac{x}{n}\right) = 1 \right\} \right|$.

טענה: $|\mathbb{P} \cap (5\mathbb{N} - 1)| = \aleph_0$.

אלגוריתם חזקה מודולורית: אלגוריתם \mathcal{A} עבורו לכל $N, m \in \mathbb{N}_+$ ולכל $a, m \in [N-1]$ מתקיים $\mathcal{A}(N, a, m) = (a^m \pmod N)$.

אלגוריתם כפל איטרטיבי: יהי \mathcal{A} אלגוריתם כפל מספרים יהי $N \in \mathbb{N}$ יהיו $m_0 \dots m_k \in \{0, 1\}$ ויהי $a \in \mathbb{Z}/N\mathbb{Z}$ אזי

Algorithm ModIteratedSquaring[\mathcal{A}](N, a, m):

```

 $a_0 \leftarrow a$ 
 $r \leftarrow a_0^{m_0}$ 
for  $i \in [1, \dots, k]$  do
     $a_i \leftarrow \mathcal{A}(a_{i-1}, a_{i-1}) \pmod N$ 
    if  $m_i = 1$  then  $r \leftarrow \mathcal{A}(r, a_i^{m_i}) \pmod N$ 
end

```

טענה: יהי \mathcal{A} אלגוריתם כפל מספרים יהיו $N, m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}/N\mathbb{Z}$ אזי $\text{ModIteratedSquaring}[\mathcal{A}](N, a, (m)_2) = (a^m \pmod N)$.

טענה: יהי \mathcal{A} אלגוריתם כפל מספרים ויהיו $N, m \in \mathbb{N}$ אזי סיבוכיות הריצה של ModIteratedSquaring הינה

$\mathcal{O}(\log(m) \cdot \text{Time}(\mathcal{A})(\log_2(N)))$.

מסקנה: יהיו $N, m \in \mathbb{N}$ אזי סיבוכיות הריצה של ModIteratedSquaring[NaiveMul] הינה $\mathcal{O}(\log(m) \cdot \log^2(N))$.

מסקנה: יהיו $N, m \in \mathbb{N}$ אזי סיבוכיות הריצה של ModIteratedSquaring[CooleyTukeyMul] הינה

$\mathcal{O}(\log(m) \cdot \log(N) \log \log(N) \log \log \log(N))$.

אלגוריתם חלוקה ניסיונית: יהי $N \in \mathbb{N}_+$ אזי

Algorithm TrialDivision(N):

```

for  $i \in [1, \dots, \sqrt{N}]$  do
     $(q, r) \leftarrow \text{RemainderDiv}(N, i)$ 
    if  $r = 0$  then return False
end
return True

```

טענה: יהי $N \in \mathbb{N}_+$ אזי $(N \in \mathbb{P}) \iff (\text{TrialDivision}(N) = \text{True})$.

טענה: סיבוכיות הריצה של TrialDivision הינה $\mathcal{O}(2^{\frac{N}{2}})$.

אלגוריתם מבחן פרמה: יהי \mathcal{A} אלגוריתם חזקה מודולרית יהי $N \in \mathbb{N}_+$ ויהי $a \in [N-1]$ אזי

Algorithm FermatPrimalityTest[\mathcal{A}]($N; a$):

```

if  $\mathcal{A}(N, a, N-1) = 1$  then return True
return False

```

טענה: סיבוכיות הריצה של $\text{FermatPrimalityTest}[\text{ModIteratedSquaring}[\text{NaiveMul}]]$ הינה $\mathcal{O}(n^3)$.

טענה: סיבוכיות הריצה של $\text{FermatPrimalityTest}[\text{ModIteratedSquaring}[\text{CooleyTukeyMul}]]$ הינה $\mathcal{O}(n^2 \log(n) \log \log(n))$.

טענה: יהי $N \in \mathbb{P}$ אזי $\mathbb{P}_{a \leftarrow [N-1]}(\text{FermatPrimalityTest}(N; a) = \text{True}) = 1$.

מספר קרמייקל: מספר פריק $N \in \mathbb{N}_+$ עבורו לכל $a \in \mathbb{Z}$ המקיים $(a, N) = 1$ מתקיים $a^{N-1} \equiv 1 \pmod{N}$.

טענה: יהי $N \in \mathbb{N}_+$ פריק באשר N אינו מספר קרמייקל אזי $\mathbb{P}_{a \leftarrow [N-1]}(\text{FermatPrimalityTest}(N; a) = \text{False}) > \frac{1}{2}$.

טענה: יהי $k \in \mathbb{N}$ אזי $\text{FermatPrimalityTest}(F_k; 2) = \text{True}$.

השערה: לא קיים $k \in \mathbb{N}_{>5}$ עבורו $F_k \in \mathbb{P}$. השערה פתוחה

השערה: $|\{k \in \mathbb{N} \mid F_k \notin \mathbb{P}\}| = \aleph_0$. השערה פתוחה

טענה: יהי $N \in \mathbb{N}$ אזי $(N \text{ קרמייקל}) \iff (N \text{ פריק חסר ריבועים וכן לכל } p \in \mathbb{P} \text{ המקיים } p|N \text{ מתקיים } p-1|N-1)$.

מסקנה: יהי $k \in \mathbb{N}$ עבורו $6k+1, 12k+1, 18k+1 \in \mathbb{P}$ אזי $6k+1, 12k+1, 18k+1$ מספר קרמייקל.

