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

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

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

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

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

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

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

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

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

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

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

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

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

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

**טענה:** יהי $a\in\mathbb{Z}$ אזי $a|0$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**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 $d \in \{0, \ldots, b-1\}^k$ באשר $d_k > 0$ המקיים $n = \sum_{i=1}^{k} d_i b^i$.

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

**הערה:** כאשר לא כתוב בסיס בייצוג נתייחס לבסיס עשרוני.

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

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

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

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

**טענה:** קיים אלגוריתם NaiveMul 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):
    if n = 1 then return a_1 · b_1
    α ← (a_1 ... a_{n/2});    β ← (a_{n/2+1} ... a_n)
    γ ← (b_1 ... b_{n/2});    δ ← (b_{n/2+1} ... b_n)
    A ← KaratsubaMult(α, γ)
    B ← KaratsubaMult(β, δ)
    C ← KaratsubaMult(α + β, γ + δ)
    return B · 2^n + (C − B − A) · 2^{n/2} + A
```

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

**טענה:** סיבוכיות הריצה של KaratsubaMult הינה $\mathcal{O}\left(n^{\log_2(3)}\right)$.

**טענה קולי־טוקי:** קיים אלגוריתם CooleyTukeyMul 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) ∨ (b < 0) ∨ (|a| < |b|) then
        return EuclidGCD(max{|a|, |b|}, min{|a|, |b|})
    if b = 0 then return a
    (q, r) ← RemainderDiv(a, b)
    return EuclidGCD(b, r)
```

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

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

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

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

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

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

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

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

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

**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:** יהי $a_1 \dots a_n \in \mathbb{Z}$ אזי $[a_1, \dots, a_n] = [|a_1|, \dots, |a_n|]$.

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

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

**טענה:** יהי $a_1 \dots a_n \in \mathbb{Z}$ 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:** $\mathbb{P} = \{p \in \mathbb{N} \mid \text{ראשוני } p\}$.

**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 $p|\prod_{i=1}^{n} a_i$ 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]⟩;    A_1 = False
    for i ∈ [1,...,N] do
        if A_i = True then
            j ← 1
            while i + ij ≤ N do
                A_{i+ij} = False
                j ← j + 1
            end
        end
    end
    return {i ∈ [N] | A_i = True}
```

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

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

**טענה אטקין־ברנשטיין:** 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 קיים ויחיד $k \in \mathbb{N}$ וקיימים ויחידים $p_1 \dots p_k \in \mathbb{P}$ באשר $p_i \leq p_{i+1}$ 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 $\{b + i \mid i \in \{0, \dots, n\}\} \cap \mathbb{P} = \varnothing$.

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

**טענה:** יהי $n \in \mathbb{N}_{\geq 2}$ 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 $\pi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ העתקת המנה ויהי $r \in \mathbb{N}$ שארית החלוקה של $a$ ב־$n$ אזי $\pi(a) = r + n\mathbb{Z}$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**הערה:** יהי $n\in\mathbb{N}_+$ אזי נשכן $\{0,\ldots,n-1\}\hookrightarrow\mathbb{Z}/n\mathbb{Z}$ כך $i\mapsto(i \mod n)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**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

```
Algorithm ModEquationSys(m_1...m_n, a_1...a_n):
    for i ∈ [n] do
        M_i ← ∏_{j∈[n]\{i}} m_j
        N_i ← InverseMod(m_i, M_i)
    end
    return ∑_{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 $\mathbb{1}^n \cdot \text{ModEquationSys} \equiv a \mod m$.

**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 $\mathbb{1}^n x \equiv a \mod m$)$\Longleftrightarrow$(לכל $i,j \in [n]$ מתקיים $a_i \equiv a_j \mod (m_i, m_j)$).

**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 $f : \mathbb{N}_+ \to \mathbb{R}$ עבורה לכל $n,m \in \mathbb{N}$ באשר $(n,m) = 1$ מתקיים $f(nm) = f(n) f(m)$.

**טענה:** $\varphi$ פונקציה כפלית.

**טענה:** תהא $f : \mathbb{N}_+ \to \mathbb{R}$ כפלית באשר $f \neq 0$ אזי $f(1) = 1$.

**טענה:** תהיינה $f,g : \mathbb{N}_+ \to \mathbb{R}$ כפליות באשר לכל $p \in \mathbb{P}$ ולכל $k \in \mathbb{N}$ מתקיים $f(p^k) = g(p^k)$ אזי $f = g$.

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

**טענה:** תהא $f : \mathbb{N}_+ \to \mathbb{R}$ כפלית אזי $F : \mathbb{N} \to \mathbb{R}$ המוגדרת $F(n) = \sum_{\substack{d\in\mathbb{N} \\ d|n}} f(d)$ הינה כפלית.

**פונקציית סכום המחלקים:** נגדיר $\sigma : \mathbb{N}_+ \to \mathbb{N}$ כך $\sigma(n) = \sum_{\substack{d\in\mathbb{N} \\ d|n}} d$.

**מסקנה:** $\sigma$ פונקציה כפלית.

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

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

**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 $n \in \mathbb{N}_+$ תהא $G$ חבורה מסדר $n$ ויהי $g$ יוצר של $G$ אזי $\{a \in G \mid G \text{ יוצר של } a\} = \{g^d | (d,n) = 1\}$.

**מסקנה:** יהי $n \in \mathbb{N}_+$ תהא $G$ חבורה מסדר $n$ ויהי $g$ יוצר של $G$ אזי $\left|\{g^d | (d,n) = 1\}\right| = \varphi(n)$.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**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 $\left(\mathbb{Z}/p^k\mathbb{Z}\right)^\times$ ציקלית.

**טענה:** יהי $k\in\mathbb{N}_{\ge2}$ ויהי $a\in\mathbb{Z}_{\text{odd}}$ אזי קיימים ויחידים $\alpha\in\{0,1\}$ וכן $\beta\in\left\{0,\ldots,2^{k-2}\right\}$ עבורם $a\equiv(-1)^\alpha5^\beta \mod 2^k$.

**מסקנה:** יהי $k\in\mathbb{N}_{\ge2}$ אזי $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^\times\simeq C_2\times C_{2^{k-2}}$.

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

- אם $k\le1$ אזי $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\simeq\prod_{i=1}^m C_{p_i^{e_i-1}(p_i-1)}$.
- אם $k\ge2$ אזי $\left(\mathbb{Z}/n\mathbb{Z}\right)^\times\simeq C_2\times C_{2^{k-2}}\times\prod_{i=1}^m C_{p_i^{e_i-1}(p_i-1)}$.

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

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

- אם $a^{p-1}\not\equiv1 \mod p^2$ אז לכל $k\in\mathbb{N}_+$ מתקיים כי $a$ פרימיטיבי מודולו $p^k$.
- אם $a^{p-1}\equiv1 \mod p^2$ 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 $n\nmid a$ וכן קיים $x\in\mathbb{Z}$ עבורו $x^2\equiv a \mod n$.

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

**אי־שארית ריבועית:** יהי $n\in\mathbb{N}$ אזי $a\in\mathbb{Z}$ המקיים $n\nmid a$ וכן $a$ אינו שארית ריבועית מודולו $n$.

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

**טענה:** יהי $p\in\mathbb{P}_{>2}$ יהי $g$ שורש פרימיטיבי מודולו $p$ ויהיו $a,r\in\mathbb{Z}$ באשר $p\nmid a$ וכן $a\equiv g^r \mod p$ אזי $(r\in\mathbb{Z}_{\text{even}})\iff\left(a\in\mathrm{QR}_p\right)$.

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

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

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

**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 $\left(\frac{-1}{p}\right)=\begin{cases}1 & p\equiv1 \mod 4\\ -1 & p\equiv3 \mod 4\end{cases}$.

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

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

**למה גאוס:** יהי $p\in\mathbb{P}_{>2}$ תהא $S\subseteq\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ באשר $S\cap(-S)=\varnothing$ וכן $S\cup(-S)=\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ ויהי $a\in\left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 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 $\left(\frac{2}{p}\right)=\begin{cases}1 & p \mod 8\in\{1,7\}\\ -1 & p \mod 8\in\{3,5\}\end{cases}$.

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

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

**למה:** יהי $a\in\mathbb{N}_+$ ויהיו $p,q\in\mathbb{P}_{>2}$ באשר $p\equiv\pm q \mod 4a$ 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 $\left(\frac{5}{p}\right)=\begin{cases}0 & p=5\\ 1 & p \mod 5\in\{1,4\}\\ -1 & p \mod 5\in\{2,3\}\end{cases}$.

**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 $p_1\ldots p_k\in\mathbb{P}_{>2}$ שונים אזי $\left|\mathrm{QR}_{\prod_{i=1}^k p_i}\right|=\frac{1}{2^k}\varphi\left(\prod_{i=1}^k p_i\right)$.

**סמל יעקובי:** יהי $k\in\mathbb{N}$ יהיו $p_1\ldots p_k\in\mathbb{P}_{>2}$ 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 $m\equiv k \mod n$ 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 $\left(\left(\frac{m}{n}\right)=0\right)\iff((m,n)>1)$.

**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 $m\equiv a^2 \mod n$ 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 $m\equiv a^2 \mod n$)$\Longleftrightarrow$(לכל $p\in\mathbb{P}$ המקיים $p|n$ 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 $\left(\frac{-1}{n}\right)=\begin{cases}1 & n\equiv 1 \mod 4\\ -1 & n\equiv 3 \mod 4\end{cases}$.

**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 $\left(\frac{2}{n}\right)=\begin{cases}1 & n \mod 8\in\{1,7\}\\ -1 & n \mod 8\in\{3,5\}\end{cases}$.

**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)^((n-1)/2) · JacobiSymbol(-m, n)
    if m ∈ N_even then return (-1)^(((n^2-1)/8)·e_2(m)) · JacobiSymbol(m / 2^(e_2(m)), n)
    if m < n then return (-1)^(((m-1)/2)·((n-1)/2)) · JacobiSymbol(n, m)
    (q, r) ← 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 $\mathcal{O}\left(n^3\right)$.

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

**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 $p|x^2+ay^2$)$\Longleftrightarrow$($\left(\frac{-a}{p}\right)=1$).

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

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

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

**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 $\mathcal{A}(N,a,m)=(a^m \mod N)$.

**אלגוריתם ריבוע איטרטיבי:** יהי $R$ חוג יהי $\mathcal{A}$ אלגוריתם כפל מעל $R$ יהיו $m_0\ldots m_k\in\{0,1\}$ ויהי $a\in R$ אזי

```
Algorithm IteratedSquaring_R[A](a, m):
    a_0 ← a
    r ← a_0^(m_0)
    for i ∈ [1, ..., k] do
        a_i ← A(a_(i-1), a_(i-1))
        if m_i = 1 then r ← A(r, a_i^(m_i))
    end
```

**סימון:** יהיו $N,m\in\mathbb{N}$ ויהי $a\in{}^{\mathbb{Z}}/_{N\mathbb{Z}}$ אזי $\text{ModIteratedSquaring}(N,a,m)=\text{IteratedSquaring}_{\mathbb{Z}/N\mathbb{Z}}(a,m)$.

**טענה:** יהיו $N,m\in\mathbb{N}$ ויהי $a\in{}^{\mathbb{Z}}/_{N\mathbb{Z}}$ אזי $\text{ModIteratedSquaring}(N,a,(m)_2)=(a^m \mod N)$.

**טענה:** יהי $\mathcal{A}$ אלגוריתם כפל מספרים ויהיו $N,m\in\mathbb{N}$ אזי סיבוכיות הריצה של ModIteratedSquaring הינה $\mathcal{O}\left(\log(m)\cdot\text{Time}(\mathcal{A})(\log_2(N))\right)$.

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

**מסקנה:** יהיו $N,m\in\mathbb{N}$ אזי סיבוכיות הריצה של $\text{ModIteratedSquaring}\left[\text{CooleyTukeyMul}\right]$ הינה $\mathcal{O}\left(\log\left(m\right)\cdot\log\left(N\right)\log\log\left(N\right)\log\log\log\left(N\right)\right)$.

