```
a,b\in S וכן a-b\in S וכן a+b\in S מתקיים a,b\in S עבורה לכל אבורה ביחס לחיבור חיסור וכפל: קבוצה אוכן
                                                                                                         טענה: \mathbb{Z} סגורה ביחס לחיבור חיסור וכפל.
                               S \cap (0,1] = \{1\} המקיימת את האי־שיוויון היסודי של תורת המספרים: קבוצה S \subseteq \mathbb{R} המקיימת
                                                                                    . מקיימת את אי־שיוויון היסודי של תורת המספרים. מקיימת את מקיימת של מ
         S=\mathbb{Z} אזי חיסור וכפל אזי איישננה. מהארS=\mathbb{Z} המקיימת את האי־שיוויון היסודי של תורת המספרים וכן סגורה ביחס לחיבור חיסור וכפל אזי
                                                   . מסקנה עיקרון הסדר הטוב על הטבעיים: תהא S \subseteq \mathbb{N} באשר S \neq \emptyset אזי
                                                                           . סענה: תהא S\subseteq\mathbb{Z} אזי \min\left(S\right) אזי איזי מלרע באשר מלרע קיים.
                                                                        . קיים \max{(S)} אזי S \neq \varnothing חסומה מלעיל באשר S \subseteq \mathbb{Z} אזי
                                                                                           מסקנה: \mathbb{Z} אינה חסומה מלרע וכן אינה חסומה מלעיל.
מסקנה עיקרון האינדוקציה: יהי P\left(n\right)\Longrightarrow P\left(n+1\right) מאינה n\in\mathbb{N} וכן לכל P\left(0\right) באשר שנידיקט מעל P\left(n\right) איזי איזי ווער איינדוקציה: יהי פרידיקט מעל
                                                                                                                                                   .m \in \mathbb{N}
(orall m < n.P\left(m
ight)) \Longrightarrow P\left(n+1
ight) מתקיים n \in \mathbb{N} מתקיים P\left(n+1
ight) פענה עיקרון האינדוקציה החזקה: יהי
                                                                                                                                 .k \in \mathbb{N} לכל P(k) אזי
                                                            ab=ac מספר מתחלק במספר: יהיb\in\mathbb{Z} אזי איז a\in\mathbb{Z} אזי אוים מספר מתחלק במספר: יהי
                                                                                                a|b אזי aב מתחלק ב־a,b\in\mathbb{Z} אזי סימון: יהיו
                                                                                        a \nmid b אזי a באשר b אינו מתחלק ב־a,b \in \mathbb{Z} אינו מחלק יהיו
                                                                                                                             a|0 אזי a\in\mathbb{Z} טענה: יהי
                                                                                                                 -1|a טענה: יהיa\in\mathbb{Z} אזי אוכן
                                                          |a| (db + ec) מתקיים c,d \in \mathbb{Z} אזי לכל a|c וכן a|b באשר a,b,c \in \mathbb{Z} טענה: יהיו
                                                                                                a|c אזי b|c וכן a|b באשר a,b,c\in\mathbb{Z} טענה: יהיו
                                                                                                         a \leq b אזי a|b באשר a,b \in \mathbb{N} טענה: יהיו
                                                                                    ((a|b) \land (b|a)) \Longleftrightarrow (a \in \{\pm b\}) אזי a,b \in \mathbb{Z} טענה: יהיו
                   a=qd+r טענה חלוקה עם שארית: יהי d\in\mathbb{N}_+ ויהי a\in\mathbb{Z} אזי קיימים ויחידים q,r\in\mathbb{Z} באשר וכן
                                                a אזי a\in\mathbb{Z} איי של a\in\mathbb{Z} יהי a\in\mathbb{Z} יהי וויהיו a\in\mathbb{Z} יהי מנה של חלוקה: יהי
                                            x אזי a\in\mathbb{Z} יהי a\in\mathbb{Z} יהי a\in\mathbb{Z} יהי a\in\mathbb{Z} יהי ויהיו של חלוקה. יהי אחרית של a\in\mathbb{Z} אזי
                                   a\in\mathbb{Z} יהי מסקנה:
                                                                 |x|=\max\left((-\infty,x]\cap\mathbb{Z}
ight) אזי x\in\mathbb{R} החלק השלם/ערך שלם תחתון: יהי
                                                q=\lfloor rac{a}{d} 
floorיהי d\in \mathbb{N}_+ יהי a\in \mathbb{Z} ויהיו a\in \mathbb{Z} חלוקה עם שארית של a\in \mathbb{N}_+ מסקנה: יהי
                                                                                     H=d\mathbb{Z} עבורו d\in\mathbb{N} אזי קיים ויחיד ווא H\leq\mathbb{Z} עבורו
                                                                                                            a\mathbb{Z}+b\mathbb{Z}\leq\mathbb{Z} טענה: יהיו a,b\in\mathbb{Z} אזי טענה:
                                                                         d\mathbb{Z}=a\mathbb{Z}+b\mathbb{Z} עבורו d\in\mathbb{N} אזי a,b\in\mathbb{Z} יהיו מירבי: מחלק משותף מירבי:
                                                     \gcd\left(a,b
ight)=d אזי a,b\in\mathbb{Z} ויהי d\in\mathbb{N} המחלק המשותף המירבי של
                                                                                                      (a,b)=\gcd{(a,b)} אזי a,b\in\mathbb{Z} סימון: יהיו
                                                                                          \gcd\left(a,b\right)|b וכן \gcd\left(a,b\right)|a אזי a,b\in\mathbb{Z} טענה: יהיו
                                                                 \gcd\left(a,b
ight)=na+mb עבורם n,m\in\mathbb{Z} אזי קיימים a,b\in\mathbb{Z} איי היי
                                                                                     c|\gcd(a,b) אזי c|b וכן c|a באשר a,b,c\in\mathbb{Z} טענה: יהיו
```

 $\gcd(a,b)=\max\{d\in\mathbb{Z}\mid (d|a)\land (d|b)\}$ אזי $\{a,b\}
eq\{0\}$ באשר באשר $a,b\in\mathbb{Z}$ יסענה: יהיו

 $\gcd\left(a_1\dots a_n
ight)=\sum_{i=1}^n m_i\cdot a_i$ עבורו אזי קיים $m\in\mathbb{Z}^n$ אזי קיים $a_1\dots a_n\in\mathbb{Z}$ יהיו

 $d\mathbb{Z}=\sum_{i=1}^n a_i\mathbb{Z}$ עבורו אזי $d\in\mathbb{N}$ אזי $a_1\ldots a_n\in\mathbb{Z}$ יהיו

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

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

 $a_1 \ldots a_n = 1$ מספרים זרים: מספרים $a_1 \ldots a_n \in \mathbb{Z}$ מספרים מספרים מספרים

 $\gcd(a,b)=d$ אזי d=na+mb וכן $m,m\in\mathbb{Z}$ וכן קיימים ויהי d באשר $d\in\mathbb{N}$ אזי ויהי $d\in\mathbb{Z}$ אזי ויהי

 $\gcd(a_1\dots a_n)=d$ איי אוי $a_1\dots a_n$ איי היו ויהי $d\in\mathbb{N}$ המחלק המשותף המירבי של $a_1\dots a_n\in\mathbb{Z}$ איי

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

```
a=\sum_{k=1}^k d_ib^i טענה: יהי b\in\mathbb{N}באשר b\in\mathbb{N} המקיים ויחיד ויחיד אזי קיים ויחיד ויחיד ויחיד ויחיד ויחיד ויחיד מענה: יהי
      (n)_b=d אזי n=\sum_{i=1}^k d_ib^i וכן וכך d_k>0 באשר d\in\{0,\dots,b-1\}^k ויהי ויהי b\in\mathbb{N}_{\geq 2} יהיו
                                                                                             הערה: כאשר לא כתוב בסיס בייצוג נתייחס לבסיס עשרוני.
                                                                                    \mathrm{len}\left((n)_b
ight)=\left\lfloor\log_b\left(n
ight)
floor+1 אזי n\in\mathbb{N} ויהי b\in\mathbb{N}_{\geq 2} יהי יהי
                                                                                                   \mathrm{len}\left((n)_2
ight) אזי n\in\mathbb{N} מספר הביטים לייצוג מספר: יהי
                                        הערה: בסיבוכיות של אלגוריתמים מספריים נתייחס לסיבוכיות כפונקציה של אורך המספר בבינארי.
                                                                           \mathcal{O}\left(n
ight) סענה: קיים אלגוריתם \mathcal{A} המחשב חיבור מספרים בסיבוכיות ריצה
                                                                           \mathcal{O}\left(n^{2}
ight) טענה: קיים אלגוריתם \mathcal{A} המחשב כפל מספרים בסיבוכיות ריצה
                                                                                                אזי a,b \in \left\{0,1\right\}^n ויהיו n \in \mathbb{N} אזי אלגוריתם קרטסובה: יהי
Function KaratsubaMult(a, b):
     if n=1 then return a_1 \cdot b_1
     \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
                                                                                        .(KaratsubaMult ((a)_2\,,(b)_2))_{10}=ab אזי a,b\in\mathbb{N} טענה: יהיו
                                                                                          \mathcal{O}\left(n^{\log_2(3)}\right) הינה KaratsubaMult טענה: סיבוכיות הריצה של
                                                     \mathcal{O}\left(n\log\left(n
ight)\right) טענה קולי־טוקי: קיים אלגוריתם \mathcal{A} המחשב כפל מספרים בסיבוכיות ריצה
                                                                                                 \gcd(a,b)=\gcd(a+qb,b) אזי a,b,q\in\mathbb{Z} למה: יהיו
                                                                                                                         אזי a,b\in\mathbb{Z} יהיו אוקלידס: אזי
Algorithm EuclidGCD(a, b):
     if (a < 0) \lor (b < 0) \lor (|a| < |b|) then
        return EuclidGCD (\max\{|a|,|b|\},\min\{|a|,|b|\})
     if b = 0 then return a
     (q,r) \leftarrow \text{RemainderDiv}(a,b)
     return EuclidGCD(b, r)
                                                                                                 .EuclidGCD (a,b)=\gcd{(a,b)} אזי a,b\in\mathbb{Z} טענה: יהיו
                                                                                                     \mathcal{O}\left(n^2\right) הינה EuclidGCD טענה: סיבוכיות הריצה של
                                                                                (-1)^k\,F_{k-1}\cdot F_{k+1}+(-1)^{k+1}\,F_kF_k=1 טענה: יהי k\in\mathbb{N}_+ יהי
                                                                            \mathcal{O}\left(n\log^2\left(n
ight)
ight) בסיבוכיות ריצה \mathcal{G}המחשב המחשב אלגוריתם לאגוריתם בסיבוכיות ב
                                                                  d\mathbb{Z}=igcap_{i=1}^n a_i\mathbb{Z} עבורו d\in\mathbb{N} אזי a_1\ldots a_n\in\mathbb{Z} יהיו יהיו
                                \mathrm{lcm}\,(a_1\dots a_n)=d אזי a_1\dots a_n\in\mathbb{Z} ויהי a_1\dots a_n\in\mathbb{Z} ויהי יהיו
                                                                                          [a_1\ldots a_n]=\operatorname{lcm}\left(a_1\ldots a_n
ight) אזי a_1\ldots a_n\in\mathbb{Z} יהיו
                                                                                         a_i | \mathrm{lcm}\,(a_1 \ldots a_n) לכל a_i | \mathrm{lcm}\,(a_1 \ldots a_n) אזי a_1 \ldots a_n \in \mathbb{Z} טענה: יהיו
                                                                   \operatorname{lcm}\left(a_1\ldots a_n\right)|m אזי i\in[n] לכל a_i|m באשר a_1\ldots a_n, m\in\mathbb{Z} איזי
                                                  \mathrm{lcm}\,(a_1\ldots a_n)=\min\left\{m\in\mathbb{N}_+\mid orall i\in[n]\,.\,(a_i|m)
ight\} אזי a_1\ldots a_n\in\mathbb{Z}\setminus\{0\} טענה: יהיו
                                                                                             (a|b) \Longleftrightarrow \left(rac{b}{a} \in \mathbb{Z}
ight) אזי a 
eq 0 באשר a,b \in \mathbb{Z} למה: יהיו
                                                                                                              .(a|b) \Longleftrightarrow (ac|bc) אזי a,b,c \in \mathbb{Z} למה: יהיו
                                                                                                                    [a,b]=rac{ab}{(a,b)} אזי a,b\in\mathbb{N}_+ טענה: יהיו
```