השערה: $|\{k \in \mathbb{N} \mid 6k+1, 12k+1, 18k+1 \in \mathbb{P}\}| = \aleph_0$. השערה פתוחה

משפט אלפורד-גרנוויל-פומרנץ: $|\{N \in \mathbb{N}_+ \mid N \text{ מספר קרמייקל}\}| = \aleph_0$. לא הוכח בקורס

משפט אלפורד-גרנוויל-פומרנץ: החל ממקום מסוים לכל $x \in \mathbb{N}$ מתקיים $x^{\frac{2}{3}} > |\{N < x \mid N \text{ מספר קרמייקל}\}|$. לא הוכח בקורס

משפט ארדוש: קיים $c > 0$ עבורו החל ממקום מסוים לכל $x \in \mathbb{N}$ מתקיים

$$|\{N < x \mid N \text{ מספר קרמייקל}\}| < x \cdot \exp\left(\frac{-c \cdot \log(x) \cdot \log \log \log(x)}{\log \log(x)}\right)$$

לא הוכח בקורס

אלגוריתם מבחן סולובאי-סטרסן: יהי \mathcal{A} אלגוריתם חזקה מודולרית יהי $N \in \mathbb{N}_+$ ויהי $a \in [N-1]$ אזי

Algorithm SolovayStrassenPrimalityTest[\mathcal{A}]($N; a$):

```

if  $N = 2$  then return True
if  $(N < 2) \vee (2|N)$  then return False
 $s \leftarrow \text{JacobiSymbol}(a, N)$ 
if  $(s \neq 0) \wedge (\mathcal{A}(N, a, \frac{N-1}{2}) = (s \pmod{N}))$  then
    return True
return False

```

טענה: סיבוכיות הריצה של $\text{SolovayStrassenPrimalityTest}[\text{ModIteratedSquaring}[\text{NaiveMul}]]$ הינה $\mathcal{O}(n^3)$.

טענה: יהי $N \in \mathbb{N}_+$ ויהי $a \in [N-1]$ המקיים $\text{SolovayStrassenPrimalityTest}(N; a) = \text{True}$ אזי $\text{FermatPrimalityTest}(N; a) = \text{True}$.

טענה: יהי $N \in \mathbb{P}$ אזי $\mathbb{P}_{a \leftarrow [N-1]}(\text{SolovayStrassenPrimalityTest}(N; a) = \text{True}) = 1$.

טענה: יהי $N \in \mathbb{N}_+$ פריק אזי $\mathbb{P}_{a \leftarrow [N-1]}(\text{SolovayStrassenPrimalityTest}(N; a) = \text{False}) > \frac{1}{2}$.

אלגוריתם מבחן מילר-רבין: יהי \mathcal{A} אלגוריתם חזקה מודולרית יהי $N \in \mathbb{N}_+$ ויהי $a \in \mathbb{N}_{<N}$ אזי

טענה: סיבוכיות הריצה של $\text{MillerRabinPrimalityTest}[\text{ModIteratedSquaring}[\text{NaiveMul}]]$ הינה $\mathcal{O}(n^3)$.

טענה: יהי $N \in \mathbb{P}$ אזי $\mathbb{P}_{a \leftarrow \mathbb{N}_{<N}}(\text{MillerRabinPrimalityTest}(N; a) = \text{True}) = 1$.

משפט רבין: יהי $N \in \mathbb{N}$ פריק אזי $|\{a \in \mathbb{N}_{<N} \mid \text{MillerRabinPrimalityTest}(N; a) = \text{True}\}| \leq \frac{\varphi(N)}{4}$.

Algorithm MillerRabinPrimalityTest $[\mathcal{A}](N; a)$:

```

if  $N = 2$  then return True
if  $(N < 2) \vee (2 \mid N)$  then return False
 $\alpha_0 \leftarrow \mathcal{A}(N, a, \frac{N-1}{2^{e_2(N-1)}})$ 
for  $i \in [1, \dots, e_2(N-1)]$  do
     $\alpha_i \leftarrow \mathcal{A}(N, \alpha_{i-1}, 2)$ 
    if  $\alpha_i = -1$  then return True
    if  $\alpha_i \neq 1$  then return False
end
return True

```

מסקנה: יהי $N \in \mathbb{N}$ פריק אזי $\mathbb{P}_{a \leftarrow \mathbb{N}_{<N}}(\text{MillerRabinPrimalityTest}(N; a) = \text{False}) > \frac{3}{4}$.

טענה: יהי $k \in \mathbb{N}_{\text{odd}}$ באשר $2k+1, 4k+1 \in \mathbb{P}$

$$\cdot \left| \left\{ a \in \mathbb{N}_{<(2k+1) \cdot (4k+1)} \mid \text{MillerRabinPrimalityTest}((2k+1) \cdot (4k+1); a) = \text{True} \right\} \right| = \frac{\varphi((2k+1) \cdot (4k+1))}{4}$$

טענה: יהי $N \in \mathbb{N}_+$ ויהי $a \in [N-1]$ המקיים $\text{MillerRabinPrimalityTest}(N; a) = \text{True}$

$$\text{SolovayStrassenPrimalityTest}(N; a) = \text{True}$$

אלגוריתם לייצור מספרים ראשוניים: יהי \mathcal{A} אלגוריתם חזקה מודולרית יהיו $n, k \in \mathbb{N}_+$ ותהא $r : \mathbb{N} \rightarrow \{2^{n-1}, \dots, 2^n\} \times \mathbb{N}^k$ באשר

$$(r(c))_i < (r(c))_1 \text{ לכל } c \in \mathbb{N} \text{ ולכל } i \in \{2, \dots, k+1\} \text{ אזי}$$

Algorithm PrimeGenerator $[\mathcal{A}](n, k; r)$:

```

 $c \leftarrow 0$ 
while True do
     $b \leftarrow \text{True}$ 
    for  $i \in [2, \dots, k+1]$  do
         $b \leftarrow b \wedge \text{MillerRabinPrimalityTest}[\mathcal{A}]((r(c))_1; (r(c))_i)$ 
    end
    if  $b = \text{True}$  then return  $(r(c))_1$ 
     $c \leftarrow c + 1$ 
end

```

טענה: יהיו $n, k \in \mathbb{N}_+$ ויהי r עבורו $\text{PrimeGenerator}(n, k; r) < 2^n$ אזי $2^{n-1} < \text{PrimeGenerator}(n, k; r)$

טענה: יהיו $n, k \in \mathbb{N}_+$ אזי $\mathbb{E}_r[\text{Time}(\text{PrimeGenerator}[\text{ModIteratedSquaring}[\text{NaiveMul}]](n, k; r))] = \mathcal{O}(kn^4)$

טענה: יהיו $n, k \in \mathbb{N}_+$ אזי $\mathbb{P}_r(\text{PrimeGenerator}(n, k; r) \in \mathbb{P}) \geq 1 - \frac{1}{4^k}$

טענה: יהיו $p, q \in \mathbb{P}$ באשר $q \mid 2^p - 1$ אזי $q \equiv 1 \pmod{p}$

טענה אויילר: יהיו $p, q \in \mathbb{P}_{>3}$ באשר $p \equiv 3 \pmod{4}$ וכן $q = 2p + 1$ אזי $2^p - 1$ פריק.