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

```
Algorithm TrialDivision(N):
    for i ∈ [1, ..., √N] do
        (q, r) ← RemainderDiv(N, i)
        if r = 0 then return False
    end
    return True
```

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

**טענה:** סיבוכיות הריצה של TrialDivision הינה $\mathcal{O}\left(2^{\frac{n}{2}}\right)$.

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

```
Algorithm FermatPrimalityTest[A](N; a):
    if A(N, a, N − 1) = 1 then return True
    return False
```

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

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

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

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

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

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

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

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

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

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

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

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

**משפט אלפורד־גרנוויל־פומרנץ:** החל ממקום מסויים לכל $x\in\mathbb{N}$ מתקיים $\left|\left\{N<x\mid \text{מספר קרמייקל } N\right\}\right|>x^{\frac{2}{7}}$. לא הוכח בקורס

**משפט ארדוש:** קיים $c>0$ עבורו החל ממקום מסויים לכל $x\in\mathbb{N}$ מתקיים $\left|\left\{N<x\mid \text{מספר קרמייקל } N\right\}\right|<x\cdot\exp\left(\frac{-c\cdot\log(x)\cdot\log\log\log(x)}{\log\log(x)}\right)$. לא הוכח בקורס

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

```
Algorithm SolovayStrassenPrimalityTest[A](N; a):
    if N = 2 then return True
    if (N < 2) ∨ (2|N) then return False
    s ← JacobiSymbol(a, N)
    if (s ≠ 0) ∧ (A(N, a, (N−1)/2) = (s mod N)) then
        return True
    return False
```

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

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

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

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

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

```
Algorithm MillerRabinPrimalityTest[A](N; a):
    if N = 2 then return True
    if (N < 2) ∨ (2 | N) then return False
    α_0 ← A(N, a, (N−1)/2^{e_2(N−1)})
    for i ∈ [1, ..., e_2(N − 1)] do
        α_i ← A(N, α_{i−1}, 2)
        if α_i = −1 then return True
        if α_i ≠ 1 then return False
    end
    return True
```

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

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

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

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

**טענה:** יהי $k \in \mathbb{N}_{\text{odd}}$ באשר $2k+1, 4k+1 \in \mathbb{P}$ אזי
$\left|\left\{a \in \mathbb{N}_{<(2k+1)\cdot(4k+1)} \mid \text{MillerRabinPrimalityTest}\left(\left(2k+1\right)\cdot\left(4k+1\right);a\right) = \text{True}\right\}\right| = \frac{\varphi((2k+1)\cdot(4k+1))}{4}$.

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

**אלגוריתם לייצור מספרים ראשוניים:** יהי $\mathcal{A}$ אלגוריתם חזקה מודולרית יהיו $n,k \in \mathbb{N}_+$ ותהא $r : \mathbb{N} \to \left\{2^{n-1}, \ldots, 2^n\right\} \times \mathbb{N}^k$ באשר $\left(r\left(c\right)\right)_i < \left(r\left(c\right)\right)_1$ לכל $c \in \mathbb{N}$ ולכל $i \in \{2, \ldots, k+1\}$ אזי

```
Algorithm PrimeGenerator[A](n, k; r):
    c ← 0
    while True do
        b ← True
        for i ∈ [2, ..., k + 1] do
            b ← b ∧ MillerRabinPrimalityTest[A]((r(c))_1; (r(c))_i)
        end
        if b = True then return (r(c))_1
        c ← c + 1
    end
```

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

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

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

**טענה:** יהיו $p,q \in \mathbb{P}$ באשר $q | 2^p - 1$ אזי $q \equiv 1 \mod p$.

**טענה אויילר:** יהיו $p,q \in \mathbb{P}_{>3}$ באשר $p \equiv 3 \mod 4$ 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 $2^{n-1} \cdot \left(2^n - 1\right)$ מושלם.

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

```
Algorithm LucasLehmer[A, B](n, 2^n − 1):
    if A(n) = False then return False
    S_0 ← 4
    for i ∈ [1, ..., n − 2] do
        S_i ← (B(2^n − 1, S_{i−1}, 2) − 2)  mod p
    end
    if S_{n−2} = 0 then return True
    return False
```

**משפט:** יהי $n \in \mathbb{N}$ אזי $\left(2^n-1 \in \mathbb{P}\right) \Longleftrightarrow \left(\mathrm{LucasLehmer}\left(n, 2^n-1\right) = \mathrm{True}\right)$.

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

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

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

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

**משפט אגרוול־קיאל־סקסנה:** קיים אלגוריתם דטרמיניסטי AKS לבדיקת ראשוניות בעל בסיבוכיות ריצה $\tilde{\mathcal{O}}\left(n^6\right)$.

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

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

**בעיית הפירוק:** יהי $N \in \mathbb{N}_+$ אזי $\mathrm{IFP}\left(N\right) = \left(p_1, \ldots, p_k\right)$ 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 $\mathcal{O}\left(\exp\left(c \cdot n^{\frac{1}{3}} \cdot \log^{\frac{2}{3}}\left(n\right)\right)\right)$.

**הצפנה RSA:** יהיו $p, q \in \mathbb{P}$ יהיו $e, d \in \mathbb{N}$ באשר $\left(e, \varphi\left(pq\right)\right) = 1$ וכן $ed \equiv 1 \mod \varphi\left(n\right)$ ונגדיר $A : \mathbb{F}_2^* \times \mathbb{F}_2^* \to \mathbb{F}_2^*$ כך $A\left(c, \left(M, a\right)\right) = c^a \mod M$ אזי $\left(A, A, \left(pq, e\right), \left(pq, d\right)\right)$.

**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 $\mathrm{Time}\left(M\right) = \mathcal{O}\left(\log^3\left(pq\right)\right)$.

**משפט:** יהיו $p, q \in \mathbb{P}$ תהא $(M, M, k_e, k_d)$ הצפנת RSA ותהא $T : \mathbb{N} \to \mathbb{N}$ חשיבה בזמן אזי (קיים יריב $\mathcal{A}^M$ בעל כוח חישובי $\tilde{\mathcal{O}}\left(T\right)$ המקיים $\mathcal{A}^{M\left(\cdot, k_e\right)}\left(1^n\right) = k_d$)$\Longleftrightarrow$(קיים יריב $\mathcal{A}^M$ בעל כוח חישובי $\tilde{\mathcal{O}}\left(T\right)$ המקיים $\mathcal{A}^{M\left(\cdot, k_e\right)}\left(1^n\right) = \mathrm{IFP}\left(N\right)$).

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

**טענה:** יהי $p \in \mathbb{P}$ יהי $g$ שורש פרימיטיבי מודולו $p$ יהי $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ 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 $a \in \left(\mathbb{Z}/p\mathbb{Z}\right)^\times$ אזי $\mathrm{DLP}\left(p, g, a\right) = x$ באשר $x \in \mathbb{N}_{<p}$ 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 $\mathcal{O}\left(\exp\left(c \cdot \log^{\frac{1}{3}}\left(p\right) \cdot \log^{\frac{2}{3}}\left(p\right)\right)\right)$.

**פרוטוקול תקשורת דיפי־הלמן:** יהי $p \in \mathbb{P}$ ויהי $g$ שורש פרימיטיבי מודולו $p$ אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים $\Pi_{\mathrm{DiffieHellman}}$ כך

```
Communication Protocol Π_DiffieHellman(p, g):
    A draws x ∈ [p−1]
    A sends (g^x mod p) as K_A
    B draws y ∈ [p−1]
    B sends (g^y mod p) as K_B
    A calculates K_BA ← (K_B)^x
    B calculates K_AB ← (K_A)^y
```

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

**טענה**: יהי $p \in \mathbb{P}$ יהי $g$ שורש פרימטיבי מודולו $p$ תהא $T : \mathbb{N} \to \mathbb{N}$ 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 $\mathcal{B}(p, g, g^x \mod p, g^y \mod p) = g^{xy} \mod p$.

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

- יהי $y \in \mathbb{N}_{<p}$ אזי $E(c, (\alpha, \beta, \gamma)) = ((c \cdot \gamma^y) \mod \alpha, \beta^y \mod \alpha)$.
- $D((c_1, c_2), (\alpha, \beta, \gamma)) = \left(c_1 \cdot c_2^{-\gamma}\right) \mod \alpha$.

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

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

**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 $\overline{\mathbb{F}}$ אזי $\left\{(x, y) \in \mathbb{F}^2 \mid y^2 = f(x)\right\} \cup \{\infty\}$.

**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 $E \backslash \{\infty\}$ יריעה חלקה חד־מימדית.

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

- אם $P = \infty$ אז $-P = P$.
- אם $P = (x, y)$ אז $-P = (x, -y)$.

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

**טענה**: יהי $E$ עקום אליפטי ותהיינה $P, Q \in E \backslash \{\infty\}$ באשר $P \neq \pm Q$ אזי $(\text{line}_{P,Q} \backslash \{P, Q\}) \cap E \neq \varnothing$.

**טענה**: יהי $E$ עקום אליפטי ותהא $P \in E \backslash \{\infty\}$ באשר $P \neq -P$ אזי $(T_P(E \backslash \{\infty\}) \backslash \{P\}) \cap E \neq \varnothing$.

**הגדרה חיבור**: יהי $E$ עקום אליפטי ותהיינה $P, Q \in E$ אזי

- $P + \infty = P$ וכן $\infty + P = P$.
- אם $\infty \notin \{P, Q\}$ וכן $P = -Q$ אז $P + Q = \infty$.
- אם $\infty \notin \{P, Q\}$ וכן $P \neq \pm Q$ תהא $R \in (\text{line}_{P,Q} \backslash \{P, Q\}) \cap E$ אז $P + Q = -R$.
- אם $\infty \notin \{P, Q\}$ וכן $P = Q$ וכן $P \neq -Q$ תהא $R \in ((T_P(E \backslash \{\infty\}) \backslash \{P\}) \cap E)$ אז $P + Q = -R$.

**טענה**: יהי $E$ עקום אליפטי ותהיינה $P, Q \in E$ אזי $P + Q = Q + P$.

**טענה**: יהי $E$ עקום אליפטי ותהיינה $P, Q, R \in E$ 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 $\overline{\mathbb{F}_p}$ 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 $p + 1 - 2\sqrt{p} \leq |E| \leq p + 1 + 2\sqrt{p}$.

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

**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 $\mathcal{O}\left(\log(n) \cdot \log^2(p)\right)$.

**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 $\mathcal{O}\left(\sqrt{p}\right)$.

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

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

$A$ 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 $G \in E \backslash \{\infty\}$ 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 $T:\mathbb{N}\to\mathbb{N}$ חשיבה בזמן עבורה קיים יריב $\mathcal{A}$ בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{A}=\mathrm{ECDLP}$ אזי קיים יריב $\mathcal{B}$ בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{B}(p,f,G,xG,yG)=xyG$.

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

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

**סימון:** תהיינה $f,g:\mathbb{R}\to\mathbb{R}$ אסימפטוטיות אזי $f\sim g$.

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

**סימון:** תהיינה $f,g:\mathbb{R}\to\mathbb{R}$ באשר $f$ חסומה אסימפטוטית על ידי $g$ אזי $f\lesssim g$.

**טענה:** תהיינה $f,g:\mathbb{R}\to\mathbb{R}$ אזי $\left(\liminf_{x\to\infty}\frac{g(x)}{f(x)}\ge 1\right)\iff(f\lesssim g)$.

**טענה:** תהיינה $f,g:\mathbb{R}\to\mathbb{R}$ אזי $(\forall\varepsilon>0.\exists x\in\mathbb{R}.\forall y>x.\,(f(y)\le(1+\varepsilon)\,g(y)))\iff(f\lesssim g)$.

**טענה:** תהיינה $f,g:\mathbb{R}\to\mathbb{R}$ אזי $((f\lesssim g)\land(g\lesssim f))\iff(f\sim g)$.

**הערה:** בקורס זה $\log=\ln$.

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

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

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

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

**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 $\lfloor 2x\rfloor-2\lfloor x\rfloor\le 1$.

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

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

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

**טענה:** תהא $f:\mathbb{N}_+\to\mathbb{P}$ הפיכה שומרת סדר אזי קיים $\alpha\in(0,1]$ וקיים $\beta\in\mathbb{R}_{\ge 1}$ עבורם לכל $n\in\mathbb{N}_{\ge 2}$ מתקיים $\alpha n\log(n)\le f(n)\le\beta n\log(n)$.