 $.F_k=2^{2^k}+1$ אאי $k\in\mathbb{N}$ מספר פרמה: יהי איז $k\in\mathbb{N}$ איזי $.F_{k+1}-2=\prod_{i=0}^kF_i$ איזי איזי איזי איזי $k\in\mathbb{N}$ מסקנה: יהיו k0 שונים איזי k1 שונים איזי k2.

```
a,b\in\{0,\pm 1\}\cup(\pm\mathbb{P}) אזי (n|a)\vee(n|b) אז n|ab אם a,b\in\mathbb{Z} טענה: יהי n\in\mathbb{N} אזי n\in\mathbb{N}
                                                            p|a_i מסקנה: יהי p\in \mathbb{P} ויהיו a_i באשר a_1\ldots a_n\in \mathbb{Z} אזי קיים p\in \mathbb{P} מסקנה: יהי
                                                                                                                       p \mid n אזי קיים p \in \mathbb{P} המקיים n \in \mathbb{N}_{\geq 2} למה: יהי
                                                                                                                       אזי N \in \mathbb{N}_+ יהי אלגוריתם הנפה של ארטוסתנס: יהי
Algorithm EratosthenesSieve(N):
      A \leftarrow \langle \text{True} \mid n \in [1, \dots, N] \rangle; A_1 = \text{False}
      for i \in [1, \ldots, N] do
           if A_i = \text{True then}
                 while i+2j \leq N do
                      A_{i+2j} = \text{False}
                     j \leftarrow j + 1
            end
      end
      return \{i \in [N] \mid A_i = \text{True}\}
                                                                                         .EratosthenesSieve (N)=\{p\in\mathbb{P}\mid p\leq N\} אזי N\in\mathbb{N}_+ יהיN\in\mathbb{N}_+
                       \mathcal{O}\left(\left(\sum_{p\in\mathbb{P}_{\leq N}}\frac{1}{p}\right)\cdot N
ight) הינה EratosthenesSieve (N) אזי סיבוכיות הריצה של N\in\mathbb{N}_+ הינה N\in\mathbb{N}_+ וכן N\in\mathbb{N}_+ וכן N\in\mathbb{N}_+ סענה אטקין־ברנסטיין: קיים אלגוריתם \mathcal{A} עבורו \mathcal{A}(N)=\mathbb{P}_{\leq N} לכל אטקין־ברנסטיין: קיים אלגוריתם \mathcal{A}
משפט היסודי של האריתמטיקה: יהי n \in [k-1] אזי קיימים ויחידים p_i < p_{i+1} באשר באשר אזי קיימים ויחידים n \in [k-1] המקיימים
                                                                                      e_n(n)=\max\left\{m\in\mathbb{N}\mid (p^m|n)
ight\} אזי n\in\mathbb{N}_+ ויהי n\in\mathbb{N}_+ איזי n\in\mathbb{N}_+
                                                                                                                            p^{e_p(n)}\|n אזי p\in\mathbb{P} ויהי n\in\mathbb{N}_+ אזי יהי
                                                                                                                             n=\prod_{p\in\mathbb{P}}p^{e_p(n)} אזי n\in\mathbb{N}_+ מסקנה: יהי
                                                                                       .e_{p}\left(mn
ight)=e_{p}\left(m
ight)+e_{p}\left(n
ight) אזי p\in\mathbb{P} ויהי n,m\in\mathbb{N}_{+} יהיו יהיו
                                                                                       .(m|n)\Longleftrightarrow (\forall p\in\mathbb{P}.e_{p}\left(m
ight)\leq e_{p}\left(n
ight)) אזי n,m\in\mathbb{N}_{+} מסקנה: יהיו
                                                                                  a_1\dots a_n)=\prod_{p\in\mathbb{P}}p^{\min\{e_p(a_i)|i\in[n]\}} אזי a_1\dots a_n\in\mathbb{N}_+ יהיו יהיו
                                                                                  [a_1\dots a_n]=\prod_{p\in\mathbb{P}}p^{\max\{e_p(a_i)|i\in[n]\}} אזי a_1\dots a_n\in\mathbb{N}_+ יהיו יהיו
                                                                 (p|n) וכן p|m וכן p|m המקיים p\in\mathbb{P} האזי (לא קיים m,n) אזי וכן m,n
                                                                                                                                                        \|\mathbb{P}\|=leph_0 משפט אוקלידס:
                                                                              \{b+i\mid i\in\{0,\dots,n\}\}\cap\mathbb{P}=arnothing עבורו b\in\mathbb{N} אזי קיים n\in\mathbb{N} טענה: יהי
                                     השערה הראשוניים התאומים: יהי N \in \mathbb{R} אזי קיים p \in N באשר הראשוניים התאומים: יהי או איז קיים p \in \mathbb{R} השערה פתוחה
                                                                                                                            \prod_{p\in\mathbb{P}_{\leq n}}p\leq 4^{n-1} אזי n\in\mathbb{N}_{\geq 2} טענה: יהי
                                                                                                              2p+1\in\mathbb{P}^-ראשוני סופי ז'רמן: ראשוני p\in\mathbb{P} המקיים
                                                                                                                                                    |\mathbb{P}\cap (4\mathbb{N}+3)|=\aleph_0 טענה:
                                                                                                                                                   |\mathbb{P}\cap (4\mathbb{N}+1)|=\aleph_0 :טענה
                                                                                                                                           |\mathbb{Z}/n\mathbb{Z}|=n אזי n\in\mathbb{N}_+ טענה: יהי
     \pi\left(a
ight)=r+n\mathbb{Z} אאי a\in\mathbb{Z} יהי n\in\mathbb{N}_+ שארית החלוקה של \pi:\mathbb{Z}	o\mathbb{Z}/n\mathbb{Z} תהא \pi\in\mathbb{Z} איי \pi\in\mathbb{R}_+ שארית החלוקה של מענה: יהי
```

 $[a_1,\ldots,a_n]=[|a_1|,\ldots,|a_n|]$ אזי $[a_1,\ldots,a_n]=[|a_1|,\ldots,|a_n|]$ טענה: יהיו

 $.[a_1\dots a_n]=[[a_1\dots a_{n-1}]\,,a_n]$ איי $a_1\dots a_n\in\mathbb{Z}$ יהיי טענה: יהיו ab
eq p עבורו לכל $a,b\in\mathbb{N}_{\geq 2}$ מתקיים מספר ראשוני: מספר $p\in\mathbb{N}_{\geq 2}$

 $a,b\in\mathbb{Z}$ ויהיו $p\in\mathbb{P}$ אזי p|ab אזי $a,b\in\mathbb{Z}$ טענה: יהי

