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 $P(n+1)\Longrightarrow P(n)$ 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 $(a\in\{\pm b\})\Longleftrightarrow((a|b)\wedge(b|a))$.

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 $(d|a)\Longleftrightarrow(r=0)$.

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

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

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

Algorithm KaratsubaMult(a,b):

$\alpha\leftarrow(a_1\dots a_{\frac{n}{2}});\quad\beta\leftarrow(a_{\frac{n}{2}+1}\dots a_n)$

$\gamma\leftarrow(b_1\dots b_{\frac{n}{2}});\quad\delta\leftarrow(b_{\frac{n}{2}+1}\dots b_n)$

$A\leftarrow\texttt{KaratsubaMult}(\alpha,\gamma)$

$B\leftarrow\texttt{KaratsubaMult}(\beta,\delta)$

$C\leftarrow\texttt{KaratsubaMult}(\alpha+\beta,\gamma+\delta)$

return $B\cdot 2^n+(C-B-A)\cdot 2^{\frac{n}{2}}+A$

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

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 $(a<0)\vee(b<0)\vee(|a|<|b|)$ **then**

  return $\texttt{EuclidGCD}(\max\{|a|,|b|\},\min\{|a|,|b|\})$

if $b=0$ **then return** a

$(q,r)\leftarrow\text{RemainderDiv}(a,b)$

return $\texttt{EuclidGCD}(b,r)$

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 $(-1)^kF_{k-1}\cdot F_{k+1}+(-1)^{k+1}F_kF_k=1$.

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

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

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

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

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

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

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

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

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

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

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

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

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

טענה: יהיו $a_1\ldots a_n\in\mathbb{Z}$ 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: $\mathbb{P}=\{p\in\mathbb{N}\mid \text{ראשוני } p\}$.

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 $n\in\{0,\pm1\}\cup(\pm\mathbb{P})$.

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)$\iff$(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 $\{b+i\mid i\in\{0,\ldots,n\}\}\cap\mathbb{P}=\varnothing$.

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

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

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 $a,b\in\mathbb{Z}$ 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 $(a\equiv b \mod n)\Longleftrightarrow(n|(a-b))$.

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

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 $(2|a_0)\Longleftrightarrow(2|a)$.

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

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

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

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

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

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)$\Longleftrightarrow(n\in\mathbb{P})$.

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 $\left((a \mod n)\in(\mathbb{Z}/n\mathbb{Z})^\times\right)\Longleftrightarrow((a,n)=1)$.

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

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: φ 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 $k \in \mathbb{N}_+$ נגדיר $f : \mathbb{N}_+ \to \mathbb{R}$ 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: σ 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 $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $\{a \in G \mid G \text{ יוצר של } a\} = \{g^d | (d,n) = 1\}$.

מסקנה: יהי $n \in \mathbb{N}_+$ ותהא G חבורה ציקלית מסדר n אזי $|\{g^d | (d,n) = 1\}| = \varphi(n)$.

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

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

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

מסקנה: יהי $n \in \mathbb{N}_+$ אזי $\sum_{\substack{d\in\mathbb{N}_+ \\ d|n}} \varphi(d) = n$.

מסקנה: יהי $\mathbb{F}$ שדה ותהא $G \leq \mathbb{F}^\times$ סופית אזי G ציקלית.

שורש פרימיטיבי: יהי $n \in \mathbb{N}_+$ אזי $g \in \mathbb{Z}$ עבורו $(\mathbb{Z}/n\mathbb{Z})^\times = \langle g \mod n \rangle$.

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

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

טענה: יהי $k\in\mathbb{N}_{\ge2}$ ויהי $a\in\mathbb{Z}_{\text{odd}}$ אזי קיימים ויחידים $\alpha\in\{0,1\}$ וכן $\beta\in\left\{0,\dots,2^{k-2}\right\}$ עבורם $a\equiv(-1)^\alpha 5^\beta \mod 2^k$.

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

משפט: יהי $n\in\mathbb{N}_+$ ויהיו $k,m\in\mathbb{N}$ ויהיו $e_1,\dots,e_m\in\mathbb{N}_+$ 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 $k\le1$ 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 $p\in\mathbb{P}_{>2}$ יהי $a\in\mathbb{Z}$ 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 $p_1\dots p_k\in\mathbb{P}_{>2}$ 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 $p_1\dots p_k\in\mathbb{P}_{>2}$ ויהי $a\in\mathbb{Z}$ אזי $\left(\frac{a}{\prod_{i=1}^k p_i}\right)=\prod_{i=1}^k\left(\frac{a}{p_i}\right)$.

