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

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

מנה של חלוקה: יהי $d\in\mathbb{N}_+$ 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 $(d|a)\Longleftrightarrow(r=0)$.

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 $\mathcal{A}$ המחשב כפל מספרים בסיבוכיות ריצה $\mathcal{O}\left(n^2\right)$.

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

```
Algorithm KaratsubaMult(a, b):
    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 $\mathcal{A}$ המחשב כפל מספרים בסיבוכיות ריצה $\mathcal{O}(n \log(n))$.

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

אלגוריתם אוקלידס: יהיו $a, b \in \mathbb{Z}$ אזי

```
Algorithm EuclidGCD(a, b):
    if (a < 0) ∨ (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 $\mathcal{O}\left(n^2\right)$.

טענה: יהי $k \in \mathbb{N}_+$ אזי $(-1)^k F_{k-1} \cdot F_{k+1} + (-1)^{k+1} F_k F_k = 1$.

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

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 $a_1 \ldots a_n \in \mathbb{Z} \backslash \{0\}$ 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 $\left(\frac{b}{a} \in \mathbb{Z}\right) \Longleftrightarrow (a|b)$.

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

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

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

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

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

טענה: יהיו $a_1\ldots a_n\in\mathbb{Z}$ אזי $[a_1\ldots a_n]=[[a_1\ldots a_{n-1}],a_n]$.

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

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

מספר פריק: מספר $m\in\mathbb{N}_{\geq 2}$ באשר $m\notin\mathbb{P}$.

טענה: יהי $p\in\mathbb{P}$ ויהיו $a,b\in\mathbb{Z}$ באשר $p|ab$ אזי $(p|a)\vee(p|b)$.

טענה: יהי $n\in\mathbb{N}$ עבורו לכל $a,b\in\mathbb{Z}$ אם $n|ab$ אז $(n|a)\vee(n|b)$ אזי $n\in\{0,\pm1\}\cup(\pm\mathbb{P})$.

מסקנה: יהי $p\in\mathbb{P}$ ויהיו $a_1\ldots a_n\in\mathbb{Z}$ 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 + 2j ≤ N do
                A_{i+2j} = 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־ברנסטיין: קיים אלגוריתם $\mathcal{A}$ עבורו $\mathcal{A}(N)=\mathbb{P}_{\leq N}$ לכל $N\in\mathbb{N}_+$ וכן $\mathcal{A}$ רץ בסיבוכיות ריצה $\mathcal{O}(N)$.

משפט היסודי של האריתמטיקה: יהי $n\in\mathbb{N}_+$ אזי קיימים ויחידים $p_1\ldots p_k\in\mathbb{P}$ באשר $p_i<p_{i+1}$ לכל $i\in[k-1]$ המקיימים $n=\prod_{i=1}^{k}p_i$.

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

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

מסקנה: יהי $n\in\mathbb{N}_+$ אזי $n=\prod_{p\in\mathbb{P}}p^{e_p(n)}$.

מסקנה: יהיו $n,m\in\mathbb{N}_+$ ויהי $p\in\mathbb{P}$ אזי $e_p(mn)=e_p(m)+e_p(n)$.

מסקנה: יהיו $n,m\in\mathbb{N}_+$ אזי $(m|n)\iff(\forall p\in\mathbb{P}.e_p(m)\leq e_p(n))$.

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

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

מסקנה: יהיו $n,m\in\mathbb{N}_+$ אזי (m,n זרים)$\Longleftrightarrow$(לא קיים $p\in\mathbb{P}$ המקיים $p|m$ וכן $p|n$).

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

משפט אוקלידס: $|\mathbb{P}|=\aleph_0$.

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

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

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 $\pi(a)=r+n\mathbb{Z}$.

מודלו: 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 $a,b\in\mathbb{Z}$ עבורים $(a\mod n)=(b\mod n)$.

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 חילופי בעל יחידה.