a,b,c=1 מספרים זרים: מספרים $a,b\in\mathbb{Z}$ מספרים מספרים

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

 $m
otin\mathbb{R}$ באשר $m\in\mathbb{N}_{\geq 2}$ מספר פריק: מספר

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

```
a = a + nויהיn \in \mathbb{N} אזיn \in \mathbb{N}_+ ויהיn \in \mathbb{N}_+ ויהי
                              (a \mod n) = (b \mod n) מספרים שקולים תחת מודולו: יהי n \in \mathbb{N}_+ אזי a,b \in \mathbb{Z} איזי
                                                             a\equiv b\mod n אזי מודולו מודולו a,b\in\mathbb{Z} ויהיו ויהיו ח
                                                         .(n|\,(a-b))\Longleftrightarrow (a\equiv b\mod n) אזי a,b\in\mathbb{Z} ויהיו n\in\mathbb{N}_+ יהי יהי יהי
\alpha \equiv \beta \mod n \iff \left(rac{lpha}{r} \equiv rac{eta}{r} \mod rac{n}{r}
ight) אזי \alpha, \beta \in \mathbb{Z} ויהיו \alpha, \beta \in \mathbb{Z} ויהיו \alpha, \beta \in \mathbb{Z} באשר \alpha, r \in \mathbb{N}_+ אזי
     a+b\equiv c+d\mod n אזיb\equiv d\mod n וכן a\equiv c\mod n באשר a,b,c,d\in\mathbb{Z} ויהיו n\in\mathbb{N}_+ למה: יהי
                                a \pmod n + (b \mod n) = ((a+b) \mod n) \mod n אזיa,b \in \mathbb{Z} ויהיוn \in \mathbb{N}_+ הגדרה: יהיn \in \mathbb{N}_+
                                                                                                         . טענה: יהי\mathbb{N}_+ אזי \mathbb{Z}/n\mathbb{Z} חבורה אבלית n\in\mathbb{N}_+
                                              a_0\ldots a_k\in\{0,\ldots,9\} טענה: יהי k\in\mathbb{N} יהיו k\in\mathbb{N} יהיו k\in\mathbb{N} אזי a_0\ldots a_k\in\{0,\ldots,9\} יהיו k\in\mathbb{N} טענה: יהי k\in\mathbb{N} יהיו k\in\mathbb{N} יהיו k\in\mathbb{N} טענה: יהי k\in\mathbb{N} ויהיו k\in\mathbb{N} ויהיו k\in\mathbb{N} יהי k\in\mathbb{N} טענה: יהי k\in\mathbb{N} ויהיו k\in\mathbb{N} ויהיו
                           .(7|a) \Longleftrightarrow \left(7|\left(5a_0+\sum_{i=1}^k 10^{i-1}a_i
ight)
ight) אזי a_0\ldots a_k\in\{0,\ldots,9\} ויהיו k\in\mathbb{N} טענה: יהי
                                               (9|a) \Longleftrightarrow \left(9|\left(\sum_{i=0}^k a_i
ight)'
ight) איזי k \in \mathbb{N} טענה: יהי k \in \mathbb{N} יהיי
                                      a_0 : (11|a) \Longleftrightarrow \left(11|\sum_{i=0}^k \left(-1
ight)^i a_i
ight) אזיa_0 \dots a_k \in \{0,\dots,9\} ויהיו k \in \mathbb{N} טענה: יהי
              ab\equiv cd\mod n אזי b\equiv d\mod n וכן a\equiv c\mod n באשר a,b,c,d\in\mathbb{Z} אזי n\in\mathbb{N}_+ למה: יהי n\in\mathbb{N}_+
                                    (a \mod n) \cdot (b \mod n) = ((a \cdot b) \mod n) אזי a,b \in \mathbb{Z} ויהיי n \in \mathbb{N}_+ הגדרה: יהי הגדרה: יהי
                                                                          הערה: אלא אם כן נאמר אחרת חוג הינו חוג חילופי בעל יחידה.
                                                                                                                         טענה: יהי\mathbb{Z}/n\mathbb{Z} אזי n\in\mathbb{N}_+ חוג.
                                                                                                 (n\in\mathbb{P})שדה) שדה n\in\mathbb{N}_+ טענה: יהיn\in\mathbb{N}_+ אזי טענה:
                                                       a,(a,n)=(b,n) אזי a\equiv b \mod n באשר באשר n\in\mathbb{N}_+ יהי יהי למה: יהי n\in\mathbb{N}_+
                                             .((a,n)=1) \Longleftrightarrow \left((a \mod n) \in (\mathbb{Z}/n\mathbb{Z})^{	imes}
ight) אזי a \in \mathbb{Z} ויהי n \in \mathbb{N}_+ יהי יהי
                                   אזי (a,n)=1 באשר בחבורת שאריות החלוקה: יהיn\in\mathbb{N}_+ ויהיn\in\mathbb{N}_+ באשר
```

```
Algorithm InverseMod(n, a):
```

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

```
.InverseMod (n,a)=(a \mod n)^{-1} אזי (a,n)=1 באשר a\in\mathbb{Z} ויהי n\in\mathbb{N}_+ יהי יהי יהי
                                      (\mathbb{Z}/p\mathbb{Z})^{\times}=\{(i \mod p)\mid i\in\{0,\ldots,p-1\}\} אזי p\in\mathbb{P} טענה: יהי p\in\mathbb{P}
                                                  .arphi\left(n
ight)=\left|\left(\mathbb{Z}/n\mathbb{Z}
ight)^{	imes}
ight| כך arphi:\mathbb{N}_{+}	o\mathbb{N} כגדיר גגדיר אויילר: נגדיר
.arphi\left(\prod_{i=1}^k p_i^{e_i}
ight)=\prod_{i=1}^k \left(p_i^{e_i}-p_i^{e_i-1}
ight) אזי e_1\dots e_k\in\mathbb{N}_+ שונים ויהיו p_1\dots p_k\in\mathbb{P} אזי
        . טענה: יהי p\in\mathbb{P} אזי איזי אוני סופי ז'רמן ראשוני חפיים וופי n\in\mathbb{N}_+ המקיים אזי ראשוני חופי ז'רמן.
                     a^{arphi(n)}\equiv 1\mod n אזי אוי (a,m)=1 באשר a\in\mathbb{Z} ויהי n\in\mathbb{N}_+ משפט אויילר: יהי
                     a^{p-1}\equiv 1\mod p אזי אזי p
mid n אוי אוי p\in\mathbb{P} משפט הקטן של פרמה: יהי
                                                              a^p \equiv a \mod p אזי a \in \mathbb{Z} ויהי p \in \mathbb{P} מסקנה: יהי
                  a_i,j\in[n] לכל (a_i,a_j)=1 המקיימים a_1\dots a_n\in\mathbb{Z} מספרים זרים בזוגות: מספרים
                                        [a_1,\ldots,a_n]=\prod_{i=1}^n a_i טענה: יהיו a_1\ldots a_n\in\mathbb{Z} זרים בזוגות אזי
 v \equiv a \mod m אזיi \in [n] לכל v_i \equiv a_i \mod m_i באשר a,v \in \mathbb{Z}^n ויהיו m \in \mathbb{N}^n_+ לכל הגדרה: יהי
                                       .i\in[n] לכל (\mathbb{1}^n)_i=1 כך ב\mathbb{1}^n\in\mathbb{N}^n לכל (\mathbb{1}^n) לכל הגדרה: יהי
                     משפט השאריות הסיני: יהיוm_1 \dots m_n \in \mathbb{N}_+ אזי יהיו משפט השאריות הסיני: יהיו
```