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

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

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

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

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

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

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

**טענה:** יהי $n\in\mathbb{N}_+$ אזי $\mathrm{lcm}(1,\ldots,n)\ge 2^{n-2}$.

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

**טענה:** יהי $n\in\mathbb{N}_+$ אזי $\log(n!)=n\log(n)-\int_1^n\frac{\lfloor x\rfloor}{x}\mathrm{d}x$.

**טענה:** יהי $n\in\mathbb{N}_+$ אזי $\left(\frac{n}{e}\right)^n\le n!\le en\cdot\left(\frac{n}{e}\right)^n$.

**טענה:** $n!=\Theta\left(\left(\frac{n}{e}\right)^n\cdot\sqrt{n}\right)$.

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

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

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

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

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

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

**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 $n\in\mathbb{N}_{\ge N}$ מתקיים $[n,(1+\varepsilon)n]\cap\mathbb{P}\neq\varnothing$.

**פונקציית טטא של צ'בישב:** נגדיר $\vartheta:\mathbb{R}\to\mathbb{R}$ כך $\vartheta(x)=\sum_{p\in\mathbb{P}_{\le x}}\log(p)$.

**משפט:** $\lim_{x\to\infty}\frac{\vartheta(x)}{x}=1$.

**האינטגרל הלוגריתמי:** נגדיר $\mathrm{Li}:\mathbb{R}\to\mathbb{R}$ כך $\mathrm{Li}(x)=\int_2^x\frac{1}{\log(t)}\mathrm{d}t$.

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

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

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

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

**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 $\pi(x)=\mathrm{Li}(x)+\mathcal{O}\left(x\cdot\exp\left(-\log^{\frac{2}{3}+\varepsilon}(x)\right)\right)$. לא הוכח בקורס

**השערת רימן (RH):** $\pi(x)=\mathrm{Li}(x)+\mathcal{O}\left(\sqrt{x}\cdot\log(x)\right)$. השערה פתוחה

**סימון:** יהי $m\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ אזי נגדיר $\pi_{m,a}:\mathbb{R}\to\mathbb{N}$ כך $\pi_{m,a}(x)=\left|\mathbb{P}_{\le x}\cap(m\mathbb{N}+a)\right|$.

**סימון:** יהי $m\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ אזי $\pi_{m,a}(\infty)=\lim_{x\to\infty}\pi_{m,a}(x)$.

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

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

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

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

**משפט:** אם GRH אז קיים $c>0$ עבורו לכל $N\in\mathbb{N}_+$ מתקיים $(N\in\mathbb{P})\Longleftrightarrow(\mathrm{MillerRabinPrimalityTest}(N;a)=\mathrm{True}$ לכל $a\le c\log^2(N))$. לא הוכח בקורס

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

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

**טענה:** יהי $f\in\mathbb{Z}[x_1,\ldots,x_n]$ ויהי $N\in\mathbb{N}_{\ge2}$ באשר $\mathrm{sols}_{\mathbb{Z}_N}(f=0)=\varnothing$ אזי $\mathrm{sols}_{\mathbb{Z}}(f=0)=\varnothing$.

**משפט מטיאסביץ':** $\{\langle f\rangle\mid(f\in\mathbb{Z}[x_1,\ldots,x_n])\wedge(\mathrm{sols}_{\mathbb{Z}}(f=0)\ne\varnothing)\}\notin\mathcal{R}$.

**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 $f=\sum_{i=0}^n a_ix^iy^{n-i}$.

**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 ($f$ הומוגני)$\Longleftrightarrow$(לכל $x,y,\lambda\in\mathbb{R}$ מתקיים $f(\lambda x,\lambda y)=\lambda^{\deg(f)}\cdot f(x,y)$).

**טענה:** יהי $f\in\mathbb{Z}[x,y]$ הומוגני ויהיו $a,b\in\mathbb{Z}\backslash\{0\}$ 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 $(a,b)=1$.

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

- $\mathrm{sols}_{\mathbb{Z}}(f=0)=\{(da,db)\mid(d\in\mathbb{Z})\wedge($ $(a,b)$ 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 $f\in\mathbb{Z}[x]$ יהי $\zeta\in\mathbb{Z}^{n+1}$ באשר $f=\sum_{i=0}^n\zeta_ix^i$ 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 $f\in\mathbb{Z}[x]$ יהי $\zeta\in\mathbb{Z}^{n+1}$ באשר $f=\sum_{i=0}^n\zeta_ix^i$ ויהי $m\in\mathbb{Z}$ באשר $f(m)=0$ אזי $m|\zeta_0$.

**משוואה דיופנטית לינארית בשני משתנים:** יהי $f\in\mathbb{Z}_{\le1}[x,y]$ אזי $f=0$.

**טענה:** ויהי $a,b,c\in\mathbb{Z}$ אזי $((a,b)\,|c)\Longleftrightarrow(\mathrm{sols}_{\mathbb{Z}}(ax+by=c)\ne\varnothing)$.

**טענה:** ויהי $a,b,c\in\mathbb{Z}$ ויהי $(\alpha,\beta)\in\mathrm{sols}_{\mathbb{Z}}(ax+by=c)$ אזי $\mathrm{sols}_{\mathbb{Z}}(ax+by=c)=\left\{\left(\alpha+\frac{m\cdot b}{(a,b)},\beta-\frac{m\cdot a}{(a,b)}\right)\;\middle|\;m\in\mathbb{Z}\right\}$.

**טענה:** ויהי $a_1\ldots a_n,b\in\mathbb{Z}$ אזי $((a_1,\ldots,a_n)\,|b)\Longleftrightarrow(\mathrm{sols}_{\mathbb{Z}}(\sum_{i=1}^n a_ix_i=b)\ne\varnothing)$.

**משוואה דיופנטית ריבועית בשני משתנים:** יהי $f\in\mathbb{Z}_{\le2}[x,y]$ אזי $f=0$.

**טענה:** יהי $f\in\mathbb{Z}_{\le2}[x,y]$ 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:** $\mathrm{sols}_{\mathbb{Z}}\left(y=x^2\right)=\left\{\left(m,m^2\right)\mid m\in\mathbb{Z}\right\}$.

**טענה:** יהי $a\in\mathbb{Z}$ אזי $(a=\square)\iff\left(\mathrm{sols}_{\mathbb{Z}}\left(x^2=a\right)\neq\varnothing\right)$.

**מסקנה:** יהי $a\in\mathbb{Z}$ באשר $a=\square$ אזי $\mathrm{sols}_{\mathbb{Z}}\left(x^2=a\right)=\{\pm\sqrt{a}\}$.

**טענה:** יהי $a\in\mathbb{Z}$ ויהי $d\in\mathbb{Z}_{<0}$ אזי $\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)\subseteq\left\{\left(s\cdot\sqrt{a+dy^2},y\right)\;\middle|\;(s\in\{\pm1\})\wedge\left(-\sqrt{\left|\frac{a}{d}\right|}\le y\le\sqrt{\left|\frac{a}{d}\right|}\right)\right\}$.

**טענה:** יהי $d\in\mathbb{N}_+$ אזי $(d=\square)\iff\left(\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=0\right)\setminus\{(0,0)\}\neq\varnothing\right)$.

**מסקנה:** יהי $d\in\mathbb{N}_+$ באשר $d=\square$ אזי $\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=0\right)=\left\{\left(sm\cdot\sqrt{d},rm\right)\;\middle|\;(s,r\in\{\pm1\})\wedge(m\in\mathbb{Z})\right\}$.

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

**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 $\mathbb{Z}\left[\sqrt{d}\right]=\mathbb{Z}+\sqrt{d}\cdot\mathbb{Z}$.

**טענה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי $\mathbb{Z}\left[\sqrt{d}\right]$ חוג אבלי בעל יחידה.

**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 $\beta=\delta$.

**העתקת המקדמים:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי נגדיר $\mathrm{coeff}:\mathbb{Z}\left[\sqrt{d}\right]\to\mathbb{Z}^2$ כך $\mathrm{coeff}\left(\alpha+\beta\sqrt{d}\right)=(\alpha,\beta)$.

**מסקנה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי $\mathrm{coeff}$ חח"ע ועל.

**הערה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ נשכן את $\mathbb{Z}^2$ בתוך $\mathbb{Z}\left[\sqrt{d}\right]$ כך $(\alpha,\beta)\mapsto\alpha+\beta\sqrt{d}$.

**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 $\alpha,\beta\in\mathbb{Z}\left[\sqrt{d}\right]$ 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 $\alpha\in\mathbb{Z}\left[\sqrt{d}\right]$ אזי $(\alpha\in\mathbb{Z})\iff(\overline{\alpha}=\alpha)$.

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

**הגדרה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי נגדיר $N:\mathbb{Z}\left[\sqrt{d}\right]\to\mathbb{Z}$ כך $N(\alpha)=\alpha\cdot\overline{\alpha}$.

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

**טענה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי $\mathbb{Z}\left[\sqrt{d}\right]^{\times}=\left\{\alpha\in\mathbb{Z}\left[\sqrt{d}\right]\;\middle|\;N(\alpha)\in\{\pm1\}\right\}$.

**מסקנה:** יהי $d\in\mathbb{Z}_{<0}$ אזי $\mathbb{Z}\left[\sqrt{d}\right]^{\times}=\left\{\begin{smallmatrix}\{\pm1,\pm i\} & d=-1\\ \{\pm1\} & d<-1\end{smallmatrix}\right.$.

**טענה:** יהי $a\in\mathbb{Z}\setminus\{0\}$ ויהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי $\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)=\left\{g\in\mathbb{Z}\left[\sqrt{d}\right]\;\middle|\;N(g)=a\right\}$.

**מסקנה:** יהיו $a,b\in\mathbb{Z}\setminus\{0\}$ יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ ויהיו $\alpha,\beta,\gamma,\delta\in\mathbb{Z}$ באשר $\alpha^2-d\beta^2=a$ וכן $\gamma^2-d\delta^2=b$ אזי $(\alpha\gamma+d\beta\delta)^2-d(\alpha\delta+\beta\gamma)^2=ab$.

**הגדרה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי נגדיר $\mathrm{SG}:\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)^2\to\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)$ כך $\mathrm{SG}((\alpha,\beta),(\gamma,\delta))=(\alpha\gamma+d\beta\delta,\alpha\delta+\beta\gamma)$.

**טענה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ ויהיו $(\alpha,\beta),(\gamma,\delta)\in\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)$ אזי $\mathrm{SG}((\alpha,\beta),(\gamma,\delta))=\left(\alpha+\beta\sqrt{d}\right)\left(\gamma+\delta\sqrt{d}\right)$.

**מסקנה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ אזי $\left(\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right),\mathrm{SG}\right)$ חבורה אבלית.

**הגדרה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\mathbb{Z}\left[\sqrt{d}\right]_1^{\times}=\left\{\alpha\in\mathbb{Z}\left[\sqrt{d}\right]\;\middle|\;N(\alpha)=1\right\}$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)=\mathbb{Z}\left[\sqrt{d}\right]_1^{\times}$.

**הגדרה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\mathbb{Z}\left[\sqrt{d}\right]_{1+}^{\times}=\left\{\alpha\in\mathbb{Z}\left[\sqrt{d}\right]_1^{\times}\;\middle|\;\alpha>0\right\}$.

**טענה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ ויהי $\alpha\in\mathbb{Z}\left[\sqrt{d}\right]_1^{\times}$ אזי קיים ויחיד $\beta\in\mathbb{Z}\left[\sqrt{d}\right]_{1+}^{\times}$ וקיים ויחיד $s\in\{\pm1\}$ עבורם $\alpha=s\beta$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\mathbb{Z}\left[\sqrt{d}\right]_1^{\times}\simeq\mathbb{Z}\left[\sqrt{d}\right]_{1+}^{\times}\times\{\pm1\}$.

**סימון:** יהי $\alpha\in\mathbb{R}$ אזי $[\alpha]=\alpha$.

**שבר משולב:** יהי $n\in\mathbb{N}$ יהי $a_0\in\mathbb{R}$ ויהיו $a_1\ldots a_n\in\mathbb{R}_+$ אזי $[a_0,\ldots,a_n]=a_0+\frac{1}{[a_1,\ldots,a_n]}$.