מספר מרסן: יהי $n \in \mathbb{N}$ אזי $M_n = 2^n - 1$

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 $p = 2^q - 1$

מסקנה: יהי $p \in \mathbb{P}$ ראשוני מרסן אזי p הינו מספר מרסן.

טענה: יהי $n \in \mathbb{N}$ באשר M_n ראשוני אזי $(2^n - 1) \cdot 2^{n-1}$ מושלם.

אלגוריתם לוקס-להמר: יהי \mathcal{A} אלגוריתם בדיקת ראשוניות יהי \mathcal{B} אלגוריתם חזקה מודולרית ויהי $n \in \mathbb{N}$ אזי

Algorithm LucasLehmer $[\mathcal{A}, \mathcal{B}] (n, 2^n - 1)$:

```

if  $\mathcal{A}(n) = \text{False}$  then return False
 $S_0 \leftarrow 4$ 
for  $i \in [1, \dots, n-2]$  do
   $S_i \leftarrow (\mathcal{B}(2^n - 1, S_{i-1}, 2) - 2) \bmod p$ 
end
if  $S_{n-2} = 0$  then return True
return False

```

משפט: יהי $n \in \mathbb{N}$ אזי $(\text{LucasLehmer}(n, 2^n - 1) = \text{True}) \iff (2^n - 1 \in \mathbb{P})$.

טענה: סיבוכיות הריצה של $\text{LucasLehmer}[\text{TrialDivision}, \text{ModIteratedSquaring}[\text{NaiveMul}]]$ הינה $\mathcal{O}(n^3)$.

טענה: סיבוכיות הריצה של $\text{LucasLehmer}[\text{TrialDivision}, \text{ModIteratedSquaring}[\text{CooleyTukeyMul}]]$ הינה $\mathcal{O}(n^2 \log(n) \log \log(n))$.

טענה: $2^{136276841} - 1 \in \mathbb{P}$.

הגדרה: יהי $\alpha \in \mathbb{R}_+$ אזי $\tilde{\mathcal{O}}(n^\alpha) = \mathcal{O}(n^\alpha) \cdot \text{poly}(\log(n))$.

משפט אגרוול-קאל-סקסנה: קיים אלגוריתם דטרמיניסטי AKS לבדיקת ראשוניות בעל סיבוכיות ריצה $\tilde{\mathcal{O}}(n^6)$.

הצפנה סימטרית: יהי $n \in \mathbb{N}$ ותהייה $E, D : \mathbb{F}_2^n \times \mathbb{F}_2^n \rightarrow \mathbb{F}_2^n$ באשר $E(p, k), D(p, k) = p$ לכל $p, k \in \mathbb{F}_2^n$ אזי (E, D) .

הצפנה אסימטרית: יהיו $n, m \in \mathbb{N}$ יהיו $k_e, k_d \in \mathbb{F}_2^m$ ותהייה $E, D : \mathbb{F}_2^n \times \mathbb{F}_2^m \rightarrow \mathbb{F}_2^n$ באשר $E(p, k_e), D(p, k_d) = p$ לכל $p \in \mathbb{F}_2^n$ אזי (E, D, k_e, k_d) .

בעיית הפירוק: יהי $N \in \mathbb{N}_+$ אזי $\text{IFP}(N) = (p_1, \dots, p_k)$ באשר $\prod_{i=1}^k p_i = N$ וכן $p_i \in \mathbb{P}$ לכל $i \in [k]$.

טענה נפת שדות המספרים: קיים $c > 0$ עבורו קיים אלגוריתם \mathcal{A} לבעיית הפירוק בעל סיבוכיות ריצה $\mathcal{O}\left(\exp\left(c \cdot n^{\frac{1}{3}} \cdot \log^{\frac{2}{3}}(n)\right)\right)$.

הצפנת RSA: יהיו $p, q \in \mathbb{P}$ יהיו $e, d \in \mathbb{N}$ באשר $(e, \varphi(pq)) = 1$ וכן $(e, \varphi(pq)) = 1$ ונגדיר $A : \mathbb{F}_2^* \times \mathbb{F}_2^* \rightarrow \mathbb{F}_2^*$ כך $A(c, (M, a)) = c^a \bmod M$ אזי $(A, A, (pq, e), (pq, d))$.

טענה: יהיו $p, q \in \mathbb{P}$ ותהא (M, M, k_e, k_d) הצפנת RSA אזי (M, M, k_e, k_d) הינה הצפנה אסימטרית.

טענה: יהיו $p, q \in \mathbb{P}$ ותהא (M, M, k_e, k_d) הצפנת RSA אזי $\text{Time}(M) = \mathcal{O}(\log^3(pq))$.

משפט: יהיו $p, q \in \mathbb{P}$ ותהא (M, M, k_e, k_d) הצפנת RSA ותהא $T : \mathbb{N} \rightarrow \mathbb{N}$ חשיבה בזמן אזי (קיים יריב \mathcal{A}^M בעל כוח חישובי

$\tilde{\mathcal{O}}(T)$ המקיים $(\mathcal{A}^{M(\cdot, k_e)}(1^n) = \text{IFP}(N) \iff (\mathcal{A}^{M(\cdot, k_e)}(1^n) = k_d)$ בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $(\mathcal{A}^{M(\cdot, k_e)}(1^n) = \text{IFP}(N))$.