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

```
Algorithm ModEquationSys (m_1 \dots m_n, a_1 \dots a_n):
     for i \in [n] do
         M_i \leftarrow \prod_{j \in [n] \setminus \{i\}} m_j
         N_i \leftarrow \text{InverseMod}(m_i, M_i)
     return \sum_{i=1}^{n} a_i M_i N_i
                                      \mathbb{1}^n · ModEquationSys \equiv a \mod m אזי a_1 \ldots a_n \in \mathbb{Z} ארים באוגות ויהיו m_1 \ldots m_n \in \mathbb{N}_+ יהיו
i,j\in [n] טענה: יהיו m_1\ldots m_n\in \mathbb{N} ויהיט איי (קיים x\in \mathbb{Z} איי (קיים a_1\ldots a_n\in \mathbb{Z} ויהיע ויהיע איי (קיים a_1\ldots a_n\in \mathbb{Z}
                                                                                                                                                (a_i \equiv a_i \mod (m_i, m_i))
                                                   \mathbb{Z}/(\prod_{i=1}^n m_i)\mathbb{Z}\simeq\prod_{i=1}^n\mathbb{Z}/m_i\mathbb{Z} אונות אזי m_1\dots m_n\in\mathbb{N}_+ יהיו הסיני: יהיו
                                                                                                         \sum_{\substack{k\in[n]\\gcd(k,n)=1}} k=rac{1}{2}n\cdotarphi\left(n
ight) אזי n\in\mathbb{N}_{\geq2} טענה: יהי
                      f(nm)=f(n) מתקיים (n,m)=1 באשר n,m\in\mathbb{N} באשר f:\mathbb{N}_+	o\mathbb{R} מתקיים f:\mathbb{N}_+	o\mathbb{R}
                                                                                                                                                   .טענה: \varphi פונקציה כפלית
                                                                                              f\left(1
ight)=1 אזי f
eq0 איזי f:\mathbb{N}_{+}
ightarrow\mathbb{R} אזי מענה: תהא
                               f=g אזי אf\left(p^k
ight)=g\left(p^k
ight) מתקיים k\in\mathbb{N} מתקיים לכל כפליות באשר לכל באשר לכל לכל פליות באשר לכל
                                                                         . כפלית. f(n)=\gcd(n,k) כך f:\mathbb{N}_+	o\mathbb{R} ונגדיר k\in\mathbb{N}_+ אזי f(n)=\gcd(n,k)
                                                . הינה פלית. F\left(n
ight)=\sum_{d\in\mathbb{N}}f\left(d
ight) המוגדרת F:\mathbb{N}	o\mathbb{R} הינה כפלית אזי הינה כפלית.
                                                                                      .\sigma\left(n
ight)=\sum_{\substack{d\in\mathbb{N}\d\mid n}}d כך \sigma:\mathbb{N}_{+}	o\mathbb{N} פונקציית סכום המחלקים: נגדיר
                                                                                                                                                 מסקנה: \sigma פונקציה כפלית.
                                                                                                                \sigma(n)=2n מספר מושלם: מספר מספר מספר מחשלם
                                 (n|d) \Longleftrightarrow \left(g^d=1
ight) אזי G יוצר של g \in G יוצר מסדר מסדר ציקלית מסדר תהא חבורה G תהא תהא מסדר מסדר מסדר ויהי
                                       .ord \left(g^d\right)=\frac{n}{(n,d)} אזי G יוצר של g\in G יוצר מסדר ציקלית מסדר חבורה G תהא חבורה n,d\in\mathbb{N}_+ יהיו
                                 .arphi\left(d
ight)=|\{a\in G\mid \mathrm{ord}\left(a
ight)=d\}| אזי מסדר מסדר G ותהא ותהא d|n באשר באשר ליהיי יהיו יהיו ליהיו
                                     \{a\in G\mid G טענה: יהי\{a\}=\{g^d\mid (d,n)=1\} אזי מסדר מסדר מסדר G יוצר של n\in\mathbb{N}_+ יוצר אזי ותהא
                                                          |\{g^d|\,(d,n)=1\}|=arphi\,(n) אזי מסקנה: יהי ותהא n\in\mathbb{N}_+ ותהא חבורה ציקלית מסדר n\in\mathbb{N}_+
                                         |\{a\in G\mid a^d=1\}|=d אזי מסקנה: יהיו d|n ותהא ותהא d|n באשר d,n\in\mathbb{N}_+ מסקנה: יהיו
                                                   |\{a\in G\mid a^d=1\}|=(n,d) אזי מסקנה: יהיו d,n\in\mathbb{N}_+ ותהא מסקנה: יהיו להא מסקנה: יהיו
                  \|a\| \|a\| \|a\| \|a\| \|a\| \|a\| מסקנה: יהי \|a\| \|a\| \|a\| \|a\| \|a\| מסקנה: יהי ותהא \|a\| \|a\| \|a\| \|a\| \|a\| אזי (\|a\| \|a\| \|a\| \|a\| \|a\| \|a\| \|a\| \|a\|
                                                                                                     \sum_{\substack{d\in\mathbb{N}_+\\d|n}}arphi\left(d
ight)=n אזי n\in\mathbb{N}_+ יהי יהי מסקנה: יהי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ ציקלית. מסקנה: יהי n\in\mathbb{N}_+ שדה ותהא n\in\mathbb{N}_+ סופית אזי n\in\mathbb{N}_+
                                                                                \left(\mathbb{Z}/n\mathbb{Z}
ight)^	imes=\langle g\mod n
angle עבורו g\in\mathbb{Z} אזי n\in\mathbb{N}_+ יהי יהי
                                                          .(חבורה ציקלית) אזי (קיים שורש פרימיטיבי מודולו (\mathbb{Z}/n\mathbb{Z})^{\times}) אזי (קיים שורש פרימיטיבי מודולו n\in\mathbb{N}_{+}
                       (k, \varphi(n)) = 1כענה: יהיו k \in \mathbb{N}_+ ויהי a שורש פרימיטיבי מודולו a אזי a שורש פרימיטיבי מודולו a
           \left. . \middle| \left\{ g \in [n-1] \mid \langle g \mod n 
angle = (\mathbb{Z}/n\mathbb{Z})^	imes 
ight\} \middle| = arphi \left( arphi \left( n 
ight) 
ight) אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ באשר קיים שורש פרימיטיבי מודולו n \in \mathbb{N}_+
                                                                        \left|\left\{g\in\left[p-1
ight]\mid\left\langle g\mod n
ight
angle=\left(\mathbb{Z}/p\mathbb{Z}
ight)^{	imes}
ight\}
ight|=arphi\left(p-1
ight) אזי p\in\mathbb{P} אזי מה: יהי
                                                                                                            n אזי קיים שורש פרימטיבי מודולו p\in\mathbb{P} משפט: יהי
                                                                                                (p-1)! \equiv -1 \mod p אזי p \in \mathbb{P} מסקנה משפט וילסון: יהי
                                                                                            n\in\mathbb{P} אזי (n-1)!\equiv -1\mod n באשר n\in\mathbb{N}_{\geq 2} אזי n\in\mathbb{N}_{\geq 2}
                (g^{rac{e}{q}} 
eq 1) מתקיים q \mid n באשר q \in \mathbb{P} למה: יהי q \in \mathbb{P} אזי q \in \mathbb{P} מתקיים q \in \mathbb{P}
                                                                                                                      p(\binom{p}{m}) אזי m\in [p-1] ויהי p\in \mathbb{P}
                                               (1+ap)^{p^{k-2}}\equiv 1+ap^{k-1}\mod p^k אזי a\in\mathbb{Z} ויהי k\in\mathbb{N}_{\geq 2} ראשוני יהי ראשוני יהי למה: יהי
                                                                                  (\mathbb{Z}/p^k\mathbb{Z})^	imes\simeq C_{p^{k-1}(p-1)} אזי k\in\mathbb{N}_+ ראשוני ויהי p\in\mathbb{P}_{>2} יהי יהי
```

```
מסקנה: יהי p\in\mathbb{P}_{>2} ראשוני ויהי k\in\mathbb{N}_+ אזי p\in\mathbb{P}_{>2} ציקלית.
          a\equiv (-1)^lpha\, 5^eta\mod 2^k עבורם eta\in \{0,\ldots,2^{k-2}\} וכן lpha\in \{0,1\} ויהי אזי קיימים ויחידים a\in \mathbb{Z}_{\mathrm{odd}} אזי קיימים ויחידים
                                                                                                                                       (\mathbb{Z}/2^k\mathbb{Z})^	imes\simeq C_2	imes C_{2^{k-2}} אזי a\in\mathbb{Z}_{	ext{odd}} ויהי k\in\mathbb{N}_{\geq 2}
                            אזי n=2^k\cdot\prod_{i=1}^mp_i^{e_i} יהיי שונים באשר p_1\dots p_m\in\mathbb{P} ויהיי ויהיי e_1,\dots,e_m\in\mathbb{N}_+ יהיי ויהיי k,m\in\mathbb{N} יהיי יהי k,m\in\mathbb{N}
                                                                                                                                                                    .(\mathbb{Z}/n\mathbb{Z})^{	imes}\simeq\prod_{i=1}^mC_{p_i^{e_i-1}(p_i-1)} אם k\leq 1 אם •
                                                                                                                                  (\mathbb{Z}/n\mathbb{Z})^{	imes}\simeq C_2	imes C_{2^{k-2}}	imes\prod_{i=1}^m C_{p_i^{e_i-1}(p_i-1)}^{e_i-1} אם 2 אם •
                        (n\in\{p^k,2p^k\}) עבורו k\in\mathbb{N}_+ וקיים p\in\mathbb{P}_{>2} וקיים (n\in\{2,4\}) ציקלית) ציקלית) ציקלית) ציקלית) אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+
                                                                                                                                                            טענה: יהי p \in \mathbb{P}_{>2} יויהי שורש פרימיטיבי מודולו p \in \mathbb{P}_{>2}
                                                                                                    a^pאז לכל a^{p-1} \not\equiv 1 \mod p^2 מתקיים כי a^{p-1} \not\equiv 1 \mod p^2 אם •
                                                                                          a^k מתקיים כי a+p פרימיטיבי מודולו אז לכל מודולו אז מתקיים אז מתקיים מודולו a^{p-1} \equiv 1 \mod p^2
                                                                             x^2\equiv a\mod n וכן קיים x\in\mathbb{Z} שארית היבועית: יהי n
eq a אזי אזי a\in\mathbb{Z} המקיים n
eq a וכן קיים
                                                                                                                                \mathrm{QR}_n = \{a \in \mathbb{Z} \mid n \;  סימון: יהי n \in \mathbb{N} אזי a \in \mathbb{N} אזי סימון: יהי
                                                                             n וכן n \nmid a וכן n \nmid a אזי n \in \mathbb{N} אזי מודולו היבועית: יהי n \in \mathbb{N} אזי אי־שארית היבועית: יהי
                                                                                                                     \mathrm{QNR}_n = \{a \in \mathbb{Z} \mid n \;  מימון: יהי n \in \mathbb{P} אזי אי־שארית ריבועית מודולו אזי n \in \mathbb{P}
                                                      טענה: יהי p \nmid a \equiv g^r \mod p וכן p \nmid a באשר a, r \in \mathbb{Z} ויהיו ויהיו פרימיטיבי שורש פרימיטיבי p \notin \mathbb{P}_{>2} אזי יהי