טענה: יהי $n\in\mathbb{N}_{\text{odd}}$ ויהיו $m,k\in\mathbb{Z}$ באשר $m\equiv k \mod n$ 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: יהי $n,m\in\mathbb{N}_{\text{odd}}$ 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 $\left(\frac{-1}{n}\right)=\begin{cases}1 & n\equiv1\mod4\\-1 & n\equiv3\mod4\end{cases}$.

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 $\left(\frac{2}{n}\right)=\begin{cases}1 & n\mod8\in\{1,7\}\\-1 & n\mod8\in\{3,5\}\end{cases}$.

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 $\mathcal{A}$ עבור לכל $N,m\in\mathbb{N}_+$ ולכל $a,m\in[N-1]$ מתקיים $\mathcal{A}(N,a,m)=(a^m\mod N)$.

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 $\text{ModIteratedSquaring}[\mathcal{A}](N,a,(m)_2)=(a^m\mod N)$.

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

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 $\left(N\in\mathbb{P}\right)\Longleftrightarrow\left(\text{TrialDivision}\left(N\right)=\text{True}\right)$.

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 $a^{N-1}\equiv1\mod N$.

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

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

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

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

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

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

```
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: 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 $\left|\left\{a \in \mathbb{N}_{<N} \mid \text{MillerRabinPrimalityTest}\left(N;a\right) = \text{True}\right\}\right| \leq \frac{\varphi(N)}{4}$.

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

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

```
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 $\mathbb{P}_r\left(\text{PrimeGenerator}\left(n,k;r\right) \in \mathbb{P}\right) \geq 1 - \frac{1}{4^k}$.

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

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

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

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

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

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

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

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 $D(E(p,k), k) = p$ לכל $p, k \in \mathbb{F}_2^n$ אזי (E, D).

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

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

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

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

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

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

משפט: יהיו $p, q \in \mathbb{P}$ 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 $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{A}^{M(\cdot, k_e)}(1^n) = k_d$)$\iff$(קיים יריב $\mathcal{A}^M$ בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{A}^{M(\cdot, k_e)}(1^n) = \text{IFP}(N)$).

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

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

בעיית הלוגריתם הדיסקרטי: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p ויהי $a \in (\mathbb{Z}/p\mathbb{Z})^\times$ אזי $\text{DLP}(p, g, a) = x$ 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 $\mathcal{O}\left(\exp\left(c \cdot \log^{\frac{1}{3}}(p) \cdot \log^{\frac{2}{3}}(p)\right)\right)$.

פרוטוקול תקשורת דיפי־הלמן: יהי $p \in \mathbb{P}$ ויהי g שורש פרימיטיבי מודולו p אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים $\Pi_{\text{DiffieHellman}}$ 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 $\Pi_{\text{DiffieHellman}}(p, g) = (K_{AB}, K_{BA})$ אזי $K_{AB} = K_{BA}$.

טענה: יהי $p \in \mathbb{P}$ יהי g שורש פרימיטיבי מודולו p 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 $E\left(c, (\alpha, \beta, \gamma)\right) = \left((c \cdot \gamma^y) \mod \alpha, \beta^y \mod \alpha\right)$.
- $D\left((c_1, c_2), (\alpha, \beta, \gamma)\right) = \left(c_1 \cdot c_2^{-\gamma}\right) \mod \alpha$.

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 חד־מימדית גזירה.

עקום אליפטי: יהי $\mathbb{F}$ שדה באשר $\text{char}(\mathbb{F}) \neq 2$ ויהי $f \in \mathbb{F}[x]$ באשר $\deg(f) = 3$ וכן f בעל שורשים פשוטים מעל $\overline{\mathbb{F}}$ 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 חד־מימדית חלקה.

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

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

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

טענה: יהי E עקום אליפטי 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 $P, Q \in E$ אז

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

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 $\Pi^{\text{EC}}_{\text{DiffieHellman}}$ כך

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

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 $\Pi^{\text{EC}}_{\text{DiffieHellman}}(p, g) = (K_{AB}, K_{BA})$ 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 $\mathcal{A} = \text{ECDLP}$ אזי קיים יריב $\mathcal{B}$ בעל כוח חישובי $\tilde{\mathcal{O}}(T)$ המקיים $\mathcal{B}(p, f, G, xG, yG) = xyG$.

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

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 $\left(f\lesssim g\right)\iff\left(\liminf_{x\to\infty}\frac{g(x)}{f(x)}\ge 1\right)$.

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

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

הערה: בקורס זה $\log=\ln$.

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

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

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

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 $e_p\left(n!\right)=\sum_{i=1}^{\infty}\left\lfloor\frac{n}{p^i}\right\rfloor$.