**למה:** יהי $a_0\in\mathbb{R}$ ויהיו $a_1\ldots a_n\in\mathbb{R}_+$ ונגדיר $M\in M_{2\times2}(\mathbb{R})$ כך $M=\prod_{i=0}^{n}\left(\begin{smallmatrix}a_i & 1\\ 1 & 0\end{smallmatrix}\right)$ אזי $[a_0,\ldots,a_n,x]=\frac{(M)_{1,1}\cdot x+(M)_{1,2}}{(M)_{2,1}\cdot x+(M)_{2,2}}$.

**טענה:** יהי $a_0 \in \mathbb{R}$ יהיו $a_1 \ldots a_n \in \mathbb{R}_+$ ונגדיר $p_{-1}, \ldots, p_n, q_{-1}, \ldots, q_n \in \mathbb{R}$ כך $\left(\begin{smallmatrix} p_k \\ q_k \end{smallmatrix}\right) = \left(\prod_{i=0}^{k} \left(\begin{smallmatrix} a_i & 1 \\ 1 & 0 \end{smallmatrix}\right)\right) \cdot \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ אזי

- לכל $k \in \mathbb{N}_{\le n}$ מתקיים $\frac{p_k}{q_k} = [a_0, \ldots, a_k]$.
- לכל $k \in \mathbb{N}_{\le n}$ מתקיים $\left(\begin{smallmatrix} p_k & p_{k-1} \\ q_k & q_{k-1} \end{smallmatrix}\right) = \prod_{i=0}^{k} \left(\begin{smallmatrix} a_i & 1 \\ 1 & 0 \end{smallmatrix}\right)$.
- לכל $k \in \mathbb{N}_{\le n}$ מתקיים $p_k = a_k p_{k-1} + p_{k-2}$ וכן $q_k = a_k q_{k-1} + q_{k-2}$.
- לכל $k \in \mathbb{N}_{\le n}$ מתקיים $p_k q_{k-1} - q_k p_{k-1} = (-1)^{k+1}$.

**טענה:** יהי $a_0 \in \mathbb{R}$ יהיו $a_1 \ldots a_n \in \mathbb{R}_+$ ויהי $i \in \mathbb{N}_{\text{even}} \cap \mathbb{N}_{\le n}$ אזי $[a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots a_n]$ מונוטונית עולה.

**טענה:** יהי $a_0 \in \mathbb{R}$ יהיו $a_1 \ldots a_n \in \mathbb{R}_+$ ויהי $i \in \mathbb{N}_{\text{odd}} \cap \mathbb{N}_{\le n}$ אזי $[a_0, \ldots, a_{i-1}, x, a_{i+1}, \ldots a_n]$ מונוטונית יורדת.

**שבר משולב פשוט:** יהי $n \in \mathbb{N}$ יהי $a_0 \in \mathbb{Z}$ ויהיו $a_1 \ldots a_n \in \mathbb{N}_+$ אזי $[a_0, \ldots, a_n]$.

**טענה:** יהיו $n, m \in \mathbb{N}$ יהי $a_0, b_0 \in \mathbb{Z}$ ויהיו $a_1 \ldots a_n, b_1 \ldots b_m \in \mathbb{N}_+$ באשר $[a_0, \ldots, a_n] = [b_0, \ldots, b_m]$ אזי אחד מהבאים נכון

- $n = m$ וכן $a_i = b_i$ לכל $i \in \mathbb{N}_{\le n}$.
- $n = m + 1$ וכן $a_i = b_i$ לכל $i \in \mathbb{N}_{\le m-1}$ וכן $b_m - 1 = a_m$ וכן $a_n = 1$.
- $n + 1 = m$ וכן $a_i = b_i$ לכל $i \in \mathbb{N}_{\le n-1}$ וכן $a_n - 1 = b_n$ וכן $b_m = 1$.

**טענה:** יהי $\alpha \in \mathbb{Q}$ אזי קיים ויחיד $n \in \mathbb{N}$ וכן קיים ויחיד $a_0 \in \mathbb{Z}$ וכן קיימים ויחידים $a_1 \ldots a_n \in \mathbb{N}_+$ באשר $a_n > 1$ עבורם $\alpha = [a_0, \ldots, a_n]$.

**אלגוריתם שבר משולב פשוט למספר רציונלי:** יהי $a \in \mathbb{Z}$ ויהי $b \in \mathbb{Z} \backslash \{0\}$ אזי

```
Algorithm RationalContinuedFraction(a, b):
    if b = 0 then return
    (q, r) ← RemainderDiv(a, b)
    return [q] || RationalContinuedFraction(b, r)
```

**טענה:** יהי $a \in \mathbb{Z}$ ויהי $b \in \mathbb{Z} \backslash \{0\}$ אזי $\frac{a}{b} = \text{RationalContinuedFraction}(a, b)$.

**שבר משולב אינסופי:** תהא $a : \mathbb{N} \to \mathbb{R}$ באשר $a_i > 0$ לכל $i \in \mathbb{N}_+$ אזי $[a] = \lim_{n \to \infty} [a_0, \ldots, a_n]$.

**טענה:** תהא $a : \mathbb{N} \to \mathbb{R}$ באשר $a_i \ge 1$ לכל $i \in \mathbb{N}_+$ אזי $[a]$ קיים.

**שבר משולב פשוט אינסופי:** תהא $a : \mathbb{N} \to \mathbb{Z}$ באשר $a_i \in \mathbb{N}_+$ לכל $i \in \mathbb{N}_+$ אזי $[a]$.

**גלגול:** נגדיר $\text{Cycling} : \mathbb{R} \backslash \mathbb{Q} \to (1, \infty) \backslash \mathbb{Q}$ כך $\text{Cycling}(x) = \frac{1}{x - \lfloor x \rfloor}$.

**משפט:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ אזי קיים ויחיד שבר משולב פשוט אינסופי $[a]$ המקיים $\alpha = [a]$.

**אלגוריתם שבר משולב פשוט אינסופי למספר אי־רציונלי:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ אזי

```
Algorithm IrrationalContinuedFraction(n, α):
    if n = 0 then return
    return [⌊α⌋] || IrrationalContinuedFraction(n − 1, Cycling(α))
```

**טענה:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ אזי $\lim_{n \to \infty} \text{IrrationalContinuedFraction}(n, \alpha) = \alpha$.

**ייצוג שברי של שבר משולב פשוט אינסופי:** יהי $[a]$ שבר משולב פשוט אינסופי ונגדיר $p, q : \mathbb{Z}_{\ge -1} \to \mathbb{Z}$ כך $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \left(\prod_{i=0}^{k} \left(\begin{smallmatrix} a_i & 1 \\ 1 & 0 \end{smallmatrix}\right)\right) = \left(\begin{smallmatrix} p_k \\ q_k \end{smallmatrix}\right)$ אזי $(p, q)$.

**מסקנה:** יהי $[a]$ שבר משולב פשוט אינסופי ויהי $(p, q)$ ייצוג שברי של $[a]$ אזי לכל $k \in \mathbb{N}$ מתקיים $\frac{p_k}{q_k} = [a_0, \ldots, a_k]$.

**מסקנה:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ יהי $(p, q)$ ייצוג שברי של $\alpha$ ויהי $k \in \mathbb{N}_{\text{even}}$ אזי $\frac{p_k}{q_k} < \alpha < \frac{p_{k+1}}{q_{k+1}}$ וכן $\frac{p_k}{q_k} < \frac{p_{k+2}}{q_{k+2}}$ וכן $\frac{p_{k+1}}{q_{k+1}} < \frac{p_{k+3}}{q_{k+3}}$.

**משפט קירוב דיופנטי:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ ויהי $(p, q)$ ייצוג שברי של $\alpha$ אזי לכל $n \in \mathbb{N}_+$ מתקיים $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.

**טענה:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ יהי $(p, q)$ ייצוג שברי של $\alpha$ יהי $n \in \mathbb{N}$ יהי $\zeta \in \mathbb{Z}$ ויהי $\xi \in \mathbb{N}$ באשר $\xi < q_n$ אזי $\left|\alpha - \frac{p_n}{q_n}\right| < \left|\alpha - \frac{\zeta}{\xi}\right|$.

**משפט לז'נדר:** יהי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ יהי $(p, q)$ ייצוג שברי של $\alpha$ יהי $\zeta \in \mathbb{Z}$ ויהי $\xi \in \mathbb{N}$ באשר $\left|\alpha - \frac{\zeta}{\xi}\right| < \frac{1}{2\xi^2}$ אזי קיים $n \in \mathbb{N}$ עבורו $p_n = \zeta$ וכן $q_n = \xi$.

**משפט דיריכלה המוכלל לקירוב דיופנטי:** יהיו $d, N \in \mathbb{N}_+$ ויהי $v \in \mathbb{R}^d$ אזי קיים $q \in \left[N^d\right]$ וקיים $u \in \mathbb{Z}^d$ עבורם לכל $i \in [d]$ מתקיים $\left|v_i - \frac{1}{q} u_i\right| < \frac{1}{qN}$.

**פונקציה מחזורית החל ממקום מסויים:** יהיו $N, T \in \mathbb{N}$ אזי פונקציה $a : \mathbb{N} \to \mathbb{R}$ המקיימת $a_n = a_{n+T}$ לכל $n \in \mathbb{N}_{\ge N}$.

**סימון:** יהיו $N, T \in \mathbb{N}$ ותהא $a : \mathbb{N} \to \mathbb{R}$ מחזורית בעלת מחזור $T$ החל מ־$N$ אזי $a = a_0 \ldots a_{N-1} \overline{a_N \ldots a_{N+T-1}}$.

**שבר משולב פשוט מחזורי:** שבר משולב פשוט אינסופי $[a]$ עבורו $a$ מחזורית החל ממקום מסויים.

**הגדרה:** יהי $d\in\mathbb{R}$ אזי $\mathbb{Q}\left(\sqrt{d}\right)=\mathbb{Q}+\sqrt{d}\cdot\mathbb{Q}$.

**טענה:** יהי $d\in\mathbb{R}$ אזי $\mathbb{Q}\left(\sqrt{d}\right)$ שדה.

**טענה:** יהי $d\in\mathbb{R}$ באשר $\sqrt{d}\notin\mathbb{Q}$ ויהיו $\alpha,\beta,\gamma,\delta\in\mathbb{Q}$ באשר $\alpha+\beta\sqrt{d}=\gamma+\delta\sqrt{d}$ אזי $\alpha=\gamma$ וכן $\beta=\delta$.

**העתקת המקדמים:** יהי $d\in\mathbb{R}$ באשר $\sqrt{d}\notin\mathbb{Q}$ אזי נגדיר $\mathrm{coeff}:\mathbb{Q}\left(\sqrt{d}\right)\to\mathbb{Q}^2$ כך $\mathrm{coeff}\left(\alpha+\beta\sqrt{d}\right)=(\alpha,\beta)$.

**מסקנה:** יהי $d\in\mathbb{R}$ באשר $\sqrt{d}\notin\mathbb{Q}$ אזי coeff חח"ע ועל.

**הצמדה:** יהי $d\in\mathbb{R}$ ויהיו $\alpha,\beta\in\mathbb{Q}$ אזי $\overline{\alpha+\beta\sqrt{d}}=\alpha-\beta\sqrt{d}$.

**טענה:** יהי $d\in\mathbb{R}$ באשר $\sqrt{d}\notin\mathbb{Q}$ ונגדיר $f:\mathbb{Q}\left(\sqrt{d}\right)\to\mathbb{Q}\left(\sqrt{d}\right)$ כך $f(x)=\overline{x}$ אזי $f$ הינו אוטומורפיזם שדות.

**מספר ריבועי:** מספר $\alpha\in\mathbb{R}$ עבורו קיים $d\in\mathbb{Q}$ המקיים $\alpha\in\mathbb{Q}\left(\sqrt{d}\right)$.

**טענה:** יהי $\alpha\in\mathbb{R}$ ריבועי ויהי $d\in\mathbb{Q}$ עד להיות $\alpha$ ריבועי אזי $\mathrm{Cycling}(\alpha)$ ריבועי וכן $d$ עד להיות $\mathrm{Cycling}(\alpha)$ ריבועי.