לוגריתם דיסקרטי: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ויהי $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ אזי $a \in \mathbb{N}_{<p}$ באשר $a = g^x \bmod p$.

טענה: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ויהי $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ ויהיו $x, y \in \mathbb{N}_{<p}$ לוגריתמים דיסקרטיים של a מודולו p בבסיס g אזי $x = y$.

בעיית הלוגריתם הדיסקרטי: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ויהי $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ באשר $\text{DLP}(p, g, a) = x$ אזי $x \in \mathbb{N}_{<p}$ הינו הלוגריתם הדיסקרטי של a מודולו p בבסיס g .

טענה נפת שדות המספרים: קיים $c > 0$ עבורו קיים אלגוריתם \mathcal{A} ל-DLP באשר לכל $p \in \mathbb{P}$ מתקיים כי \mathcal{A} בעל סיבוכיות ריצה $\mathcal{O}\left(\exp\left(c \cdot \log^{\frac{1}{3}}(p) \cdot \log^{\frac{2}{3}}(p)\right)\right)$.

פרוטוקול תקשורת דיפי-הלמן: יהי $p \in \mathbb{P}$ ויהי g שורש פרימיטיבי מודולו p אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים

כך $\Pi_{\text{DiffieHellman}}$

Communication Protocol $\Pi_{\text{DiffieHellman}}(p, g)$:

```

A draws  $x \in [p-1]$ 
A sends  $(g^x \bmod p)$  as  $K_A$ 
B draws  $y \in [p-1]$ 
B sends  $(g^y \bmod p)$  as  $K_B$ 
A calculates  $K_{BA} \leftarrow (K_B)^x$ 
B calculates  $K_{AB} \leftarrow (K_A)^y$ 

```

טענה: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ויהיו K_{AB}, K_{BA} באשר $\Pi_{\text{DiffieHellman}}(p, g) = (K_{AB}, K_{BA})$ אזי $K_{AB} = K_{BA}$.

טענה: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ותהא $T : \mathbb{N} \rightarrow \mathbb{N}$ חשיבה בזמן עבורה קיים יריב \mathcal{A} בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{A} = \text{DLP}$ אזי קיים יריב \mathcal{B} בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{B}(p, g, g^x \bmod p, g^y \bmod p) = g^{xy} \bmod p$.

הצפנת ElGamal: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p יהי $x \in \mathbb{N}_{<p}$ ונגדיר $E, D : \mathbb{F}_2^* \times \mathbb{F}_2^* \rightarrow \mathbb{F}_2^*$ כך

• יהי $y \in \mathbb{N}_{<p}$ אזי $E(c, (\alpha, \beta, \gamma)) = ((c \cdot \gamma^y) \bmod \alpha, \beta^y \bmod \alpha)$

• $D((c_1, c_2), (\alpha, \beta, \gamma)) = (c_1 \cdot c_2^{-\gamma}) \bmod \alpha$

אזי $(E, D, (p, g, g^x \bmod p), (p, g, x))$

טענה: יהי $f \in \mathbb{R}[x]$ באשר $\deg(f) = 3$ וכן f בעל שורש מרובה אזי $\{(x, y) \in \mathbb{R}^2 \mid y^2 = f(x)\}$ אינה יריעה חד-מימדית גזירה.

עקום אליפטי: יהי \mathbb{F} שדה באשר $\text{char}(\mathbb{F}) \neq 2$ ויהי $f \in \mathbb{F}[x]$ באשר $\deg(f) = 3$ וכן f בעל שורשים פשוטים מעל \mathbb{F} אזי $\{(x, y) \in \mathbb{F}^2 \mid y^2 = f(x)\} \cup \{\infty\}$

סימון: יהי \mathbb{F} שדה באשר $\text{char}(\mathbb{F}) \neq 2$ ויהי E עקום אליפטי מעל \mathbb{F} אזי E/\mathbb{F}

טענה: יהי E/\mathbb{R} עקום אליפטי אזי $E \setminus \{\infty\}$ יריעה חד-מימדית חלקה.

הגדרה שיקוף: יהי E עקום אליפטי ותהא $P \in E$

• אם $P = \infty$ אזי $-P = P$

• אם $P = (x, y)$ אזי $-P = (x, -y)$

טענה: יהי E עקום אליפטי ויהי $P \in E$ אזי $-P \in E$ וכן $-(-P) = P$

טענה: יהי E עקום אליפטי ותהינה $P, Q \in E \setminus \{\infty\}$ באשר $P \neq \pm Q$ אזי $(\text{line}_{P,Q} \setminus \{P, Q\}) \cap E \neq \emptyset$

טענה: יהי E עקום אליפטי ותהא $P \in E \setminus \{\infty\}$ באשר $P \neq -P$ אזי $(T_P(E \setminus \{\infty\}) \setminus \{P\}) \cap E \neq \emptyset$

הגדרה חיבור: יהי E עקום אליפטי ותהינה $P, Q \in E$

• אם $\infty \in \{P, Q\}$ אזי $P + Q = \infty$

• אם $\infty \notin \{P, Q\}$ אזי $P + Q = \infty$ וכן $P = -Q$

• אם $\infty \notin \{P, Q\}$ וכן $P \neq \pm Q$ תהא $R \in (\text{line}_{P,Q} \setminus \{P, Q\}) \cap E$ אזי $P + Q = -R$

• אם $\infty \notin \{P, Q\}$ וכן $P = Q$ וכן $P \neq -Q$ תהא $R \in ((T_P(E \setminus \{\infty\})) \setminus \{P\}) \cap E$ אזי $P + Q = -R$

טענה: יהי E עקום אליפטי ותהינה $P, Q \in E$ אזי $P + Q = Q + P$

טענה: יהי E עקום אליפטי ותהינה $P, Q, R \in E$ אזי $(P + Q) + R = P + (Q + R)$

מסקנה: יהי E עקום אליפטי אזי $(E, +)$ חבורה אבלית.