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

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

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

```
Algorithm InverseMod(n, a):
    (b, c) ← ExtendedEuclidGCD(a, n)   // ba + cn = gcd(a, n)
    (q, r) ← 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 אויילר: 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 $\varphi\left(\prod_{i=1}^{k}p_i^{k_i}\right)=\prod_{i=1}^{k}\left(p_i^{e_i}-p_i^{e_i-1}\right)$.

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

משפט אויילר: יהי $n\in\mathbb{N}_{+}$ ויהי $a\in\mathbb{Z}$ באשר $(a,m)=1$ אזי $a^{\varphi(n)}\equiv1\mod n$.

משפט הקטן של פרמה: יהי $p\in\mathbb{P}$ ויהי $a\in\mathbb{Z}$ באשר $p\nmid a$ אזי $a^{p-1}\equiv1\mod p$.

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

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

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 $\sum_{\substack{k\in[n] \\ \gcd(k,n)=1}} k = \frac{1}{2} n \cdot \varphi(n)$.

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

מסקנה: יהי $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n 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 $\langle g \mod n \rangle = (\mathbb{Z}/n\mathbb{Z})^\times$.

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 $g^{\frac{e}{q}} \neq 1$).

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

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

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

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

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

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

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

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

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

שארית ריבועית: יהי $p\in\mathbb{P}$ אזי $a\in\mathbb{Z}$ המקיים $p\nmid a$ וכן קיים $x\in\mathbb{Z}$ עבורו $x^2\equiv a \mod p$.

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

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

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

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

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 $\left(\frac{-1}{p}\right)=\begin{cases}1 & p\equiv 1 \mod 4\\ -1 & p\equiv 3 \mod 4\end{cases}$.

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 $\left|\text{sols}\left(x^2=a\right)\right|=1+\left(\frac{a}{p}\right)$.

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

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

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

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 $\left(\frac{a}{p}\right)=(-1)^{\sum_{i=1}^{\lfloor\frac{a}{2}\rfloor}\left(\lfloor\frac{ip}{a}\rfloor-\lfloor\frac{(2i-1)p}{2a}\rfloor\right)}$.

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

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 $m\equiv a^2 \mod n$)$\iff$(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 $\text{JacobiSymbol}\left(m, n\right) = \left(\frac{m}{n}\right)$.

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

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

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

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

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

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

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

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

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$[\mathcal{A}](N;a)$:
  if $\mathcal{A}(N,a,N-1)=1$ **then** **return** True
  return False

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

טענה: סיבוכיות הריצה של FermatPrimalityTest [ModIteratedSquaring [CooleyTukeyMul]] 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: $|\{k\in\mathbb{N} \mid F_k \notin \mathbb{P}\}|=\aleph_0$. השערה פתוחה

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

טענה: יהי $N \in \mathbb{N}$ אזי (N קרמייקל)$\Longleftrightarrow$(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: $|\{k\in\mathbb{N} \mid 6k+1,12k+1,18k+1\in\mathbb{P}\}|=\aleph_0$. השערה פתוחה

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

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

משפט ארדוש: קיים $c \in \mathbb{R}_+$ עבורו החל ממקום מסויים לכל $x \in \mathbb{N}$ מתקיים
$|\{N<x \mid \text{מספר קרמייקל } N\}|<x\cdot\exp\left(\frac{-c\cdot\log(x)\cdot\log\log\log(x)}{\log\log(x)}\right)$.

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

Algorithm SolovayStrassenPrimalityTest$[\mathcal{A}](N;a)$:
  if $N=2$ **then return** True
  if $(N<2)\vee(2|N)$ **then return** False
  $s \leftarrow \text{JacobiSymbol}\left(a,N\right)$
  if $(s\neq 0)\wedge\left(\mathcal{A}\left(N,a,\frac{N-1}{2}\right)=\left(s \mod N\right)\right)$ **then**
    return True
  return False

טענה: סיבוכיות הריצה של SolovayStrassenPrimalityTest [ModIteratedSquaring [NaiveMul]] 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$[\mathcal{A}](N;a)$:
  if $N=2$ **then return** True
  if $(N<2)\vee(2\mid N)$ **then return** False
  $\alpha_0 \leftarrow \mathcal{A}(N,a,\frac{N-1}{2^{e_2(N-1)}})$
  for $i \in [1,\ldots,e_2(N-1)]$ **do**
    $\alpha_i \leftarrow \mathcal{A}(N,\alpha_{i-1},2)$
    if $\alpha_i=-1$ **then return** True
    if $\alpha_i\neq 1$ **then return** False
  end
  return True

טענה: סיבוכיות הריצה של MillerRabinPrimalityTest [ModIteratedSquaring [NaiveMul]] 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 $\mathbb{P}_r\left(\text{PrimeGenerator}\left(n,k;r\right) \in \mathbb{P}\right) \ge 1 - \frac{1}{4^k}$.

מספר מרסן: מספר $n \in \mathbb{N}$ עבורו קיים $p \in \mathbb{P}$ המקיים $n = 2^p - 1$.

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

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 $\left(\text{LucasLehmer}\left(n, 2^n - 1\right) = \text{True}\right) \iff \left(2^n - 1 \in \mathbb{P}\right)$.

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

טענה: סיבוכיות הריצה של $\text{LucasLehmer}\left[\text{TrialDivision}, \text{ModIteratedSquaring}\left[\text{CooleyTukeyMul}\right]\right]$ 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 $\tilde{\mathcal{O}}\left(n^\alpha\right) = \mathcal{O}\left(n^\alpha\right) \cdot \text{poly}\left(\log\left(n\right)\right)$.

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