**מסקנה:** יהי $\alpha\in\mathbb{R}$ אזי ($\alpha$ ריבועי)$\Longleftrightarrow$(קיים $d\in\mathbb{N}$ וקיימים $A,B\in\mathbb{Z}$ עבורם $\alpha=\frac{B+\sqrt{d}}{A}$).

**מסקנה:** יהי $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ אזי ($\alpha$ ריבועי)$\Longleftrightarrow$(קיים $d\in\mathbb{N}$ עבורו $d\neq\square$ וקיימים $A,B\in\mathbb{Z}$ עבורם $\alpha=\frac{B+\sqrt{d}}{A}$).

**מסקנה:** יהי $\alpha\in\mathbb{R}$ אזי ($\alpha$ ריבועי)$\Longleftrightarrow$(קיים $a\in\mathbb{Z}\backslash\{0\}$ וקיימים $b,c\in\mathbb{Z}$ עבורם $a\alpha^2+b\alpha+c=0$).

**טענה:** יהי $\alpha\in\mathbb{R}$ אזי ($\alpha$ ריבועי)$\Longleftrightarrow$(קיים $d\in\mathbb{N}$ וקיימים $A,B\in\mathbb{Z}$ עבורם $B^2\equiv d \mod A$ וכן $\alpha=\frac{B+\sqrt{d}}{A}$).

**מספר ריבועי מצומצם:** מספר ריבועי $\alpha\in\mathbb{R}_{>1}$ המקיים $\overline{\alpha}\in(-1,0)$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\sqrt{d}+\left\lfloor\sqrt{d}\right\rfloor$ ריבועי מצומצם.

**טענה:** יהי $\alpha\in\mathbb{R}$ ריבועי מצומצם אזי $\mathrm{Cycling}(\alpha)$ ריבועי מצומצם.

**טענה:** יהיו $\alpha,\beta\in\mathbb{R}$ ריבועיים מצומצמים באשר $\mathrm{Cycling}(\alpha)=\mathrm{Cycling}(\beta)$ אזי $\alpha=\beta$.

**טענה:** יהי $d\in\mathbb{N}$ ויהיו $A,B\in\mathbb{Z}$ באשר $B^2\equiv d \mod A$ וכן $\frac{B+\sqrt{d}}{A}$ ריבועי מצומצם אזי $A\in(0,d)$ וכן $B\in\left(0,\sqrt{d}\right)$.

**מסקנה:** יהי $d\in\mathbb{N}$ אזי $\left|\left\{\alpha\in\mathbb{Q}\left(\sqrt{d}\right)\mid \alpha \text{ ריבועי מצומצם}\right\}\right|<\aleph_0$.

**פונקציה מחזורית טהורה:** יהי $T\in\mathbb{N}$ אזי פונקציה $a:\mathbb{N}\to\mathbb{R}$ המקיימת $a_n=a_{n+T}$ לכל $n\in\mathbb{N}$.

**שבר משולב פשוט מחזורי טהור:** שבר משולב פשוט מחזורי $[a]$ עבורו $a$ מחזורית טהורה.

**משפט:** יהי $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ אזי (קיים שבר משולב פשוט מחזורי טהור $[a]$ עבורו $\alpha=[a]$)$\Longleftrightarrow$($\alpha$ ריבועי מצומצם).

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי קיים $n\in\mathbb{N}$ וקיימים $a_0\ldots a_{n-1}\in\mathbb{N}$ עבורם $\sqrt{d}=\left[a_0,\overline{a_1,\ldots,a_{n-1},2a_0}\right]$.

**מסקנה:** יהי $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ ריבועי נגדיר $a:\mathbb{N}\to\mathbb{R}\backslash\mathbb{Q}$ כך $a_0=\alpha$ וכן $a_{n+1}=\mathrm{Cycling}(a_n)$ אזי קיים $m\in\mathbb{N}$ עבורו $a_m$ ריבועי מצומצם וכן $a$ מחזורית החל מ־$m$.

**משפט:** יהי $\alpha\in\mathbb{R}\backslash\mathbb{Q}$ אזי (קיים שבר משולב פשוט מחזורי $[a]$ עבורו $\alpha=[a]$)$\Longleftrightarrow$($\alpha$ ריבועי).

**משפט:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ יהי $n\in\mathbb{N}$ תהא $a:\mathbb{N}\to\mathbb{N}$ מחזורית בעלת מחזור $n$ החל מ־1 באשר $\sqrt{d}=[a]$ ויהי $(p,q)$ ייצוג שברי של $[a]$ אזי

- לכל $k\in\mathbb{N}$ מתקיים $p_{kn-1}^2-dq_{kn-1}^2=(-1)^{kn}$.
- $\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2\in\{\pm1\}\right)=\{(p_{kn-1},q_{kn-1})\mid k\in\mathbb{N}\}$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ יהי $n\in\mathbb{N}$ תהא $a:\mathbb{N}\to\mathbb{N}$ מחזורית בעלת מחזור $n$ החל מ־1 באשר $\sqrt{d}=[a]$ ויהי $(p,q)$ ייצוג שברי של $[a]$ אזי

- $\left(\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=-1\right)\neq\varnothing\right)\Longleftrightarrow\left(n\in\mathbb{N}_{\mathrm{odd}}\right)$.
- אם $n\in\mathbb{N}_{\mathrm{odd}}$ אז $\min_{\pi_2}\left(\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2=-1\right)\right)=(p_{n-1},q_{n-1})$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ יהי $n\in\mathbb{N}$ תהא $a:\mathbb{N}\to\mathbb{N}$ מחזורית בעלת מחזור $n$ החל מ־1 באשר $\sqrt{d}=[a]$ ויהי $(p,q)$ ייצוג שברי של $[a]$ אזי

- $\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)\setminus\{(1,0),(-1,0)\}\neq\varnothing$.
- אם $n\in\mathbb{N}_{\mathrm{even}}$ אז $\min_{\pi_2}\left(\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2=1\right)\setminus\{(1,0),(-1,0)\}\right)=(p_{n-1},q_{n-1})$.
- אם $n\in\mathbb{N}_{\mathrm{odd}}$ אז $\min_{\pi_2}\left(\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2=1\right)\setminus\{(1,0),(-1,0)\}\right)=(p_{2n-1},q_{2n-1})$.

**הפתרון היסודי למשוואת פל:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ אזי $\min_{\pi_2}\left(\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2=1\right)\setminus\{(1,0),(-1,0)\}\right)$.

**סימון:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ ויהי $(u,v)$ הפתרון היסודי של $x^2-dy^2=1$ אזי $\varepsilon=u+v\sqrt{d}$.

**משפט:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ ויהי $\varepsilon$ הפתרון היסודי של $x^2-dy^2=1$ אזי $\langle\varepsilon\rangle=\mathbb{Z}\left[\sqrt{d}\right]_{1+}^{\times}$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ יהי $\varepsilon$ הפתרון היסודי של $x^2-dy^2=1$ ויהי $(\alpha,\beta)\in\text{sols}_{\mathbb{Z}}\left(x^2-dy^2=1\right)$ אזי קיים $n\in\mathbb{Z}$ וקיים $s\in\{\pm1\}$ עבורם $\alpha+\beta\sqrt{d}=s\cdot\varepsilon^n$.

**טענה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ ויהי $a\in\mathbb{Z}\backslash\{0\}$ באשר $\text{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)\neq\varnothing$ אזי $a\in\text{QR}_d\cup\{0\}$.

**מסקנה:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ ויהי $a\in\mathbb{Z}\backslash\{0\}$ באשר $\text{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)\neq\varnothing$ אזי

- לכל $p\in\mathbb{P}_{>2}$ המקיים $p|d$ מתקיים $\left(\frac{a}{p}\right)\in\{0,1\}$.
- אם $4|d$ אז $a \mod 4\in\{0,1\}$.
- אם $8|d$ אז $a \mod 8\in\{0,1,4\}$.

**משפט:** יהי $d\in\mathbb{N}$ באשר $d\neq\square$ יהי $\varepsilon$ הפתרון היסודי של $x^2-dy^2=1$ יהי $a\in\mathbb{Z}\backslash\{0\}$ ויהי $(\alpha,\beta)\in\text{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)$ אזי קיימים $z,w\in\mathbb{N}$ באשר $z+w\sqrt{d}<\sqrt{|a|}\varepsilon$ וקיים $n\in\mathbb{Z}$ וקיים $s\in\{\pm1\}$ עבורם $\alpha+\beta\sqrt{d}=s\cdot\varepsilon^n\cdot\left(z+w\sqrt{d}\right)$.

**מסקנה:** $\{\langle f\rangle\mid(f\in\mathbb{Z}_{\leq2}[x,y])\wedge(\text{sols}_{\mathbb{Z}}(f=0)\neq\varnothing)\}\in\mathcal{R}$.

**מספרי גאוס:** $\mathbb{Q}(i)=\mathbb{Q}+i\cdot\mathbb{Q}$.

**מסקנה:** $\mathbb{Q}(i)$ שדה.

**שלמי גאוס:** $\mathbb{Z}[i]=\mathbb{Z}+i\cdot\mathbb{Z}$.

**מסקנה:** $\mathbb{Z}[i]$ חוג אבלי בעל יחידה.

**תחום שלמות:** חוג $A$ עבורו לכל $a,b\in A$ המקיימים $ab=0$ מתקיים $(a=0)\vee(b=0)$.

**הגדרה:** יהי $A$ תחום שלמות אזי $A^\times=\{a\in A\mid\exists h\in A.ah=ha=1\}$.

**איבר מחלק איבר:** יהי $A$ תחום שלמות ויהי $a\in A$ אזי $b\in A$ עבורו קיים $c\in A$ המקיים $b=ac$.

**סימון:** יהי $A$ תחום שלמות ויהיו $a,b\in A$ באשר $a$ מחלק את $b$ אזי $a|b$.

**טענה:** יהי $A$ תחום שלמות ויהיו $a,b,c\in A$ אזי

- אם $a|b$ וכן $b|c$ אז $a|c$.
- אם $a|b$ וכן $a|c$ אז לכל $d,e\in A$ מתקיים $a|ab+ec$.
- $1|a$ וכן $a|0$.
- $((b|a)\wedge(a|b))\iff(\exists u\in A^\times.a=bu)$.

**חברים:** יהי $A$ תחום שלמות אזי $a,b\in A$ המקיימים $a|b$ וכן $b|a$.

**סימון:** יהי $A$ תחום שלמות ויהיו $a,b\in A$ חברים אזי $a\sim b$.

**טענה:** יהי $A$ תחום שלמות אזי $\sim$ יחס שקילות.

**טענה:** יהי $A$ תחום שלמות ויהיו $a,b,c,d\in A$ באשר $a\sim b$ וכן $c\sim d$ אזי $ac\sim bd$.

**טענה:** יהי $\alpha\in\mathbb{Z}[i]$ אזי $N(\alpha)=|\alpha|^2$.

**מסקנה:** יהי $\alpha\in\mathbb{Z}[i]$ אזי $(\alpha=0)\iff(N(\alpha)=0)$.

**משפט חלוקה עם שארית בשלמי גאוס:** יהי $\alpha\in\mathbb{Z}[i]$ ויהי $\beta\in\mathbb{Z}[i]\setminus\{0\}$ אזי קיימים $\kappa,\rho\in\mathbb{Z}[i]$ המקיימים $N(\rho)<N(\beta)$ וכן $\alpha=\kappa\beta+\rho$.

**טענה:** יהי $d\in\{2,-2,3\}$ יהי $\alpha\in\mathbb{Z}\left[\sqrt{d}\right]$ ויהי $\beta\in\mathbb{Z}\left[\sqrt{d}\right]\setminus\{0\}$ אזי קיימים $\kappa,\rho\in\mathbb{Z}\left[\sqrt{d}\right]$ המקיימים $|N(\rho)|<|N(\beta)|$ וכן $\alpha=\kappa\beta+\rho$.

**נורמה אוקלידית:** יהי $A$ תחום שלמות אזי $N:A\to\mathbb{N}$ המקיימת

- לכל $a\in A$ מתקיים $(N(a)=0)\iff(a=0)$.
- לכל $a\in A$ ולכל $b\in A\backslash\{0\}$ המקיימים $a|b$ מתקיים $N(a)\leq N(b)$.
- לכל $a\in A$ ולכל $b\in A\backslash\{0\}$ קיימים $q,r\in A$ המקיימים $a=qb+r$ וכן $N(r)<N(b)$.