טענה: יהי $p \in \mathbb{P}_{>2}$ ויהי E/\mathbb{F}_p עקום אליפטי המוגדר על ידי f אזי $|E| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)$

משפט האסה: יהי $p \in \mathbb{P}_{>2}$ ויהי $f \in \mathbb{F}_p[x]$ באשר $\deg(f) = 3$ וכן f בעל שורשים פשוטים מעל \mathbb{F}_p אזי $\left|\sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right)\right| \leq 2\sqrt{p}$

מסקנה: יהי $p \in \mathbb{P}_{>2}$ ויהי E/\mathbb{F}_p עקום אליפטי אזי $|E| \leq p + 1 + 2\sqrt{p}$

טענה: יהי $p \in \mathbb{P}_{>2}$ אזי קיים אלגוריתם \mathcal{A} המחשב חיבור נקודות על עקום אליפטי מעל \mathbb{F}_p בסיבוכיות ריצה $\mathcal{O}(\log^2(p))$

טענה: יהי $p \in \mathbb{P}_{>2}$ ויהי $n \in \mathbb{N}$ אזי קיים אלגוריתם \mathcal{A} המחשב הכפלת נקודה על עקום אליפטי מעל \mathbb{F}_p ב- n בסיבוכיות ריצה $\mathcal{O}(\log(n) \cdot \log^2(p))$

בעיית הלוגריתם הדיסקרטי בעקומים אליפטיים: יהי $p \in \mathbb{P}_{>2}$ יהי E/\mathbb{F}_p עקום אליפטי יהי $G \in E$ ויהי $n \in \mathbb{N}_+$ אזי

$\text{ECDLP}(p, E, G, nG) = n$

טענה: קיים אלגוריתם \mathcal{A} ל- ECDLP באשר לכל $p \in \mathbb{P}_{>2}$ מתקיים כי \mathcal{A} בעל סיבוכיות ריצה $\mathcal{O}(\sqrt{p})$

פרוטוקול תקשורת דיפי-הלמן בעקומים אליפטיים: יהי $p \in \mathbb{P}_{>2}$ יהי E/\mathbb{F}_p עקום אליפטי המוגדר על ידי f ויהי $G \in E \setminus \{\infty\}$ אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים $\Pi_{\text{DiffieHellman}}^{\text{EC}}$ כך

Communication Protocol $\Pi_{\text{DiffieHellman}}^{\text{EC}}(p, f, G)$:

A draws $x \in [p-1]$
 A sends xG as K_A
 B draws $y \in [p-1]$
 B sends yG as K_B
 A calculates $K_{BA} \leftarrow x \cdot K_B$
 B calculates $K_{AB} \leftarrow y \cdot K_A$

טענה: יהי $p \in \mathbb{P}_{>2}$ יהי E/\mathbb{F}_p עקום אליפטי המוגדר על ידי f ויהי $G \in E \setminus \{\infty\}$ ויהיו K_{AB}, K_{BA} באשר $\Pi_{\text{DiffieHellman}}^{\text{EC}}(p, g) = K_{AB} = K_{BA}$ אזי (K_{AB}, K_{BA})

טענה: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p תהא $T : \mathbb{N} \rightarrow \mathbb{N}$ חשיבה בזמן עבורה קיים יריב \mathcal{A} בעל כוח חישובי $\tilde{O}(T)$ המקיים $\mathcal{B}(p, f, G, xG, yG) = xyG$ המקיים $\tilde{O}(T)$ בעל כוח חישובי $\mathcal{A} = \text{ECDLP}$

פונקציית ספירת הראשוניים: נגדיר $\pi : \mathbb{R}_+ \rightarrow \mathbb{N}$ כך $\pi(x) = |\mathbb{P}_{\leq x}|$.

פונקציות אסימפטוטיות: פונקציות $f, g : \mathbb{R} \rightarrow \mathbb{R}$ המקיימות $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$.

סימון: תהייה $f, g : \mathbb{R} \rightarrow \mathbb{R}$ אסימפטוטיות אזי $f \sim g$.

פונקציה חסומה אסימפטוטית: תהא $f : \mathbb{R} \rightarrow \mathbb{R}$ אזי $g : \mathbb{R} \rightarrow \mathbb{R}$ המקיימת $\limsup_{x \rightarrow \infty} \frac{f(x)}{g(x)} \leq 1$.

סימון: תהייה $f, g : \mathbb{R} \rightarrow \mathbb{R}$ באשר f חסומה אסימפטוטית על ידי g אזי $f \lesssim g$.

טענה: תהייה $f, g : \mathbb{R} \rightarrow \mathbb{R}$ אזי $(f \lesssim g) \iff \left(\liminf_{x \rightarrow \infty} \frac{g(x)}{f(x)} \geq 1 \right)$.

טענה: תהייה $f, g : \mathbb{R} \rightarrow \mathbb{R}$ אזי $(f \lesssim g) \iff (\forall \varepsilon > 0. \exists x \in \mathbb{R}. \forall y > x. (f(y) \leq (1 + \varepsilon)g(y)))$.

טענה: תהייה $f, g : \mathbb{R} \rightarrow \mathbb{R}$ אזי $(f \sim g) \iff ((f \lesssim g) \wedge (g \lesssim f))$.

הערה: בקורס זה $\log = \ln$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\pi(2n) - \pi(4) \leq \frac{\log(4) \cdot n}{\log(n)}$.

משפט צ'בישב: $\pi(x) \lesssim \frac{\log(4) \cdot x}{\log(x)}$.

מסקנה: $\sum_{p \in \mathbb{P}_{\leq x}} \log(p) \lesssim \log(4) \cdot x$.

למה: יהי $n \in \mathbb{N}_+$ אזי $\binom{2n}{n} \geq \frac{4^n}{2n+1}$.