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

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

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

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

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

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

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

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

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

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

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 $\varphi\left(n\right)\ge c\cdot\frac{n}{\log\log(n)}$.

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

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

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

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

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 $\pi\left(x\right)\lesssim\frac{c\cdot x}{\log(x)}$ אז $c\ge 1$.

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

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

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

טענה: יהי $\varepsilon>0$ אזי קיים $N\in\mathbb{N}$ עבורו לכל $n\in\mathbb{N}_{\ge N}$ מתקיים $\left[n,\left(1+\varepsilon\right)n\right]\cap\mathbb{P}\ne\varnothing$.

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

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

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

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

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

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

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

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

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

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

טענה: יהי $m\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ באשר $\left(m,a\right)>1$ אזי $\pi_{m,a}\left(\infty\right)\le1$.

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

משפט דה-לה-ואלה-פוסן/המספרים הראשוניים בסדרות חשבוניות: יהי $m\in\mathbb{N}$ ויהי $a\in\mathbb{Z}$ באשר $\left(a,m\right)=1$ אזי $\pi_{m,a}\left(x\right)\sim\frac{x}{\varphi\left(m\right)\cdot\log\left(x\right)}$. לא הוכח בקורס

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

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

משפט: אם GRH אז קיים $c>0$ עבור לכל $N\in\mathbb{N}_{+}$ מתקיים $\left(N\in\mathbb{P}\right)\Longleftrightarrow($לכל $\text{MillerRabinPrimalityTest}\left(N;a\right)=\text{True}$ $\left.a\le c\log^{2}\left(N\right)\right)$. 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 $f\in\mathbb{Z}\left[x_{1},\ldots,x_{n}\right]$ אזי $f=0$.

טענה: יהי $f\in\mathbb{Z}\left[x_{1},\ldots,x_{n}\right]$ ויהי $N\in\mathbb{N}_{\ge2}$ באשר $\text{sols}_{\mathbb{Z}_{N}}\left(f=0\right)=\varnothing$ אזי $\text{sols}_{\mathbb{Z}}\left(f=0\right)=\varnothing$.

משפט מטיאסביץ': $\left\{\left\langle f\right\rangle \mid\left(f\in\mathbb{Z}\left[x_{1},\ldots,x_{n}\right]\right)\wedge\left(\text{sols}_{\mathbb{Z}}\left(f=0\right)\ne\varnothing\right)\right\}\notin\mathcal{R}$.

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

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

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

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

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

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

- $\text{sols}_{\mathbb{Z}}\left(f=0\right)=\left\{\left(da,db\right)\mid\left(d\in\mathbb{Z}\right)\wedge\left(f=0\right.\right.$ פתרון פרימיטיבי של $\left.\left.\left(a,b\right)\right)\right\}$.
- לכל פתרון פרימיטיבי $\left(a,b\right)$ של $f=0$ מתקיים $a|\zeta_{0}$ וכן $b|\zeta_{n}$.

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

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

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

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

טענה: יהיו $a,b,c\in\mathbb{Z}$ אזי $\left(\left(a,b\right)|c\right)\iff\left(\text{sols}_{\mathbb{Z}}\left(ax+by=c\right)\ne\varnothing\right)$.

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

טענה: יהיו $a_{1}\ldots a_{n},b\in\mathbb{Z}$ אזי $\left(\left(a_{1},\ldots,a_{n}\right)|b\right)\iff\left(\text{sols}_{\mathbb{Z}}\left(\sum_{i=1}^{n}a_{i}x_{i}=b\right)\ne\varnothing\right)$.

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

טענה: יהי $f\in\mathbb{Z}_{\le2}\left[x,y\right]$ אזי קיימים $\alpha,\beta,\gamma,\delta,\varepsilon,\zeta\in\mathbb{Q}$ עבורם אחד מהבאים מתקיים

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

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

טענה: יהי $a\in\mathbb{Z}$ אזי $\left(a=\square\right)\iff\left(\text{sols}_{\mathbb{Z}}\left(x^{2}=0\right)\ne\varnothing\right)$.

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

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

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

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

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

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

משוואת פל מוכללת: יהי $a \in \mathbb{Z} \backslash \{0\}$ 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.

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

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

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

נורמה בחוג $\mathbb{Z}\left[\sqrt{d}\right]$: יהי $d \in \mathbb{Z}$ באשר $d \neq \square$ ויהי $\alpha \in \mathbb{Z}\left[\sqrt{d}\right]$ 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 $\mathbb{Z}\left[\sqrt{d}\right]^\times = \left\{\alpha \in \mathbb{Z}\left[\sqrt{d}\right] \;\middle|\; N(\alpha) \in \{\pm 1\}\right\}$.

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