                                                                                                                                                                                                                     .(r \in \mathbb{Z}_{\text{even}}) \iff (a \in QR_p)
                                                                                                                                      .ig| \mathrm{QR}_p ig| = ig| \mathrm{QNR}_p ig| = rac{p-1}{2} אזי p \in \mathbb{P}_{>2} יהי יהי מסקנה: יהי p \in \mathbb{P}_{>2} ויהי a \in \mathbb{Q} אזי a \in \mathbb{Z} ויהי ויהי a \in \mathbb{Z} יהי יהי a \in \mathbb{Z} ויהי ויהי a \in \mathbb{Z} ויהי
                                                                                                                                                     \begin{pmatrix} 0 & p|a \ .\Big(rac{a}{p}\Big) \equiv a^{rac{p-1}{2}} \mod p אזי a \in \mathbb{Z} ויהי p \in \mathbb{P}_{>2} יהי
                                                                                                                                                \left(rac{ab}{p}
ight)=\left(rac{a}{p}
ight)\cdot\left(rac{b}{p}
ight) אזי a,b\in\mathbb{Z} ויהיו p\in\mathbb{P}_{>2} יהי
                                                                                                                                                                 .ig(rac{-1}{p}ig)=\left\{egin{array}{ll} 1&p\equiv 1\mod 4\\ -1&p\equiv 3\mod 4 \end{array}
ight.איי p\in\mathbb{P}_{>2} יהי
                                                                                                                                                        a \in \mathbb{Z} ויהי a \in \mathbb{Z} איזי p \in \mathbb{P}_{>2} הגדרה: יהי יהי p \in \mathbb{P}_{>2}
                                                                                                                                \left. - \left| \operatorname{sols}\left(x^2 = a 
ight) 
ight| = 1 + \left(rac{a}{p} 
ight) אזי a \in \mathbb{Z}/p\mathbb{Z} ויהי p \in \mathbb{P}_{>2} היהי
אזי a\in (\mathbb{Z}/p\mathbb{Z})^{	imes} ויהי S\cup (-S)=(\mathbb{Z}/p\mathbb{Z})^{	imes} וכן S\cap (-S)=\varnothing באשר באוס: S\cap (-S)=\varnothing באשר באשר באוס: S\cap (-S)=\varnothing
                                                                                                                                                         למה גאוס: p \in \mathbb{F}_{>2} למה גאוס: p \in \mathbb{F}_{>2} למה גאוס: p \in \mathbb{F}_{>2} לוב p \in (-1)^{|aS\cap(-S)|} .  (\frac{a}{p}) = (-1)^{|aS\cap(-S)|} מסקנה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי p \in \mathbb{F}_{>2} טענה: יהי p \in \mathbb{F}_{>2} אזי
                                                                                          L\left(rac{a}{p}
ight)=(-1)^{\sum_{i=1}^{\left\lfloorrac{a}{2}
ight\rfloor}\left(\left\lfloorrac{ip}{a}
ight
floor-\left\lfloorrac{(2i-1)p}{2a}
ight
floor
ight)} אזי p
mid a אזי p
mid a אזי p\in\mathbb{P}_{>2} יהי p
mid a ויהי p\in\mathbb{P}_{>2}
                                                                                                      .ig(rac{a}{p}ig)=\Big(rac{a}{q}\Big) אזי p\equiv \pm q \mod 4a באשר p,q\in \mathbb{P}_{>2} ויהיו a\in \mathbb{N}_+ יהי למה: יהי a\in \mathbb{N}_+ יהי היי a\in \mathbb{N}_+ אזי a\in \mathbb{N}_+ אזי a\in \mathbb{N}_+ משפט חוק ההדדיות הריבועית: יהיו a\in \mathbb{P}_{>2} אזי a\in \mathbb{N}_+
                                                                                                                                .\binom{p}{q}=\binom{-q}{p} \text{ אזי } p,q\in\mathbb{P}_{>2} \text{ היו } . מסקנה: יהיו p,q\in\mathbb{P}_{>2} אזי p,q\in\mathbb{P}_{>2} מסקנה: יהי p\in\mathbb{P}_{>2} אזי p\in\mathbb{P}_{>2} מסקנה: יהי p\in\mathbb{P}_{>2} אזי p\in\mathbb{P}_{>2} מספר חסר ריבועים: מספר p\in\mathbb{P} עבורו לכל p\in\mathbb{P} מתקיים p\in\mathbb{P} מספר הסר ריבועים: מספר p\in\mathbb{P}
                                                                                            \left|\operatorname{QR}_{\prod_{i=1}^k p_i}
ight|=rac{1}{2^k}arphi\left(\prod_{i=1}^k p_i
ight) שונים אזי p_1\dots p_k\in\mathbb{P}_{\geq 2} ויהיו k\in\mathbb{N}_+ יהי
                                                                                       a = \prod_{i=1}^k \binom{a}{p_i} אזי a \in \mathbb{Z} איהיו p_1 \dots p_k \in \mathbb{P}_{>2} יהיו k \in \mathbb{N} יהיי k \in \mathbb{N} אזי m \equiv k \mod n באשר m, k \in \mathbb{Z} אזי n \in \mathbb{N}_{\text{odd}} טענה: יהי n \in \mathbb{N}_{\text{odd}} ויהיו n \in \mathbb{N}_{\text{odd}}
                                                                                                                                .((\frac{m}{n})=0)\Longleftrightarrow ((m,n)>1) אזי m\in\mathbb{Z} ויהי n\in\mathbb{N}_{\mathrm{odd}} יהי
                                                                                                                                                       a, (\frac{ab}{n}) = (\frac{a}{n}) \cdot (\frac{b}{n}) אזי a, b \in \mathbb{Z} ויהיו n \in \mathbb{N}_{\text{odd}} טענה: יהי
```

```
a \cdot (rac{a}{nm}) = (rac{a}{n}) \cdot (rac{a}{m}) אזי a \in \mathbb{Z} ויהי n, m \in \mathbb{N}_{	ext{odd}} טענה: יהיו
                               a\in\mathbb{Z} אזי m\equiv a^2\mod n המקיים a\in\mathbb{Z} וכן קיים m\in\mathbb{Z} אזי m\in\mathbb{N}_{\mathrm{odd}} ויהי m\in\mathbb{N}_{\mathrm{odd}} אזי וכן קיים
p|n אזי (קיים p\in\mathbb{P}) אזי (m\equiv a^2\mod n עבורו a\in\mathbb{Z} אזי (קיים m\in\mathbb{Z} באשר המקיים m\in\mathbb{Z} ויהי m\in\mathbb{Z}
                                                                                                                    .(rac{-1}{n})=(-1)^{rac{n-1}{2}} אזי n\in\mathbb{N}_{\mathrm{odd}} יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מסקנה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מסקנה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}}
                                                                                         a(rac{m}{n})=(-1)^{rac{m-1}{2}\cdotrac{n-1}{2}}\cdotig(rac{n}{m}) אזי n,m\in\mathbb{N}_{\mathrm{odd}} ישענה חוק ההדדיות: יהיו
                                                                                                             אזי m \in \mathbb{Z} ויהי n \in \mathbb{N}_{	ext{odd}} אזי יהי יעקובי: יהי
Algorithm JacobiSymbol (m, n):
      if m=0 then return 0
      if n=1 then return 1
     if m < 0 then return (-1)^{\frac{n-1}{2}} · JacobiSymbol (-m,n)
      if m \in \mathbb{N}_{\mathrm{even}} then return (-1)^{\frac{n^2-1}{8} \cdot e_2(m)} \cdot \mathtt{JacobiSymbol}(\frac{m}{2^{e_2(m)}}, n)
      if m < n then return (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} JacobiSymbol (n, m)
      (q, r) \leftarrow \text{RemainderDiv}(m, n)
      return JacobiSymbol(r, n)
                                                                                                    .JacobiSymbol (m,n)=\left(rac{m}{n}
ight) אזי m\in\mathbb{Z} ויהי ויהי n\in\mathbb{N}_{\mathrm{odd}}
                                                                                                                       \mathcal{O}\left(n^{3}
ight) הינה JacobiSymbol טענה: סיבוכיות הריצה של
                                                              \mathcal{O}\left(n\log^2\left(n
ight)\log\log\left(n
ight)
ight) טענה: קיים אלגוריתם \mathcal{A} המחשב סמל יעקובי בסיבוכיות ריצה
                               (a+ay^2) = 1 איי (קיימים x,y \in \mathbb{Z} איי (קיימים p \nmid a איי ויהי p \nmid a ויהי ויהי איי ויהי ויהי מענה: יהי
                                                                                                                                                               |\mathbb{P}\cap(3\mathbb{N}+1)|=\aleph_0 טענה:
                                                                                               m=m^2 מספר ריבוע שלם: מספר m\in\mathbb{Z} עבורו קיים n\in\mathbb{Z} מספר
                                                                                                                                            n=\square יימון: יהיn\in\mathbb{Z} ריבוע שלם אזי
                                                                       a \in \mathbb{Z} אזי n = \square אזי n \in \mathbb{N}_{\mathrm{odd}} \setminus \{1\} אזי יהי n \in \mathbb{N}_{\mathrm{odd}} \setminus \{1\} אזי
                                                                                     a\in\mathbb{Z} טענה: יהי n
eq n באשר באשר n\in\mathbb{N}_{\mathrm{odd}}ackslash\{1\} טענה: יהי
                                                                     \left|\left\{x\in \left(\mathbb{Z}/n\mathbb{Z}
ight)^{	imes}\;\middle|\;\left(rac{x}{n}
ight)=1
ight\}
ight|=rac{1}{2}arphi\left(n
ight) אזי n
eq\square באשר n\in\mathbb{N}_{\mathrm{odd}}\setminus\{1\} טענה: יהי
                                                                                                                                                               |\mathbb{P}\cap (5\mathbb{N}-1)|=\aleph_0 טענה:
 \mathcal{A}(N,a,m)=(a^m\mod N) מתקיים a,m\in[N-1] ולכל ולכל אלגוריתם \mathcal{A} עבורו לכל עבורו לכל ולכל ולכל וולכל וולכל מתקיים n,m\in\mathbb{N}_+
                           אזי a\in\mathbb{Z}/N\mathbb{Z} ויהי m_0\dots m_k\in\{0,1\} יהיו אלגוריתם כפל מספרים יהי אלגוריתם כפל איטרטיבי: יהי אלגוריתם כפל מספרים יהי
Algorithm ModIteratedSquaring [\mathcal{A}] (N, a, m):
      \begin{array}{l} a_0 \leftarrow a \\ r \leftarrow a_0^{m_0} \end{array}
      for i \in [1, \ldots, k] do
          a_i \leftarrow \mathcal{A}(a_{i-1}, a_{i-1}) \mod N
        if m_i = 1 then r \leftarrow \mathcal{A}(r, a_i^{m_i}) \mod N
.ModIteratedSquaring [\mathcal{A}] (N,a,(m)_2)=(a^m\mod N) איז n\in\mathbb{Z}/N ויהי n,m\in\mathbb{N} ויהי היי אלגוריתם כפל מספרים יהיו
                                        הינה ModIteratedSquaring איז סיבוכיות הריצה של איז ויהיו מספרים ויהיו אלגוריתם כפל מספרים ויהיו N,m\in\mathbb{N}
```