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

למה: יהי $x \in \mathbb{R}$ אזי $2 \lfloor x \rfloor - 2 \lfloor x \rfloor \leq 1$.

למה: יהי $n \in \mathbb{N}_+$ ויהי $p \in \mathbb{P}$ אזי $e_p\left(\binom{2n}{n}\right) \leq \log_p(2n)$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\pi(2n) \geq \frac{\log(2) \cdot 2n}{\log(2n)} - 2$.

משפט צ'בישב: $\pi(x) \gtrsim \frac{\log(2) \cdot x}{\log(x)}$.

טענה: תהא $f : \mathbb{N}_+ \rightarrow \mathbb{P}$ הפיכה ושומרת סדר אזי קיים $\alpha \in (0, 1]$ וקיים $\beta \in \mathbb{R}_{\geq 1}$ עבורם לכל $n \in \mathbb{N}_{\geq 2}$ מתקיים $\alpha n \log(n) \leq f(n) \leq \beta n \log(n)$.

משפט סכימה בחלקים/נוסחת אבל: יהי $x \in \mathbb{R}_{\geq 1}$ תהא $a : \mathbb{N} \rightarrow \mathbb{C}$ ותהא $f \in C^1([1, x], \mathbb{R})$ אזי $\sum_{n \in \mathbb{N}_{\leq x}} (a_n \cdot f(n)) = \left(\sum_{n \in \mathbb{N}_{\leq x}} a_n \right) \cdot f(x) - \int_1^x \left(\sum_{n \in \mathbb{N}_{\leq t}} a_n \right) \cdot f'(t) dt$.

למה: $\log(n!) = n \cdot \log(n) + \mathcal{O}(n)$.

טענה: $\log(n!) = n \cdot \log(n) - n + \mathcal{O}(\log(n))$.

משפט מרטנס: $\sum_{p \in \mathbb{P}_{\leq x}} \frac{\log(p)}{p} = \log(x) + \mathcal{O}(1)$.

משפט מרטנס: קיים $c > 0$ עבורו $\sum_{p \in \mathbb{P}_{\leq x}} \frac{1}{p} = \log \log(x) + c + \mathcal{O}\left(\frac{1}{\log(x)}\right)$.

משפט: קיים $K > 0$ עבורו $\prod_{p \in \mathbb{P}_{\leq x}} \left(1 - \frac{1}{p}\right) \sim \frac{K}{\log(x)}$.

מסקנה: קיים $c > 0$ עבורו לכל $n \in \mathbb{N}_+$ מתקיים $\varphi(n) \geq c \cdot \frac{n}{\log \log(n)}$.

טענה: יהי $n \in \mathbb{N}_+$ אזי $\text{lcm}(1, \dots, n) \geq 2^{n-2}$.

מסקנה: יהי $n \in \mathbb{N}_+$ אזי $\pi(n) \geq \frac{\log(2) \cdot n}{\log(n)} - \frac{2 \log(2)}{\log(n)}$.

קבוע אוילר-מסקרוני: נגדיר $\gamma \in \mathbb{R}$ כך $\gamma = 1 - \int_1^\infty \frac{t - \lfloor t \rfloor}{t^2} dt$.

טענה: $\gamma = \lim_{n \rightarrow \infty} \left(\left(\sum_{i=1}^n \frac{1}{i} \right) - \log(n) \right)$.

משפט מרטנס: $\prod_{p \in \mathbb{P}_{\leq x}} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log(x)}$. לא הוכח בקורס.

טענה: יהי $c \in \mathbb{R}$ אזי אם $c \geq 1$ אז $\pi(x) \lesssim \frac{c \cdot x}{\log(x)}$.

טענה: יהי $c \in \mathbb{R}$ אזי אם $c \leq 1$ אז $\pi(x) \gtrsim \frac{c \cdot x}{\log(x)}$.

מסקנה: יהי $c \in \mathbb{R}$ אזי אם $c = 1$ אז $\pi(x) \sim \frac{c \cdot x}{\log(x)}$.

משפט המספרים הראשוניים: $\pi(x) \sim \frac{x}{\log(x)}$. לא הוכח בקורס.

טענה: יהי $\varepsilon > 0$ אזי קיים $N \in \mathbb{N}$ עבורו לכל $n \in \mathbb{N}_{\geq N}$ מתקיים $[n, (1 + \varepsilon)n] \cap \mathbb{P} \neq \emptyset$.

האינטגרל הלוגריתמי: נגדיר $\text{Li} : \mathbb{R} \rightarrow \mathbb{R}$ כך $\text{Li}(x) = \int_2^x \frac{1}{\log(t)} dt$.

טענה: $\text{Li}(x) = \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + \mathcal{O}\left(\frac{x}{\log^3(x)}\right)$.

מסקנה: $\text{Li}(x) \sim \frac{x}{\log(x)}$.

טענה: יהי $m \in \mathbb{N}$ אזי $\text{Li}(x) = \sum_{k=0}^m \frac{(m-1)! \cdot x}{\log^m(x)} + \mathcal{O}\left(\frac{x}{\log^{m+1}(x)}\right)$.

משפט אדמר-דה-לה-וואלה-פוסן: קיים $c > 0$ עבורו $\pi(x) = \text{Li}(x) + \mathcal{O}\left(x \cdot \exp\left(-c \cdot \sqrt{\log(x)}\right)\right)$. לא הוכח בקורס.

$$\text{מסקנה: } \pi(x) = \frac{x}{\log(x)} + \frac{x}{\log^2(x)} + \mathcal{O}\left(\frac{x}{\log^3(x)}\right)$$

משפט וינוגרדוב: יהי $\varepsilon > 0$ אזי $\pi(x) = \text{Li}(x) + \mathcal{O}\left(x \cdot \exp\left(-\log^{\frac{2}{3}+\varepsilon}(x)\right)\right)$ לא הוכח בקורס

השערת רימן (RH): $\pi(x) = \text{Li}(x) + \mathcal{O}(\sqrt{x} \cdot \log(x))$ השערה פתוחה