**טענה:** נגדיר $f:\mathbb{Z}\to\mathbb{N}$ כך $f(n)=|n|$ אזי $f$ הינה נורמה אוקלידית מעל $\mathbb{Z}$.

**טענה:** $N$ הינה נורמה אוקלידית מעל $\mathbb{Z}[i]$.

**טענה:** יהי $d\in\{2,-2,3\}$ אזי $|N|$ הינה נורמה אוקלידית מעל $\mathbb{Z}\left[\sqrt{d}\right]$.

**תחום אוקלידי:** תחום שלמות $A$ עבורו קיימת נורמה אוקלידית $N:A\to\mathbb{N}$.

**טענה:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי קיים $d\in A$ עבורו $dA=aA+bA$.

**טענה:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי $(a\sim b)\iff(aA=bA)$.

**סימון:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי $\text{Gcd}(a,b)=\{d\in A\mid dA=aA+bA\}$.

**מחלק משותף מירבי:** יהי $A$ תחום אוקלידי אזי $\gcd:A^2\to A$ המקיימת $\gcd(a,b)\in\text{Gcd}(a,b)$.

**סימון:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי $(a,b)=\gcd(a,b)$.

**טענה:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי $\gcd(a,b)|a$ וכן $\gcd(a,b)|b$.

**מסקנה:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי קיימים $n,m\in A$ עבורם $\gcd(a,b)=na+mb$.

**טענה:** יהי $A$ תחום אוקלידי ויהיו $a,b,c\in A$ באשר $c|a$ וכן $c|b$ אזי $c|\gcd(a,b)$.

**איבר אי־פריק:** יהי $A$ תחום שלמות אזי $\rho\in A\backslash\left(A^{\times}\cup\{0\}\right)$ עבורו לכל $a,b\in A$ המקיימים $\rho=ab$ מתקיים $(a\in A^{\times})\vee(b\in A^{\times})$.

**איבר ראשוני:** יהי $A$ תחום שלמות אזי $p\in A\backslash\left(A^{\times}\cup\{0\}\right)$ עבורו לכל $a,b\in A$ המקיימים $p|ab$ מתקיים $(p|a)\vee(p|b)$.

**טענה:** יהי $A$ תחום אוקלידי ויהי $a\in A$ אזי ($a$ אי־פריק)$\Longleftrightarrow$($a$ ראשוני).

**תחום בעל פריקות יחידה לראשוניים:** תחום שלמות $A$ המקיים

- לכל $a\in A\backslash\{0\}$ קיים $k\in\mathbb{N}_{+}$ וקיימים $p_1\ldots p_k\in A$ ראשוניים עבורם $a\sim\prod_{i=1}^{k}p_i$.
- לכל $k,\ell\in\mathbb{N}_{+}$ ולכל $p_1\ldots p_k,q_1\ldots q_\ell\in A$ ראשוניים באשר $\prod_{i=1}^{k}p_i\sim\prod_{i=1}^{\ell}q_i$ מתקיים $k=\ell$ וכן קיימת $\sigma\in S_k$ עבורה $p_i\sim q_{\sigma(i)}$ לכל $i\in[k]$.

**למה:** יהי $A$ תחום אוקלידי ויהיו $p,q\in A$ באשר $p\sim q$ אזי

- ($p$ ראשוני)$\Longleftrightarrow$($q$ ראשוני).
- ($p$ אי־פריק)$\Longleftrightarrow$($q$ אי־פריק).

**למה:** יהי $A$ תחום אוקלידי ויהיו $a,b\in A$ אזי $((N(a)=N(b))\wedge(a|b))\iff(a\sim b)$.

**משפט:** יהי $A$ תחום אוקלידי אזי $A$ תחום בעל פריקות יחידה לראשוניים.

**מסקנה:** $\mathbb{Z}[i]$ הינו תחום בעל פריקות יחידה לראשוניים.

**משפט:** אם GRH אז לכל $d\in\mathbb{Z}$ באשר $d\neq\square$ מתקיים ($\mathbb{Z}\left[\sqrt{d}\right]$ תחום בעל פריקות יחידה לראשוניים)$\Longleftrightarrow$($\mathbb{Z}\left[\sqrt{d}\right]$ תחום אוקלידי).

לא הוכח בקורס

**מודולו:** יהי $A$ חוג ויהי $a,n\in A$ אזי $(a\mod n)=a+nA$.

**איברים שקולים תחת מודולו:** יהי $A$ חוג ויהי $n\in A$ אזי $a,b\in A$ עבורם $(a\mod n)=(b\mod n)$.

**סימון:** יהי $A$ חוג יהי $n\in A$ ויהיו $a,b\in A$ שקולים מודולו $n$ אזי $a\equiv b\mod n$.

**טענה:** יהי $A$ חוג ויהיו $n,a,b\in A$ אזי $(a\equiv b\mod n)\iff(n|(a-b))$.

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

**הגדרה:** יהי $A$ חוג יהי $n\in A$ ויהיו $a,b\in A$ אזי $(a\mod n)+(b\mod n)=((a+b)\mod n)$.

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

**הגדרה:** יהי $A$ חוג יהי $n\in A$ ויהיו $a,b\in A$ אזי $(a\mod n)\cdot(b\mod n)=((a\cdot b)\mod n)$.

**טענה:** יהי $A$ חוג ויהי $n\in A$ אזי ${}^{A}/_{nA}$ חוג.

**חוג השאריות מודולו:** יהי $A$ חוג ויהי $n\in A$ אזי ${}^{A}/_{nA}$.

**טענה:** יהי $A$ תחום אוקלידי ויהי $n\in A\backslash\{0\}$ אזי (${}^{A}/_{nA}$ שדה)$\Longleftrightarrow$($n$ ראשוני).

**סימון:** יהי $A$ תחום שלמות אזי $\mathbb{P}_A=\{a\in A\mid A\text{ ראשוני מעל } a\}$.

**טענה:** $\left\{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid 0\in\{\mathrm{Re}(\pi),\mathrm{Im}(\pi)\}\right\}=\{p\in\mathbb{P}\mid p\equiv3\mod 4\}\cdot\mathbb{Z}[i]^{\times}$.

**למה:** יהי $\pi\in\mathbb{P}_{\mathbb{Z}[i]}$ אזי $\overline{\pi}\in\mathbb{P}_{\mathbb{Z}[i]}$.

**טענה:** $N\left(\left\{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid(0\notin\{\mathrm{Re}(\pi),\mathrm{Im}(\pi)\})\wedge(\pi\not\sim1+i)\right\}\right)=\{p\in\mathbb{P}\mid p\equiv1\mod 4\}$.

**מסקנה:** יהי $p\in\mathbb{P}$ באשר $p\equiv1\mod 4$ אזי קיימים $a,b\in\mathbb{Z}$ עבורם $p=a^2+b^2$.

**אלגוריתם ראשוני כסכום ריבועיים:** יהי $p\in\mathbb{P}$ באשר $p\equiv1\mod 4$ אזי

**Algorithm** SumSquaresPrime($p$):
- $c\leftarrow\mathrm{QNR}_p$
- $t\leftarrow c^{\frac{p-1}{4}}\mod p$
- $a+ib\leftarrow\mathrm{EuclidGCD}_{\mathbb{Z}[i]}(p,t+i)$
- **return** $(a,b)$

**טענה:** יהי $p\in\mathbb{P}$ באשר $p\equiv1\mod 4$ אזי $\mathrm{SumSquaresPrime}(p)\in\mathbb{Z}^2$ וכן $\sum_{i=1}^{2}(\mathrm{SumSquaresPrime}(p))_i^2=p$.

**טענה:** $\left\{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid\pi\sim1+i\right\}=\{\pi\in\mathbb{Z}[i]\mid\pi\sim1+i\}$.

**משפט:** יהי $n\in\mathbb{N}$ אזי (קיימים $a,b\in\mathbb{Z}$ עבורם $n=a^2+b^2$)$\iff$(קיימים $k,r,s\in\mathbb{N}$ קיימים $p_1\dots p_r,q_1\dots q_s\in\mathbb{P}$ שונים באשר $p_i\equiv1\mod4$ וכן $q_j\equiv3\mod4$ וקיימים $e_1\dots e_r,f_1\dots f_s\in\mathbb{N}_+$ עבורם $n=2^k\cdot\prod_{i=1}^r p_i^{e_i}\cdot\prod_{i=1}^s q_i^{2f_i}$).

**טענה:** יהי $\alpha\in\mathbb{Z}[i]$ אזי $\mathbb{N}_{<\frac{a^2+b^2}{\gcd_{\mathbb{N}}(a,b)}}+i\cdot\mathbb{N}_{<\gcd_{\mathbb{N}}(a,b)}$ מערכת נציגים של $\mathbb{Z}[i]/\alpha\mathbb{Z}[i]$.

**מסקנה:** יהי $\alpha\in\mathbb{Z}[i]$ אזי $\left|\mathbb{Z}[i]/\alpha\mathbb{Z}[i]\right|=N(\alpha)$.

**טענה:** יהי $d\in\mathbb{Z}$ באשר $d\neq\square$ ויהי $\alpha\in\mathbb{Z}\left[\sqrt{d}\right]$ אזי $\left|\mathbb{Z}[\sqrt{d}]/\alpha\mathbb{Z}[\sqrt{d}]\right|=|N(\alpha)|$.

**מסקנה משפט פרמה ב־$\mathbb{Z}[i]$:** יהי $p\in\mathbb{P}$ באשר $p\equiv3\mod4$ ויהי $\alpha\in\mathbb{Z}[i]$ אזי $\alpha^{p^2-1}\equiv1\mod p$.

**פולינום:** יהי $\mathbb{F}$ שדה אזי $f:\mathbb{F}\to\mathbb{F}$ עבורה קיים $n\in\mathbb{N}$ וקיים $\zeta\in\mathbb{F}^{n+1}$ המקיים $\zeta_{n+1}\neq0$ וכן $f=\sum_{i=0}^n\zeta_{i+1}x^i$.

**חוג הפולינומים:** יהי $\mathbb{F}$ שדה אזי $\mathbb{F}[x]=\{f:\mathbb{F}\to\mathbb{F}\mid \text{פולינום } f\}$.

**טענה:** יהי $\mathbb{F}$ שדה אזי $\mathbb{F}[x]$ הינו חוג אבלי בעל יחידה.

**הערה:** יהי $\mathbb{F}$ אזי נשכן $\mathbb{F}\hookrightarrow\mathbb{F}[x]$ כך $\alpha\mapsto\lambda x.\alpha$.

**מעלה של פולינום:** יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}$ ויהי $\zeta\in\mathbb{F}^{n+1}$ באשר $\zeta_{n+1}\neq0$ אזי $\deg\left(\sum_{i=0}^n\zeta_{i+1}x^i\right)=n$.

**הגדרה:** יהי $\mathbb{F}$ שדה אזי $\deg(0)=-\infty$.

**המקדם המוביל:** יהי $\mathbb{F}$ שדה יהי $n\in\mathbb{N}$ ויהי $\zeta\in\mathbb{F}^{n+1}$ באשר $\zeta_{n+1}\neq0$ אזי $\operatorname{lc}\left(\sum_{i=0}^n\zeta_{i+1}x^i\right)=\zeta_{i+1}$.

**הגדרה:** יהי $\mathbb{F}$ שדה אזי $\operatorname{lc}(0)=0$.

**טענה:** יהי $\mathbb{F}$ שדה ויהיו $f,g\in\mathbb{F}[x]$ אזי $\deg(fg)=\deg(f)+\deg(g)$ וכן $\operatorname{lc}(fg)=\operatorname{lc}(f)\operatorname{lc}(g)$.