 $\mathcal{O}\left(\log\left(m\right)\cdot\log^2\left(N
ight)
ight)$ הינה ModIteratedSquaring [NaiveMul] מסקנה: יהיו איי סיבוכיות הריצה של

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

```
אזי N \in \mathbb{N}_+ אזי אלגוריתם חלוקה ניסיונית: אלגוריתם
Algorithm TrialDivision(N):
       for i \in [1, \ldots, \sqrt{N}] do
              (q,r) \leftarrow \text{RemainderDiv}(N,i)
              if r = 0 then return False
       end
       return True
                                                                                                                    .(TrialDivision (N)=	ext{True})\Longleftrightarrow (N\in\mathbb{P}) אזי N\in\mathbb{N}_+ יהי יהי N\in\mathbb{N}_+
                                                                                                                                             \mathcal{O}\left(2^{\frac{n}{2}}\right) הינה TrialDivision טענה: סיבוכיות הריצה של
                                                                      אזי a \in [N-1] ויהי N \in \mathbb{N}_+ אזי אלגוריתם חזקה אלגוריתם אלגוריתם מבחן פרמה: יהי
Algorithm FermatPrimalityTest [\mathcal{A}] (N: a):
       if A(N, a, N - 1) = 1 then return True
       return False
                                                                   \mathcal{O}\left(n^3
ight) הינה FermatPrimalityTest [ModIteratedSquaring [NaiveMul]] הינה של
                 \mathcal{O}\left(n^2\log\left(n\right)\log\log\left(n\right)\right) הינה FermatPrimalityTest [ModIteratedSquaring [CooleyTukeyMul]] אינה פיבוכיות הריצה של
                                                                                                     \mathbb{P}_{a\leftarrow \lceil N-1 \rceil} (FermatPrimalityTest (N;a)= True)=1 אזי N\in\mathbb{P} טענה: יהי N\in\mathbb{P}
                                          a^{N-1}\equiv 1\mod N מספר קרמייקל: מספר פריק N\in\mathbb{N}_+ עבורו לכל א המקיים a\in\mathbb{Z} מספר קרמייקל: מספר פריק
                            \mathbb{P}_{a\leftarrow [N-1]} (FermatPrimalityTest (N;a)= False) >rac{1}{2} אינו מספר קרמייקל אינ N אינו מספר אינו מיינו מיינו מספר אינו מיינו מספר אינו מיינו 
                                                                                                                                       .FermatPrimalityTest (F_k;2)= True אזי איזי k\in\mathbb{N} טענה: יהי k\in\mathbb{N}
                                                                                                                                     השערה פתוחה F_k\in\mathbb{P} עבורו k\in\mathbb{N}_{>5} השערה פתוחה
                                                                                                                                                 השערה פתוחה .|\{k\in\mathbb{N}\mid F_k\notin\mathbb{P}\}|=leph_0 :השערה
                        (p-1|N-1 מתקיים p|N מתקיים וכן לכל p\in\mathbb{N} המיים איז p\in\mathbb{N} מתקיים איז p\in\mathbb{N} מענה: יהי
                               מספר קרמייקל. (6k+1)\cdot (12k+1)\cdot (18k+1)\cdot (18k+1) איי איי (6k+1,12k+1,18k+1) מספר קרמייקל.
                                                                                                     השערה: \{k \in \mathbb{N} \mid 6k+1, 12k+1, 18k+1 \in \mathbb{P}\} = \aleph_0 השערה:
                                                                            משפט אלפורד־גרנוויל־פומרנץ: N\}|=leph_0: מספר קרמייקל אלפורד־גרנוויל־פומרנץ: N\}|=lpha_0
  משפט אלפורד־גרנוויל־פומרנץ: החל ממקום מסויים לכל x\in\mathbb{N} מתקיים x\in\mathbb{N} מספר קרמייקל החל ממקום מסויים לכל
                                                                                                         משפט ארדוש: קיים c>0 עבורו החל ממקום מסויים לכל מתקיים מתקיים
                                                                                   מספר קרמייקל .|\{N < x \mid N\}| < x \cdot \exp\left(rac{-c \cdot \log(x) \cdot \log\log\log(x)}{\log\log(x)}
ight)
                                                אזי a\in [N-1] ויהי וויהי אלגוריתם חזקה מודולרית יהי אלגוריתם היהי אלגוריתם אזי אלגוריתם אזי אלגוריתם אזי אלגוריתם אויהי
Algorithm SolovayStrassenPrimalityTest [\mathcal{A}] (N; a):
       if N=2 then return True
       if (N < 2) \lor (2|N) then return False
       s \leftarrow \text{JacobiSymbol}(a, N)
       if (s \neq 0) \land \left(\mathcal{A}\left(N, a, \frac{N-1}{2}\right) = (s \mod N)\right) then return True
       return False
                                                   \mathcal{O}\left(n^3
ight) הינה SolovayStrassenPrimalityTest [ModIteratedSquaring [NaiveMul]] אינה של
```

ModIteratedSquaring [CooleyTukeyMul] אי סיבוכיות הריצה של $N,m\in\mathbb{N}$ הינה

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

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

```
Algorithm MillerRabinPrimalityTest[\mathcal{A}] (N; a):
     if N=2 then return \operatorname{True}
     if (N < 2) \lor (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,\tilde{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
     return True
                                                                   \mathbb{P}_{a\leftarrow\mathbb{N}_{< N}} (MillerRabinPrimalityTest (N;a)= True)=1 אזי N\in\mathbb{P} טענה: יהי
                                        .|\{a\in\mathbb{N}_{< N}\mid 	ext{MillerRabinPrimalityTest}\,(N;a)=	ext{True}\}|\leq rac{arphi(N)}{4} פריק אזי N\in\mathbb{N} משפט רבין: יהי N\in\mathbb{N}
                                                        \mathbb{P}_{a\leftarrow\mathbb{N}_{< N}} (MillerRabinPrimalityTest (N;a)= False) >rac{3}{4} צריק אזי N\in\mathbb{N} מסקנה: יהי
                                                                                                      טענה: יהיk\in\mathbb{N}_{	ext{odd}} באשר צk\in\mathbb{N}_{	ext{odd}} אזי
                              . \big| \big\{ a \in \mathbb{N}_{<(2k+1)\cdot(4k+1)} \mid \mathsf{MillerRabinPrimalityTest}\left((2k+1)\cdot(4k+1)\,; a\right) = \mathsf{True} \big\} \big| = \frac{\varphi((2k+1)\cdot(4k+1))}{4}
                                                    אזי MillerRabinPrimalityTest (N;a)= True מענה: יהי n\in [N-1] ויהי N\in \mathbb{N}_+ יהי איזי איזי
                                                                                                                  .SolovayStrassenPrimalityTest (N; a) = True
באשר r:\mathbb{N}	o \{2^{n-1},\dots,2^n\}	imes\mathbb{N}^k ותהא ותהא n,k\in\mathbb{N}_+ באשר אלגוריתם חזקה מודולרית יהיי
                                                                                           אזי i \in \{2,\ldots,k+1\} ולכל (r\left(c\right))_{i} < (r\left(c\right))_{1}
Algorithm PrimeGenerator [\mathcal{A}] (n, k; r):
     c \leftarrow 0
     while True do
          b \leftarrow \mathsf{True}
          for i \in [2, \dots, k+1] do
           b \leftarrow b \land \text{MillerRabinPrimalityTest}[\mathcal{A}]((r(c))_1; (r(c))_i)
          if b = \text{True then return } (r(c))_1
          c \leftarrow c + 1
                         .2^{n-1}< PrimeGenerator (n,k;r)<2^n עוצר אזי PrimeGenerator (n,k;r) עובר אויהי n,k\in\mathbb{N}_+ טענה: יהיו
                         \mathbb{E}_r\left[\mathrm{Time}\left(\mathrm{PrimeGenerator}\left[\mathrm{ModIteratedSquaring}\left[\mathrm{NaiveMul}\right]\right](n,k;r)
ight)
ight]=\mathcal{O}\left(kn^4\right) אזי n,k\in\mathbb{N}_+ אזי n,k\in\mathbb{N}_+ אזי
                                                                           \mathbb{P}_r (PrimeGenerator (n,k;r)\in\mathbb{P})\geq 1-rac{1}{4^k} אזי n,k\in\mathbb{N}_+ טענה: יהיו
                                                                                                q \equiv 1 \mod p אזי q \mid 2^p - 1 באשר p, q \in \mathbb{P} טענה: יהיו
                                                        . פריק. p=2p-1 אזי q=2p+1 וכן p\equiv 3 \mod 4 באשר p,q\in \mathbb{P}_{>3} אזי q=2p+1 פריק.
                                                                                                                 M_n=2^n-1 אזי n\in\mathbb{N} מספר מרסן: יהי
                                                                    a,p=a^n-1 המקיימים a,n\in\mathbb{N}_+ עבורו קיימים עבורו ראשוני מרסן: ראשוני מרסן
                                                                                   p=2^q-1 טענה: יהי p\in\mathbb{P} ראשוני מרסן אזי קיים p\in\mathbb{P}
                                                                                                מסקנה: יהי p \in \mathbb{P} ראשוני מרסן אזי p \in \mathbb{P} הינו מספר מרסן.
                                                                                   . מושלם 2^{n-1}\cdot(2^n-1) אזי ראשוני אזי m\in\mathbb{N} מושלם מענה: יהי
```

```
Algorithm LucasLehmer [\mathcal{A}, \mathcal{B}] (n, 2^n - 1):
         if A(n) = False then return False
         S_0 \leftarrow 4
         for i \in [1, \ldots, n-2] do
          S_i \leftarrow (\mathcal{B}(2^n - 1, S_{i-1}, 2) - 2) \mod p
         if S_{n-2} = 0 then return True
        return False
                                                                                                             .(LucasLehmer (n,2^n-1)= True) \Longleftrightarrow (2^n-1\in \mathbb{P}) אזי n\in \mathbb{N} יהי n\in \mathbb{N} יהי
                                                              \mathcal{O}\left(n^3
ight) הינה LucasLehmer [TrialDivision, ModIteratedSquaring [NaiveMul]] אינה של
       \mathcal{O}\left(n^2\log\left(n\right)\log\log\left(n\right)\right) הינה LucasLehmer [TrialDivision, ModIteratedSquaring [CooleyTukeyMul]] הינה הריצה של
                                                                                                                                                                                                                         .2^{136276841} - 1 \in \mathbb{P} :
                                                                                                                                                   .\mathcal{\tilde{O}}\left(n^{lpha}
ight)=\mathcal{O}\left(n^{lpha}
ight)\cdot\operatorname{poly}\left(\log\left(n
ight)
ight) אזי lpha\in\mathbb{R}_{+} יהי הגדרה: יהי
                                          	ilde{\mathcal{O}}\left(n^6
ight) משפט אגרוול־קיאל־סקסנה: קיים אלגוריתם דטרמיניסטי AKS משפט אגרוול־קיאל־סקסנה: פיים אלגוריתם בערמיניסטי
                         E(E,D) אזי p,k\in\mathbb{F}_2^n לכל D(E(p,k),k)=p באשר באשר באשר E,D:\mathbb{F}_2^n	o\mathbb{F}_2^n	o\mathbb{F}_2^n ותהיינה n\in\mathbb{N} ותהיינה
p\in\mathbb{F}_2^n לכל D\left(E\left(p,k_e
ight),k_d
ight)=p באשר באשר באשר E,D:\mathbb{F}_2^n	imes\mathbb{F}_2^m	o\mathbb{F}_2^n ותהיינה ותהיינה ותהיינה ואסימטרית: יהיו יהיו וותהיינה ותהיינה וותהיינה וותהיינה
i\in[k] אזי p_i\in\mathbb{P} וכן \prod_{i=1}^kp_i=N באשר \mathrm{IFP}\left(N
ight)=(p_1,\ldots,p_k) אזי N\in\mathbb{N}_+ יהי הפירוק: יהי N\in\mathbb{N}_+ יהי N\in\mathbb{N}_+ אזי N\in\mathbb{N}_+ אזי N\in\mathbb{N}_+ באיית הפירוק בעל סיבוכיות ריצה N\in\mathbb{N}_+ פטענה נפת שדות המספרים: קיים n=1 עבורו קיים אלגוריתם n=1 לבעיית הפירוק בעל סיבוכיות ריצה n=1
רב A:\mathbb{F}_2^*	imes\mathbb{F}_2^*	o\mathbb{F}_2^* יהיו ed\equiv 1\mod arphi(n) וכן (e,arphi(pq))=1 באשר e,d\in\mathbb{N} יהיו p,q\in\mathbb{P} יהיו יהיו יהיו
                                                                                                                                                     A(A, A, (pq, e), (pq, d)) אאי A(c, (M, a)) = c^a \mod M
                                                           סטענה: יהיו \mathbb{R} ותהא (M,M,k_e,k_d) הצפנת RSA אזי ותהא (M,M,k_e,k_d) הינה הצפנה אסימטרית.
                                                                                  \operatorname{KSA} טענה: יהיו p,q\in\mathbb{P} ותהא (M,M,k_e,k_d) הצפנת אזי יהיו p,q\in\mathbb{P}
משפט: יהיו (קיים אזי (קיים אזי A^M בעל כוח חישובי T:\mathbb{N}	o\mathbb{N} ותהא תהא (M,M,k_e,k_d) הצפנת p,q\in\mathbb{P} האינ
                       .(\mathcal{A}^{M(\cdot,k_e)}\left(1^n
ight)=\mathrm{IFP}\left(N
ight) המקיים \mathcal{\tilde{O}}\left(T
ight) בעל כוח חישובי \mathcal{A}^M בעל לפיים יריב \mathcal{A}^{M(\cdot,k_e)}\left(1^n
ight)=k_d המקיים \mathcal{\tilde{O}}\left(T
ight)
                         a=g^x \mod p באשר x\in \mathbb{N}_{\leq p} אזי a\in (\mathbb{Z}/p\mathbb{Z})^	imes ויהי p\in \mathbb{Z} ויהי שורש פרימיטיבי מודולו p ויהי שורש מודולו p ויהי
a טענה: יהי p\in\mathbb{P} יהי a שורש פרימיטיבי מודולו a יהי a\in(\mathbb{Z}/p\mathbb{Z})^{	imes} יהי a\in(\mathbb{Z}/p\mathbb{Z})^{	imes} יהי a\in(\mathbb{Z}/p\mathbb{Z})^{	imes} יהי
                                                                                                                                                                                                                                                       x=y אזי q
x\in\mathbb{N}_{\leq p} באשר \mathrm{DLP}\left(p,g,a
ight)=x אזי a\in\left(\mathbb{Z}/p\mathbb{Z}
ight)^{	imes} בעיית הלוגריתם הדיסקרטי: יהי p\in\mathbb{P} יהי יהי p\in\mathbb{P} יהי
                                                                                                                                                                        g בבסיס בסינו הלוגריתם הדיסקרטי של a מודולו
טענה נפת שדות המספרים: קיים לבעל סיבוכיות באשר לבל באשר לבעל סיבוכיות ריצה בעל סיבוכיות ריצה בעל סיבוכיות ריצה ווענה נפת שדות המספרים: לבעל סיבוכיות היים אלגוריתם בא
\mathcal{O}\left(\exp\left(c\cdot\log^{\frac{1}{3}}\left(p
ight)\cdot\log^{\frac{2}{3}}\left(p
ight)
ight)
ight) פרוטוקול תקשורת דיפי־הלמן: יהי p\in\mathbb{P} ויהי p שורש פרימטיבי מודולו p אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים
                                                                                                                                                                                                                                                    כך \Pi_{	ext{DiffieHellman}}
Communication Protocol \Pi_{\texttt{DiffieHellman}}(p,g):
         A draws x \in [p-1]
         A sends (g^x \mod p) as K_A
         B draws y \in [p-1]
```