סימון: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ אזי נגדיר $\pi_{m,a} : \mathbb{R} \rightarrow \mathbb{N}$ כך $\pi_{m,a}(x) = |\mathbb{P}_{\leq x} \cap (m\mathbb{N} + a)|$

סימון: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ אזי $\pi_{m,a}(\infty) = \lim_{x \rightarrow \infty} |\mathbb{P}_{\leq x} \cap (m\mathbb{N} + a)|$

טענה: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ באשר $(m, a) > 1$ אזי $\pi_{m,a}(\infty) \leq 1$

משפט דיריכלה: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ באשר $(a, m) = 1$ אזי $\pi_{m,a}(\infty) = \infty$ לא הוכח בקורס

משפט דה-לה-ואלה-פוסן/המספרים הראשוניים בסדרות חשבוניות: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ באשר $(a, m) = 1$ אזי

$$\pi_{m,a}(x) \sim \frac{x}{\varphi(m) \cdot \log(x)} \quad \text{לא הוכח בקורס}$$

מסקנה: יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ באשר $(a, m) = 1$ אזי $\pi_{m,a}(x) \sim \frac{1}{\varphi(m)} \text{Li}(x)$

השערת רימן המוכללת (GRH): יהי $m \in \mathbb{N}$ ויהי $a \in \mathbb{Z}$ באשר $(a, m) = 1$ אזי $\pi_{m,a}(x) = \frac{1}{\varphi(m)} \text{Li}(x) + \mathcal{O}(\sqrt{x} \cdot \log(x))$

השערה פתוחה

משפט: אם GRH אז קיים $c > 0$ עבורו לכל $N \in \mathbb{N}_+$ מתקיים $\text{MillerRabinPrimalityTest}(N; a) = \text{True} \iff (N \in \mathbb{P})$ לכל

$(a \leq c \log^2(N))$ לא הוכח בקורס

מסקנה: אם GRH אז קיים אלגוריתם דטרמיניסטי \mathcal{A} לבדיקת ראשוניות בעל בסיבוכיות ריצה $\tilde{O}(n^4)$.

משוואה דיופנטית: יהי $n \in \mathbb{N}$ ויהי $f \in \mathbb{Z}[x_1, \dots, x_n]$ אזי $f = 0$

טענה: יהי $f \in \mathbb{Z}[x_1, \dots, x_n]$ ויהי $N \in \mathbb{N}_{\geq 2}$ באשר $\text{sols}_{\mathbb{Z}_N}(f = 0) = \emptyset$ אזי $\text{sols}_{\mathbb{Z}}(f = 0) = \emptyset$

משפט מטיאסביץ': $\{\langle f \rangle \mid (f \in \mathbb{Z}[x_1, \dots, x_n]) \wedge (\text{sols}_{\mathbb{Z}}(f = 0) \neq \emptyset)\} \notin \mathcal{R}$

פולינום הומוגני בשני משתנים: יהי R חוג אזי $f \in R[x, y]$ עבורו קיים $n \in \mathbb{N}$ וקיים $a \in R^{n+1}$ עבורם $f = \sum_{i=0}^n a_i x^i y^{n-i}$

משוואה דיופנטית הומוגנית בשני משתנים: יהי $f \in \mathbb{Z}[x, y]$ הומוגני אזי $f = 0$

טענה: יהי $f \in \mathbb{Z}[x, y]$ אזי $(f \text{ הומוגני}) \iff (f(x, y) = \lambda^{\deg(f)} \cdot f(x/\lambda, y/\lambda) \text{ מתקיים } x, y, \lambda \in \mathbb{R} \text{ לכל})$

טענה: יהי $f \in \mathbb{Z}[x, y]$ הומוגני והיו $a, b \in \mathbb{Z} \setminus \{0\}$ באשר $f(a, b) = 0$ אזי $f\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 0$

פתרון מצומצם/פרימיטיבי: יהי $f \in \mathbb{Z}[x, y]$ הומוגני אזי $(a, b) \in \mathbb{Z}^2$ באשר $f(a, b) = 0$ וכן $f(a, b) = 1$

טענה: יהי $f \in \mathbb{Z}[x, y]$ הומוגני ויהי $\zeta \in \mathbb{Z}^{n+1}$ באשר $f = \sum_{i=0}^n \zeta_i x^i y^{n-i}$ אזי

• $\text{sols}_{\mathbb{Z}}(f = 0) = \{(da, db) \mid (d \in \mathbb{Z}) \wedge (f = 0 \text{ פתרון פרימיטיבי של } f = 0)\}$

• לכל פתרון פרימיטיבי (a, b) של $f = 0$ מתקיים $a|\zeta_0$ וכן $b|\zeta_n$

משוואה דיופנטית במשתנה אחד: יהי $f \in \mathbb{Z}[x]$ אזי $f = 0$

מסקנה: יהי $f \in \mathbb{Z}[x]$ ויהי $\zeta \in \mathbb{Z}^{n+1}$ באשר $f = \sum_{i=0}^n \zeta_i x^i$ ויהי $\frac{a}{b} \in \mathbb{Q}$ באשר $(a, b) = 1$ וכן $f\left(\frac{a}{b}\right) = 0$ אזי $a|\zeta_0$ וכן $b|\zeta_n$

מסקנה: יהי $f \in \mathbb{Z}[x]$ ויהי $\zeta \in \mathbb{Z}^{n+1}$ באשר $f = \sum_{i=0}^n \zeta_i x^i$ ויהי $m \in \mathbb{Z}$ באשר $f(m) = 0$ אזי $m|\zeta_0$

משוואה דיופנטית לינארית בשני משתנים: יהי $f \in \mathbb{Z}_{\leq 1}[x, y]$ אזי $f = 0$

טענה: יהיו $a, b, c \in \mathbb{Z}$ אזי $(a, b) | c \iff (\text{sols}_{\mathbb{Z}}(ax + by = c) \neq \emptyset)$