**טענה:** יהי $\mathbb{F}$ שדה אזי $\mathbb{F}[x]^\times=\mathbb{F}\backslash\{0\}$.

**מסקנה:** יהי $\mathbb{F}$ שדה ויהיו $f,g\in\mathbb{F}[x]$ אזי $(f\sim g)\iff(\exists c\in\mathbb{F}.f=cg)$.

**פולינום מתוקן:** יהי $\mathbb{F}$ שדה אזי $f\in\mathbb{F}[x]$ המקיים $\operatorname{lc}(f)=1$.

**טענה:** יהי $\mathbb{F}$ שדה אזי $\{f\in\mathbb{F}[x]\mid \text{מתוקן } f\}\cup\{0\}$ מערכת נציגים של $\mathbb{F}[x]/\sim$.

**טענה:** יהי $\mathbb{F}$ שדה יהי $f\in\mathbb{F}[x]$ ויהי $g\in\mathbb{F}[x]\setminus\{0\}$ אזי קיימים ויחידים $q,r\in\mathbb{F}[x]$ המקיימים $\deg(r)<\deg(r)$ וכן $f=qg+r$.

**מסקנה:** יהי $\mathbb{F}$ שדה ויהי $f\in\mathbb{F}[x]$ אזי $\{r\in\mathbb{F}[x]\mid\deg(r)<\deg(f)\}$ מערכת נציגים של $\mathbb{F}[x]/f\mathbb{F}[x]$.

**מסקנה:** יהי $\mathbb{F}$ שדה יהי $C\in\mathbb{N}_{\geq2}$ ונגדיר $F:\mathbb{F}[x]\to\mathbb{N}$ כך $F(f)=\begin{cases}0 & f=0\\ C^{\deg(f)} & \text{else}\end{cases}$ אזי $F$ הינה נורמה אוקלידית מעל $\mathbb{F}[x]$.

**מסקנה:** יהי $\mathbb{F}$ שדה אזי $\mathbb{F}[x]$ תחום אוקלידי.

**מחלק משותף מקסימלי בחוג הפולינומים:** יהי $\mathbb{F}$ שדה אזי נגדיר $\gcd:\mathbb{F}[x]^2\to\mathbb{F}[x]$ כך $\gcd(f,g)=d$ באשר $d\in\operatorname{Gcd}(f,g)$ מתוקן.

**נגזרת:** יהי $\mathbb{F}$ שדה אזי נגדיר $\mathcal{D}:\mathbb{F}[x]\to\mathbb{F}[x]$ כך $\mathcal{D}\left(\sum_{i=0}^n\zeta_ix^i\right)=\sum_{i=1}^n i\zeta_ix^{i-1}$.

**סימון:** יהי $\mathbb{F}$ שדה ויהי $f\in\mathbb{F}[x]$ אזי $f'=D(f)$.

**טענה:** יהי $\mathbb{F}$ שדה יהיו $f,g\in\mathbb{F}[x]$ ויהי $c\in\mathbb{F}$ אזי

- $(f+g)'=f'+g'$ וכן $(f-g)'=f'-g'$.
- $(fg)'=f'g+fg'$.
- $c'=0$ וכן $(cf)'=cf'$.

**פולינום חסר ריבועים:** יהי $\mathbb{F}$ שדה אזי $f\in\mathbb{F}[x]$ עבורו לכל $p\in\mathbb{P}_{\mathbb{F}[x]}$ מתקיים $p^2\nmid f$.

**טענה קריטריון הנגזרת:** יהי $\mathbb{F}$ שדה ויהי $f\in\mathbb{F}[x]$ המקיים $\gcd(f,f')=1$ אזי $f$ חסר ריבועים.

**השערה:** $\{\langle n\rangle\mid(n\in\mathbb{N})\wedge(\text{מספר חסר ריבועים } n)\}\in\mathcal{P}$. השערה פתוחה

**משפט המשפט האחרון של פרמה לפולינומים:** יהי $n\in\mathbb{N}$ יהי $\mathbb{F}$ שדה ויהיו $a,b,c\in\mathbb{F}[x]\backslash\mathbb{F}$ באשר $a^n+b^n=c^n$ אזי $n\in\{1,2\}$.

**מינימום דיפולטי:** תהא $X$ קבוצה ויהי $\prec$ יחס סדר טוב על $X$ אזי נגדיר $\operatorname{mindef}:X\times\mathcal{P}(X)\to X$ כך

- לכל $x\in X$ מתקיים $\operatorname{mindef}(x,\varnothing)=x$.
- לכל $x\in X$ ולכל $A\in\mathcal{P}(X)\setminus\{\varnothing\}$ מתקיים $\operatorname{mindef}(x,A)=\min(A)$.

**מציין של שדה:** יהי $\mathbb{F}$ שדה אזי $\operatorname{char}(\mathbb{F})=\operatorname{mindef}(0,\{n\in\mathbb{N}_+\mid n\cdot1_{\mathbb{F}}=0\})$.

**טענה:** יהי $\mathbb{F}$ שדה באשר $\operatorname{char}(\mathbb{F})\neq0$ אזי $\operatorname{char}(\mathbb{F})\in\mathbb{P}$.

**טענה:** יהי $p\in\mathbb{P}$ יהי $\mathbb{F}$ שדה באשר $\operatorname{char}(\mathbb{F})=p$ ונגדיר $\varphi:\mathbb{Z}/p\mathbb{Z}\to\mathbb{F}$ כך $\varphi(n\mod p)=n\cdot1_{\mathbb{F}}$ אזי $\varphi$ מונומורפיזם שדות.

**סימון:** יהי $p\in\mathbb{P}$ אזי $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

**הערה:** יהי $p\in\mathbb{P}$ ויהי $\mathbb{F}$ באשר $\operatorname{char}(\mathbb{F})=p$ אזי נשכן $\mathbb{F}_p\hookrightarrow\mathbb{F}$ כך $(n\mod p)\mapsto n\cdot1_{\mathbb{F}}$.

**טענה:** יהי $\mathbb{F}$ שדה סופי אזי $\operatorname{char}(\mathbb{F})\in\mathbb{P}$.

**טענה:** יהי $\mathbb{F}$ שדה סופי אזי $\mathbb{F}$ מרחב וקטורי מעל $\mathbb{F}_p$.

**מסקנה:** יהי $\mathbb{F}$ שדה סופי אזי $|\mathbb{F}| \in \{p^n \mid (p \in \mathbb{P}) \wedge (n \in \mathbb{N})\}$.

**מסקנה משפט פרמה בשדות סופיים:** יהי $\mathbb{F}$ שדה סופי ויהי $a \in \mathbb{F}$ אזי $a^{|\mathbb{F}|} = a$.

**מסקנה:** יהי $\mathbb{F}$ שדה סופי אזי $\mathbb{F}^\times$ ציקלית.

**משפט:** יהי $p \in \mathbb{P}$ ויהי $n \in \mathbb{N}_+$ אזי קיים שדה $\mathbb{F}$ המקיים $|\mathbb{F}| = p^n$.

**משפט:** יהי $p \in \mathbb{P}$ יהי $n \in \mathbb{N}_+$ יהי $\mathbb{F}$ שדה באשר $|\mathbb{F}| = p^n$ ויהי $f \in \mathbb{F}[x]$ ראשוני באשר $\deg(f) = n$ אזי $\mathbb{F} \simeq {}^{\mathbb{F}[x]}/_{f \cdot \mathbb{F}[x]}$.

**מסקנה:** יהי $p \in \mathbb{P}$ יהי $n \in \mathbb{N}_+$ ויהיו $\mathbb{F}, \mathbb{K}$ שדות באשר $|\mathbb{F}| = p^n$ וכן $|\mathbb{K}| = p^n$ אזי $\mathbb{F} \simeq \mathbb{K}$.

**סימון:** יהי $p \in \mathbb{P}$ ויהי $n \in \mathbb{N}_+$ אזי $\mathbb{F}_{p^n}$ שדה המקיים $|\mathbb{F}_{p^n}| = p^n$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $f \in \mathbb{F}_q[x]$ ראשוני אזי ${}^{\mathbb{F}_q[x]}/_{f \cdot \mathbb{F}_q[x]}$ שדה וכן $\left|{}^{\mathbb{F}_q[x]}/_{f \cdot \mathbb{F}_q[x]}\right| = q^{\deg(f)}$.

**גודל של פולינום:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה אזי נגדיר $|\cdot| : \mathbb{F}_q[x] \to \mathbb{N}$ כך $|f| = q^{\deg(f)}$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה אזי $|\cdot|$ הינה נורמה אוקלידית מעל $\mathbb{F}_q[x]$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $f \in \mathbb{F}_q[x]$ אזי $|f| = \left|{}^{\mathbb{F}_q[x]}/_{f \cdot \mathbb{F}_q[x]}\right|$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $f, g \in \mathbb{F}_q[x]$ אזי $|f \cdot g| = |f| \cdot |g|$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ אזי $x^{q^n} - x$ חסר ריבועים מעל $\mathbb{F}_q[x]$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהיו $n, m \in \mathbb{N}_+$ אזי $\gcd\left(x^{q^n} - x, x^{q^m} - x\right) = x^{q^{\gcd(n,m)}} - x$ מעל $\mathbb{F}_q[x]$.

**מורפיזם פרובניוס:** יהי $p \in \mathbb{P}$ ויהי $\mathbb{K}$ שדה המקיים $\text{char}(\mathbb{K}) = p$ אזי נגדיר $\text{Fr}_p : \mathbb{K} \to \mathbb{K}$ כך $\text{Fr}_p(a) = a^p$.

**טענה זהות פרובניוס:** יהי $p \in \mathbb{P}$ ויהי $\mathbb{K}$ שדה סופי באשר $\text{char}(\mathbb{K}) = p$ אזי $\text{Fr}_p$ אוטומורפיזם של $\mathbb{K}$.

**מסקנה:** יהי $p \in \mathbb{P}$ יהי $\mathbb{F}$ שדה באשר $\text{char}(\mathbb{F}) = p$ יהי $f \in \mathbb{F}[x]$ ויהי $n \in \mathbb{N}_+$ אזי $g(x)^{p^n} = g\left(x^{p^n}\right)$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ ויהי $P \in \mathbb{F}_q[x]$ ראשוני אזי $(\deg(P) | n) \iff \left(P | \left(x^{q^n} - x\right)\right)$.

**סימון:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $\mathcal{P}_{q,n} = \{f \in \mathbb{F}_q[x] \mid (\deg(f) = n) \wedge (\text{מתוקן וראשוני } f)\}$.

**הגדרה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה אזי נגדיר $\pi_q : \mathbb{N}_+ \to \mathbb{N}$ כך $\pi_q(n) = |\mathcal{P}_{q,n}|$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $x^{q^n} - x = \prod_{\substack{d \in \mathbb{N} \\ d | n}} \prod_{f \in \mathcal{P}_{q,d}} f$ מעל $\mathbb{F}_q[x]$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $q^n = \sum_{\substack{d \in \mathbb{N} \\ d | n}} (d \cdot \pi_q(d))$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $\pi_q(n) = \frac{1}{n}\left(q^n - \sum_{\substack{d \in \mathbb{N}_{<n} \\ d | n}} (d \cdot \pi_q(d))\right)$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $\frac{q^n}{n} - \frac{q}{q-1} \cdot \frac{q^{\left\lfloor \frac{n}{2} \right\rfloor}}{n} \leq \pi_q(n) \leq \frac{q^n}{n}$.

**מסקנה משפט הפולינומים הראשוניים:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה אזי $\pi_q(n) \sim \frac{q^n}{n}$.

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $\pi_q(n) > 0$.

**פונקציית מוביוס:** יהי $k \in \mathbb{N}$ יהיו $p_1 \ldots p_k \in \mathbb{P}$ שונים ויהי $e \in \mathbb{N}_+^k$ אזי נגדיר $\mu : \mathbb{N} \to \{0, \pm 1\}$ כך $\mu\left(\prod_{i=1}^k p_i^{e_i}\right) = \begin{cases} (-1)^k & e = \mathbb{1} \\ 0 & \text{else} \end{cases}$.

**טענה:** יהי $n \in \mathbb{N}_+$ אזי $\sum_{\substack{d \in \mathbb{N} \\ d | n}} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$.

**טענה נוסחת ההיפוך של מוביוס:** תהא $f : \mathbb{N}_+ \to \mathbb{C}$ ויהי $n \in \mathbb{N}_+$ אזי $f(n) = \sum_{\substack{d \in \mathbb{N} \\ d | n}} \left(\mu(d) \cdot \left(\sum_{\substack{a \in \mathbb{N} \\ a | \frac{n}{d}}} f(a)\right)\right)$.