 $K_{AB}=K_{BA}$ אזי $\Pi_{ ext{DiffieHellman}}\left(p,g
ight)=\left(K_{AB},K_{BA}
ight)$ באשר באשר K_{AB} באשר K_{AB} ויהיי $M_{ ext{DiffieHellman}}\left(p,g
ight)=\left(K_{AB},K_{BA}
ight)$ באשר M_{AB} באשר M_{AB} ויהיי M_{AB} שורש פרימטיבי מודולו M_{AB} תהא M_{AB} תהא M_{AB} חשיבה בזמן עבורה קיים יריב M_{AB} בעל כוח חישובי M_{AB} המקיים M_{AB} המקיים M_{AB} בעל כוח חישובי M_{AB} המקיים M_{AB} המקיים M_{AB} בעל כוח חישובי M_{AB} המקיים M_{AB} המקיים M_{AB} בעל כוח חישובי M_{AB} המקיים M_{AB} המקיים יריב M_{AB} בעל כוח חישובי M_{AB} המקיים M_{AB}

B sends $(g^y \mod p)$ as K_B A calculates $K_{BA} \leftarrow (K_B)^x$ B calculates $K_{AB} \leftarrow (K_A)^y$

 $C_p : \mathbb{F}^*_2 imes \mathbb{F}^*_2 o \mathbb{F}^*_2$ ונגדיר $x \in \mathbb{N}_{< p}$ והצפנת שורש פרימטיבי שורש פרימטיבי ודולו $x \in \mathbb{N}_{< p}$ יהי $p \in \mathbb{P}$ יהי וואר יהי $E(c,(\alpha,\beta,\gamma))=((c\cdot\gamma^y)\mod \alpha,\beta^y\mod \alpha)$ אזי $y\in\mathbb{N}_{< p}$ יהי • $D((c_1, c_2), (\alpha, \beta, \gamma)) = (c_1 \cdot c_2^{-\gamma}) \mod \alpha \bullet$ $(E, D, (p, q, q^x \mod p), (p, q, x))$ אזי . אינה חד־מימדית אינה יריעה $\{(x,y)\in\mathbb{R}^2\mid y^2=f\left(x\right)\}$ אינה אוי פעל שורש מרובה אי $f\in\mathbb{R}\left[x\right]$ אינה אינה יריעה חד־מימדית אירה. עקום אליפטי: יהי $\mathbb F$ שדה באשר $f\in\mathbb F[x]$ ויהי ויהי $f\in\mathbb F[x]$ ויהי אוירים פשוטים מעל דה שדה באשר אליפטי: יהי $\{(x,y) \in \mathbb{F}^2 \mid y^2 = f(x)\} \cup \{\infty\}$ E/\mathbb{F} אזי אזי אויפטי מעל \mathbb{F} אזי אויהי אויהי char $(\mathbb{F}) \neq 2$ אזי שדה באשר באשר . יריעה חד־מימדית חלקה אזי $E \setminus \{\infty\}$ עקום אליפטי אזי $E \setminus \{\infty\}$ אז $P \in E$ אז עקום אליפטי ותהא E יהי איקוף: יהי -P=P אזי $P=\infty$ אם -P = (x, -y) אז P = (x, y) אם • A-(-P)=P וכן $A-P\in E$ אזי איזי אליפטי ויהי אליפטי ויהי עקום אליפטי ויהי $(\mathrm{line}_{P,Q}\setminus\{P,Q\})\cap E
eq arnothing$ איי $P
eq \pm Q$ באשר $P,Q\in E\setminus\{\infty\}$ טענה: יהי P עקום אליפטי ותהיינה $.(T_P\left(Eackslash\{\infty\})\setminus\{P\})\cap E
eqarnothing$ אזי P
eq -P באשר $P\in E\setminus\{\infty\}$ נענה: יהי E עקום אליפטי ותהא אז $P,Q\in E$ אז עקום אליפטי ותהיינה אינה עקום הגדרה חיבור: יהי $.P+Q=\infty$ אזי $\infty\in\{P,Q\}$ אם • $P+Q=\infty$ אזי אם P=-Q וכן 0P+Q=-R אזי $R\in (\mathrm{line}_{P,Q}\backslash \{P,Q\})\cap E$ תהא $P
eq \pm Q$ וכן $\infty \notin \{P,Q\}$ אם Φ P+Q=-R אזי $R\in ((T_P(E\backslash \{\infty\})\backslash \{P\})\cap E)$ תהא $P\neq -Q$ וכן P=Q וכן 0P+Q=Q+P אזי איי עקום אליפטי ותהיינה על עקום אזי אזי איינה: יהי עקום אליפטי ותהיינה P(Q+Q)+R=P+(Q+R) אזי איזי אינה: יהי $P(Q,R\in E)$ טענה: יהי אליפטי ותהיינה . תבורה אבלית עקום אזי אזי עקום אליפטי אזי ההיEיהי יהי מסקנה: יהי $|E|=p+1+\sum_{x\in\mathbb{F}_p}\left(rac{f(x)}{p}
ight)$ אזי f ידי אל אליפטי המוגדר על אליפטי E/\mathbb{F}_p ויהי ויהי ויהי אליפטי המוגדר על ידי איזי איזי ויהי $\left|\sum_{x\in\mathbb{F}_p}\left(rac{f(x)}{p}
ight)
ight|\leq 2\sqrt{p}$ אזי $\overline{\mathbb{F}_p}$ אזי $p\in\mathbb{F}_{>2}$ וכן $f\in\mathbb{F}_p$ וכן $f\in\mathbb{F}_p$ באשר $f\in\mathbb{F}_p$ ויהי $p+1-2\sqrt{p} \leq |E| \leq p+1+2\sqrt{p}$ מסקנה: יהי $p \in \mathbb{P}_{>2}$ ויהי $p \in \mathbb{P}_{>2}$ עקום אליפטי אזי $\mathcal{O}\left(\log\left(n\right)\cdot\log^2\left(p\right)\right)$ ECDLP(p, E, G, nG) = n

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

אזי $n\in\mathbb{N}_+$ יהי ויהי אליפטי יהי עקום אליפטי יהי $p\in\mathbb{P}_{>2}$ יהי אליפטיים: יהי אליפטיים: יהי אליפטיים: יהי

 $\mathcal{O}\left(\sqrt{p}
ight)$ באשר ריצה $p\in\mathbb{P}_{>2}$ מתקיים כי בנכטות ריצה בCDLP טענה: קיים אלגוריתם ל-אזי $G\in Eackslash \{\infty\}$ ויהי f ויהי אליפטי המוגדר על אזי איהי $p\in \mathbb{P}_{>2}$ יהי יהי אליפטי המוגדר על ידי ויהי כך $\Pi^{ ext{EC}}_{ ext{DiffieHellman}}$ כדיים פרטיים מפתחות בעל מפתחות נגדיר