טענה: יהיו $a, b, c \in \mathbb{Z}$ ויהי $(\alpha, \beta) \in \text{sols}_{\mathbb{Z}}(ax + by = c)$ אזי $\left\{ \left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)} \right) \mid m \in \mathbb{Z} \right\} = \text{sols}_{\mathbb{Z}}(ax + by = c)$

טענה: יהיו $a_1 \dots a_n, b \in \mathbb{Z}$ אזי $(a_1, \dots, a_n) | b \iff (\text{sols}_{\mathbb{Z}}(\sum_{i=1}^n a_i x_i = b) \neq \emptyset)$

משוואה דיופנטית ריבועית בשני משתנים: יהי $f \in \mathbb{Z}_{\leq 2}[x, y]$ אזי $f = 0$

טענה: יהי $f \in \mathbb{Z}_{\leq 2}[x, y]$ אזי קיימים $\alpha, \beta, \gamma, \delta, \varepsilon, \zeta \in \mathbb{Q}$ עבורם אחד מהבאים מתקיים

• לכל $x, y \in \mathbb{Z}$ מתקיים $f(\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \zeta) = y - x^2$

• קיימים $a, d \in \mathbb{Z}$ עבורם לכל $x, y \in \mathbb{Z}$ מתקיים $f(\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \zeta) = x^2 - dy^2 - a$

טענה: $\text{sols}_{\mathbb{Z}}(y = x^2) = \{(m, m^2) \mid m \in \mathbb{Z}\}$

טענה: יהי $a \in \mathbb{Z}$ אזי $(a = \square) \iff (\text{sols}_{\mathbb{Z}}(x^2 = 0) \neq \emptyset)$

מסקנה: יהי $a \in \mathbb{Z}$ באשר $a = \square$ אזי $\text{sols}_{\mathbb{Z}}(x^2 = 0) = \{\pm\sqrt{a}\}$

טענה: יהי $a \in \mathbb{Z}$ ויהי $d \in \mathbb{Z}_{<0}$ אזי $\left\{ (s \cdot \sqrt{a + dy^2}, y) \mid (s \in \{\pm 1\}) \wedge \left(-\sqrt{\left|\frac{a}{d}\right|} \leq y \leq \sqrt{\left|\frac{a}{d}\right|}\right) \right\} = \text{sols}_{\mathbb{Z}}(x^2 - dy^2 = a)$

טענה: יהי $d \in \mathbb{N}_+$ אזי $(d = \square) \iff (\text{sols}_{\mathbb{Z}}(x^2 - dy^2 = 0) \setminus \{(0, 0)\} \neq \emptyset)$

מסקנה: יהי $d \in \mathbb{N}_+$ באשר $d = \square$ אזי $\left\{ (sm \cdot \sqrt{d}, rm) \mid (s, r \in \{\pm 1\}) \wedge (m \in \mathbb{Z}) \right\} = \text{sols}_{\mathbb{Z}}(x^2 - dy^2 = 0)$

טענה: יהי $a \in \mathbb{Z}$ ויהי $d \in \mathbb{N}_+$ באשר $d = \square$ אזי $\text{sols}_{\mathbb{Z}}(x^2 - dy^2 = a) = \bigcup_{\substack{(u,v) \in \mathbb{Z}^2 \\ a=uv}} \text{sols}_{\mathbb{Z}}\left(\begin{cases} x-\sqrt{d}y=u \\ x+\sqrt{d}y=v \end{cases}\right)$

משוואת פל: יהי $d \in \mathbb{N}_+$ באשר $d \neq \square$ אזי $x^2 - dy^2 = 1$.

משוואת פל מוכללת: יהי $a \in \mathbb{Z} \setminus \{0\}$ ויהי $d \in \mathbb{N}_+$ באשר $d \neq \square$ אזי $x^2 - dy^2 = a$.

הגדרה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ אזי $\mathbb{Z}[\sqrt{d}] = \mathbb{Z} + \sqrt{d} \cdot \mathbb{Z}$.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ אזי $\mathbb{Z}[\sqrt{d}]$ חוג.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהיו $\alpha, \beta, \gamma, \delta \in \mathbb{Z}$ באשר $\alpha + \beta\sqrt{d} = \gamma + \delta\sqrt{d}$ אזי $\alpha = \gamma$ וכן $\beta = \delta$.

הצמדה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהיו $\alpha, \beta \in \mathbb{Z}$ אזי $\overline{\alpha + \beta\sqrt{d}} = \alpha - \beta\sqrt{d}$.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהיו $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ אזי $\overline{(\overline{\alpha})} = \alpha$ וכן $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$ וכן $\overline{\alpha\beta} = \overline{\alpha} \cdot \overline{\beta}$.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהי $\alpha \in \mathbb{Z}[\sqrt{d}]$ אזי $(\overline{\alpha} = \alpha) \iff (\alpha \in \mathbb{Z})$.

מסקנה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ונגדיר $f : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}[\sqrt{d}]$ כך $f(x) = \overline{x}$ אזי f הינו אוטומורפיזם חוגים.

נורמה בחוג $\mathbb{Z}[\sqrt{d}]$: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהי $\alpha \in \mathbb{Z}[\sqrt{d}]$ אזי נגדיר $N : \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}$ כך $N(\alpha) = \alpha \cdot \overline{\alpha}$.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהיו $\alpha, \beta \in \mathbb{Z}[\sqrt{d}]$ אזי $N(\alpha\beta) = N(\alpha)N(\beta)$.

טענה: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ אזי $\mathbb{Z}[\sqrt{d}]^\times = \{\alpha \in \mathbb{Z}[\sqrt{d}] \mid N(\alpha) \in \{\pm 1\}\}$.

מסקנה: יהי $d \in \mathbb{Z}_{<0}$ אזי $\mathbb{Z}[\sqrt{d}]^\times = \begin{cases} \{\pm 1, \pm i\} & d=-1 \\ \{\pm 1\} & d<-1 \end{cases}$.