**טענה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $n \in \mathbb{N}_+$ אזי $\pi_q(n) = \frac{1}{n} \sum_{\substack{d \in \mathbb{N} \\ d | n}} \left(\mu\left(\frac{n}{d}\right) \cdot q^d\right)$.

**למה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ ויהי $f \in \mathbb{F}_q[x]$ באשר $\deg(f) = n$ אזי ($f$ ראשוני)$\iff$($f | \left(x^{q^n} - x\right)$ וכן לכל $\ell \in \mathbb{N}_{<n}$ מתקיים $\gcd\left(f, x^{q^\ell} - x\right) = 1$).

**אלגוריתם מבחן ראשוניות לפולינום:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ יהי $f \in \mathbb{F}_q[x]$ באשר $\deg(f) = n$ יהי $\mathcal{A}$ אלגוריתם חזקה מעל ${}^{\mathbb{F}_q[x]}/_{f \cdot \mathbb{F}_q[n]}$ ויהי $\mathcal{B}$ אלגוריתם gcd מעל $\mathbb{F}_q[x]$ אזי

**מסקנה:** יהי $q \in \mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $n \in \mathbb{N}_+$ ויהי $f \in \mathbb{F}_q[x]$ באשר $\deg(f) = n$ אזי ($f$ ראשוני)$\iff$($\text{PolynomialPrimality}(q, n, f) = \text{True}$).

**טענה:** סיבוכיות הריצה של $\text{PolynomialPrimality}[\text{IteratedSquaring}[\text{NaiveMul}], \text{EuclidGCD}]$ הינה $\mathcal{O}\left((n \cdot \log(q))^3\right)$.

**טענה:** סיבוכיות הריצה של $\text{PolynomialPrimality}[\text{IteratedSquaring}[\text{CooleyTukeyMul}], \text{FastGCD}]$ הינה $\tilde{\mathcal{O}}\left((n \cdot \log(q))^2\right)$.

**למה:** יהי $p \in \mathbb{P}$ יהי $r \in \mathbb{N}_+$ ויהי $g \in \mathbb{F}_{p^r}[x]$ אזי $(g' = 0) \iff (\exists h \in \mathbb{F}_{p^r}[x] . g = h^p)$.

**אלגוריתם שורש מעל שדה סופי:** יהי $p \in \mathbb{P}$ יהי $r \in \mathbb{N}_+$ יהי $a \in \mathbb{F}_{p^r}$ ויהי $\mathcal{A}$ אלגוריתם חזקה מעל $\mathbb{F}_{p^r}$ אזי $\text{FiniteFieldRoot}[\mathcal{A}](p, r, a) = \mathcal{A}\left(a, p^{r-1}\right)$.

```
Algorithm PolynomialPrimality[𝒜, ℬ](q, n, f):
    L ∈ (𝔽_q[x]/f·𝔽_q[x])^n ;      L_1 ← (x^q mod f)
    for i ∈ [2, ..., n] do
        L_i ← 𝒜(f, L_{i−1}, q)
    end
    if L_n ≠ (x mod f) then return False
    for d ∈ [1, ..., n − 1] do
        if ℬ(L_d − x, f) ≠ 1 then return False
    end
    return True
```

**טענה:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ יהי $a\in\mathbb{F}_{p^r}$ אזי $\sqrt[p]{a}=\mathrm{FiniteFieldRoot}\left(p,r,a\right)$.

**אלגוריתם שורש לפולינום:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ יהי $n\in\mathbb{N}_+$ ויהיו $a_0,\ldots,a_n\in\mathbb{F}_{p^r}$ באשר $\left(\sum_{i=0}^{n}a_ix^i\right)'=0$ ויהי $\mathcal{A}$ אלגוריתם חזקה מעל $\mathbb{F}_{p^r}$ אזי $\mathrm{FiniteFieldPolynomialRoot}\left[\mathcal{A}\right]\left(p,r,a\right)=\sum_{i=0}^{\frac{n}{p}}\mathrm{FiniteFieldRoot}\left[\mathcal{A}\right]\left(a_{pi}\right)x^i$.

**טענה:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ ויהי $f\in\mathbb{F}_{p^r}\left[x\right]$ אזי $\sqrt[p]{f}=\mathrm{FiniteFieldPolynomialRoot}\left(p,r,f\right)$.

**למה:** יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה ויהי $f\in\mathbb{F}_q\left[x\right]$ אזי $\left(\gcd\left(f,f'\right)=1\right)\Longleftrightarrow\left(f\right.$ חסר ריבועים$\left.\right)$.

**אלגוריתם פירוק פולינום לפולינומים חסרי ריבועים:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ יהי $f\in\mathbb{F}_{p^r}\left[x\right]$ יהי $\mathcal{A}$ אלגוריתם gcd מעל $\mathbb{F}_{p^r}\left[x\right]$ ויהי $\mathcal{B}$ אלגוריתם חזקה מעל $\mathbb{F}_{p^r}$ אזי

```
Algorithm PolyFactorNoSquare[𝒜, ℬ](p, r, f):
    G ← 𝒜(f, f′)
    if G = 1 then return {(f, 1)}
    if f′ ≠ 0 then
        A ← PolyFactorNoSquare[𝒜, ℬ](p, r, G)
        B ← PolyFactorNoSquare[𝒜, ℬ](p, r, f/G)
        return A + B
    end
    g ← FiniteFieldPolynomialRoot[ℬ](p, r, f)
    S ← PolyFactorNoSquare[𝒜, ℬ](p, r, g)
    return {(q, n + p) | (q, n) ∈ S}
```

**טענה:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ ויהי $f\in\mathbb{F}_{p^r}\left[x\right]$ אזי

- $\prod\mathrm{PolyFactorNoSquare}\left(p,r,f\right)=f$.
- לכל $q\in\mathrm{PolyFactorNoSquare}\left(p,r,f\right)$ מתקיים $q$ חסר ריבועים.

**אלגוריתם פירוק פולינום חסר ריבועים לפולינומים בעלי פירוק לראשוניים בעלי אותה דרגה:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ יהי $f\in\mathbb{F}_{p^r}\left[x\right]$ חסר ריבועים יהי $\mathcal{A}$ אלגוריתם gcd מעל $\mathbb{F}_{p^r}\left[x\right]$ ויהי $\mathcal{B}$ אלגוריתם חזקה מעל $\mathbb{F}_{p^r}\left[x\right]$ אזי

```
Algorithm PolyFactorSameDeg[𝒜, ℬ](p, r, f):
    S ← ∅
    for d ∈ [1, ..., deg(f)] do
        f_d ← 𝒜(ℬ(x, q^d) − x, f)
        if f_d ≠ 1 then S ← S ∪ {f_d}
    end
    return S
```

**פונקציית חזקה:** נגדיר $\mathrm{power}:R\times\mathbb{N}\to R$ כך $\mathrm{power}\left(r,n\right)=r^n$.

**טענה:** יהי $p\in\mathbb{P}$ יהי $r\in\mathbb{N}_+$ ויהי $f\in\mathbb{F}_{p^r}\left[x\right]$ חסר ריבועים אזי

- $\left(\prod\mathrm{power}\left(\mathrm{PolyFactorSameDeg}\left(p,r,f\right)\right)\right)|f$.
- לכל $\left(f_d,n\right)\in\mathrm{PolyFactorSameDeg}\left(p,r,f\right)$ ולכל $Q\in\mathbb{F}_{p^r}\left[x\right]$ ראשוני המקיים $Q|f_d$ מתקיים $\deg\left(Q\right)=d$.

**למה:** יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $d\in\mathbb{N}_+$ ויהי $a\in\mathbb{F}_{q^d}$ אזי

- אם $2\nmid q$ אז $x^{q^d}-x=\left(x+a\right)\left(\left(x+a\right)^{\frac{q^d-1}{2}}+1\right)\left(\left(x+a\right)^{\frac{q^d-1}{2}}-1\right)$ מעל $\mathbb{F}_q\left[x\right]$.

• אם $2|q$ אז $x^{q^d}-x=\left(\sum_{i=1}^{d\cdot\log_2(q)}(x+a)^{\frac{q^d}{2^i}}\right)\left(\left(\sum_{i=1}^{d\cdot\log_2(q)}(x+a)^{\frac{q^d}{2^i}}\right)+1\right)$ מעל $\mathbb{F}_q[x]$.

**אלגוריתם מציאת שורש של פולינום חסר ריבועים בעל פירוק לראשוניים בעלי אותה דרגה:** יהי $p\in\mathbb{P}$ יהיו $r,d\in\mathbb{N}_+$ יהי $f\in\mathbb{F}_{p^r}[x]$ חסר ריבועים עבורו לכל $Q\in\mathbb{F}_{p^r}[x]$ ראשוני המקיים $Q|f$ מתקיים $\deg(Q)=d$ יהי $\mathcal{A}$ אלגוריתם gcd מעל $\mathbb{F}_{(p^r)^d}[x]$ ויהי $R:\mathbb{N}\to\mathbb{F}_{(p^r)^d}$ אזי

```
Algorithm PolySameDegSol[𝒜](p, r, f, d; R):
    a ← R(0)
    if f(a) = 0 then return a
    if p = 2 then
        F ← (Σ_{i=1}^{rd} (x+a)^{2^{rd−i}}) mod f        // Can be computed quickly using IteratedSquaring
    else
        F ← ((x+a)^{(p^{rd}−1)/2} − 1) mod f             // Can be computed quickly using IteratedSquaring
    g ← 𝒜(f, F)
    if g ∈ {1, f} then return ∅
    return PolySameDegSol[𝒜](p, r, g, d; R↾ℕ₊)
```

**טענה:** יהי $p\in\mathbb{P}$ יהיו $r,d\in\mathbb{N}_+$ ויהי $f\in\mathbb{F}_{p^r}[x]$ חסר ריבועים עבורו לכל $Q\in\mathbb{F}_{p^r}[x]$ ראשוני המקיים $Q|f$ מתקיים $\deg(Q)=d$ אזי $\mathbb{P}_R\left(\text{PolySameDegSol}(p,r,f,d;r)\in\text{sols}_{\mathbb{F}_{(p^r)^d}}(f)\right)\ge\frac{1}{3^d}$.

**למה:** יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה יהי $d\in\mathbb{N}_+$ יהי $a\in\mathbb{F}_{q^d}$ באשר $f(a)=0$ ונגדיר $P\in\mathbb{F}_{q^d}[x]$ כך $P=\prod_{i=1}^{d}\left(x-a^{q^i}\right)$ אזי $P\in\mathbb{F}_q[x]$ וכן $P$ ראשוני מעל $\mathbb{F}_q[x]$ וכן $P|f$.

**אלגוריתם פירוק פולינום חסר ריבועים בעל פירוק לראשוניים בעלי אותה דרגה:** יהי $p\in\mathbb{P}$ יהיו $r,d\in\mathbb{N}_+$ יהי $f\in\mathbb{F}_{p^r}[x]$ חסר ריבועים עבורו לכל $Q\in\mathbb{F}_{p^r}[x]$ ראשוני המקיים $Q|f$ מתקיים $\deg(Q)=d$ יהי $\mathcal{A}$ אלגוריתם gcd מעל $\mathbb{F}_{(p^r)^d}[x]$ ויהי $R:\mathbb{N}\to\mathbb{F}_{(p^r)^d}$ אזי

```
Algorithm PolySameDegFactor[𝒜](p, r, f, d; R):
    a ∈ 𝔽_{(p^r)^d}
    while f(a) ≠ 0 do
        a ← PolySameDegSol(p, r, f, d; R)
        R ← R↾ℕ_{>deg(f)}
    end
    Q ← Π_{i=1}^{d} (x − a^{(p^r)^i})                     // Can be computed quickly using IteratedSquaring
    return [Q] ∥ PolySameDegFactor[𝒜](p, r, f/Q, d; R)
```

**מסקנה:** יהי $q\in\mathbb{N}$ באשר $\mathbb{F}_q$ שדה אזי קיים אלגוריתם $\mathcal{A}$ הסתברותי פולינומי לפירוק פולינומים לראשוניים מעל $\mathbb{F}_q[x]$.