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

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 $K_{AB} \leftarrow y \cdot K_A$

 $\Pi^{ ext{EC}}_{ ext{DiffieHellman}}\left(p,g
ight)=$ יהי E/\mathbb{F}_p יהי $f\in\mathbb{F}_{>2}$ יהי $f\in\mathbb{F}_{>2}$ יהי $f\in\mathbb{F}_{>2}$ יהי $f\in\mathbb{F}_{>2}$ יהי ויהי $.K_{AB}=K_{BA}$ אז (K_{AB},K_{BA})

 $\tilde{\mathcal{O}}\left(T
ight)$ המקיים ביריב \mathcal{A} שורש פרימטיבי מודולו $p\in\mathbb{R}$ תהא \mathcal{A} חשיבה בזמן עבורה קיים יריב \mathcal{A} בעל כוח חישובי \mathcal{A} המקיים טענה: יהי $\mathcal{B}(p,f,G,xG,yG)=xyG$ המקיים $\tilde{\mathcal{O}}(T)$ העל כוח חישובי בעל כוח אזי קיים יריב \mathcal{B}

```
\lim_{x	o\infty}rac{f(x)}{g(x)}=1 המקיימות f,g:\mathbb{R}	o\mathbb{R} פונקציות אסימפטוטיות: פונקציות פונקציות החימפטוטיות:
                                                                                                                                            f,g:\mathbb{R} 
ightarrow \mathbb{R} אסימפטוטיות אזי קימון: תהיינה
                                             \limsup_{x	o\infty}rac{f(x)}{g(x)}\le 1 המקיימת g:\mathbb{R}	o\mathbb{R} אזי f:\mathbb{R}	o\mathbb{R} הוא הוא הסימפטוטית: תהא
                                                                                     f,g:\mathbb{R} 	o \mathbb{R} אזי איזי אסימפטוטית אסימפטוטית באשר לf,g:\mathbb{R} 	o \mathbb{R} איזי
                                                                                                  (f\lesssim g)\Longleftrightarrow \left(\liminf_{x	o\infty}rac{g(x)}{f(x)}\geq 1
ight) איי f,g:\mathbb{R}	o\mathbb{R} טענה: תהיינה
                                        (f\lesssim g)\Longleftrightarrow (orallarepsilon>0.\exists x\in\mathbb{R}.orall y>x. \ (f\left(y
ight)\leq \left(1+arepsilon
ight)g\left(y
ight))) אזי f,g:\mathbb{R}
ightarrow\mathbb{R} טענה: תהיינה
                                                                                                           (f\sim g)\Longleftrightarrow ((f\lesssim g)\land (g\lesssim f)) אזי f,g:\mathbb{R}\to\mathbb{R} טענה: תהיינה
                                                                                                                                                                                                          .\log = \ln הערה: בקורס זה
                                                                                                                                                   \pi\left(2n
ight)-\pi\left(n
ight)\leqrac{\log(4)\cdot n}{\log(n)} אזי n\in\mathbb{N}_{+} יהי \pi\left(2n
ight)-\pi\left(n
ight)\leqrac{\log(4)\cdot x}{\log(x)} משפט צ'בישב: \pi\left(x
ight)\lesssimrac{\log(4)\cdot x}{\log(x)}
                                                                                                                                     \sum_{p\in\mathbb{P}_{\leq x}}\log\left(p
ight) pprox \log\left(x
ight) מסקנה: \sum_{p\in\mathbb{P}_{\leq x}}\log\left(p
ight) \lesssim \log\left(4
ight) \cdot x מסקנה: יהי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} למה: יהי n\in\mathbb{N}_{+} ויהי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} למה: יהי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} למה: יהי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+} אזי n\in\mathbb{N}_{+}
                                                                                                                                     .e_p\left(inom{2n}{n}
ight) \leq \log_p\left(2n
ight) אזי p \in \mathbb{P} ויהי n \in \mathbb{N}_+ למה: יהי
                                                                                                                                                          0 \leq \log_p(2n) אוי n \in \mathbb{N} אוי n \in \mathbb{N}_+ טענה: יהי n \in \mathbb{N}_+ אוי n \in \mathbb{N}_+ משפט צ'בישב: \frac{\log(2) \cdot x}{\log(x)} \gtrsim \frac{\log(2) \cdot x}{\log(x)}
            מתקיים n\in\mathbb{N}_{\geq 2} עבורם לכל עבורם eta\in\mathbb{R}_{\geq 1} וקיים lpha\in(0,1] מתקיים הפיכה ושומרת סדר אזי קיים \alpha\in(0,1]
                                                                                                                                                                                         .\alpha n \log(n) \le f(n) \le \beta n \log(n)
                                                משפט סכימה בחלקים/נוסחת אבל: יהי x\in\mathbb{R}_{\geq 1} תהא a:\mathbb{N}	o\mathbb{C} תהא x\in\mathbb{R}_{\geq 1} אזי אינ
                                                                                 \sum_{n\in\mathbb{N}_{\leq x}}\left(a_{n}\cdot f\left(n
ight)
ight)=\left(\sum_{n\in\mathbb{N}_{\leq x}}a_{n}\right)\cdot f\left(x
ight)-\int_{1}^{x}\left(\sum_{n\in\mathbb{N}_{\leq t}}a_{n}\right)\cdot f'\left(t
ight)\mathrm{d}t .log (n!)=n\cdot\log\left(n
ight)+\mathcal{O}\left(n
ight)
                                                                                                                                                         \log(n!) = n \cdot \log(n) - n + \mathcal{O}(\log(n)) טענה:
                                                                                       \sum_{p\in\mathbb{P}_{\leq x}}rac{\log(p)}{p}=\log\left(x
ight)+\mathcal{O}\left(1
ight)משפט מרטנס: \sum_{p\in\mathbb{P}_{\leq x}}rac{1}{p}=\log\log\left(x
ight)+c+\mathcal{O}\left(rac{1}{\log(x)}
ight) עבורו c>0 עבורו
                                                                                                       .\prod_{p\in\mathbb{P}_{\leq x}}\left(1-rac{1}{p}
ight)\simrac{K}{\log(x)} עבורו עבורו K>0 משפט: קיים c>0 עבורו לכל מסקנה: קיים c>0 עבורו לכל מחקיים מחקיים
                                                                                                                            \log\log(n) .lcm (1,\ldots,n)\geq 2^{n-2} אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ מסקנה: יהי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי קבוע אויילר־מסקרוני: נגדיר n\in\mathbb{N}_+ כך אויילר־מסקרוני: נגדיר n\in\mathbb{N}_+
                                                                                                                              \gamma=\lim_{n	o\infty}\left(\left(\sum_{i=1}^nrac{1}{i}
ight)-\log\left(n
ight)
ight) טענה: \prod_{p\in\mathbb{P}_{\leq x}}\left(1-rac{1}{p}
ight)\simrac{e^{-\gamma}}{\log(x)} לא הוכח בקורס .c\geq 1 אזי אם c\in\mathbb{R} אזי אס c\in\mathbb{R} אזי אס
                                                                                                                                                   c \leq 1 אז \pi\left(x
ight) \gtrsim rac{c \cdot x}{\log(x)}טענה: יהי c \in \mathbb{R} אזי אם
                                                                                                                                               c=1 אז \pi\left(x
ight)\simrac{c}{\log\left(x
ight)}מסקנה: יהי c\in\mathbb{R} אזי אם c\in\mathbb{R}
                                                                                                                             משפט המספרים הראשוניים: \pi\left(x
ight)\sim rac{x}{\log(x)} לא הוכח בקורס
                                                               [n,(1+arepsilon)\,n]\cap\mathbb{P}
eqarnothing מתקיים n\in\mathbb{N}_{\geq N} עבורו לכל N\in\mathbb{N} אזי קיים arepsilon>0 אזי איי קיים אזי לכל
                                                                                                                   \mathrm{Li}\left(x
ight)=\int_{2}^{x}rac{1}{\log(t)}\mathrm{d}t כך בי \mathrm{Li}:\mathbb{R}	o\mathbb{R} האינטגרל הלוגריתמי: נגדיר
                                                                                                                                                        	ext{Li}\left(x
ight) = rac{x}{\log(x)} + rac{x}{\log^2(x)} + \mathcal{O}\left(rac{x}{\log^3(x)}
ight)מסקנה: 	ext{Li}\left(x
ight) \sim rac{x}{\log(x)}
                                                                                                              \operatorname{Li}(x) = \sum_{k=0}^m rac{(m-1)! \cdot x}{\log^m(x)} + \mathcal{O}\left(rac{x}{\log^{m+1}(x)}
ight) אזי m \in \mathbb{N} טענה: יהי
משפט אדמר־דה-לה-ואלה-פוסן: קיים c>0 עבורו \pi\left(x
ight)=\mathrm{Li}\left(x
ight)+\mathcal{O}\left(x\cdot\exp\left(-c\cdot\sqrt{\log\left(x
ight)}
ight)
ight) שבורו לה-ואלה-פוסן: קיים
```

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

```
\pi\left(x
ight)=rac{x}{\log(x)}+rac{x}{\log^2(x)}+\mathcal{O}\left(rac{x}{\log^3(x)}
ight) מסקנה:
                                                           משפט וינוגרדוב: יהי \pi\left(x
ight)=\mathrm{Li}\left(x
ight)+\mathcal{O}\left(x\cdot\exp\left(-\log^{rac{2}{3}+arepsilon}\left(x
ight)
ight)
ight) אזי arepsilon>0 אזי arepsilon>0 אזי
                                                                                                            השערה פתוחה \pi\left(x\right) \doteq \mathrm{Li}\left(x\right) + \mathcal{O}\left(\sqrt[]{x}\cdot\log\left(x\right)\right) השערה פתוחה השערת רימן
                                                                     \pi_{m,a}\left(x
ight)=|\mathbb{P}_{\leq x}\cap\left(m\mathbb{N}+a
ight)| כך \pi_{m,a}:\mathbb{R}	o\mathbb{N} איי נגדיר a\in\mathbb{Z} איי ויהי m\in\mathbb{N} ייהי m\in\mathbb{N}
                                                                                                 \pi_{m,a}\left(\infty
ight)=\lim_{x	o\infty}\left|\mathbb{P}_{< x}\cap\left(m\mathbb{N}+a
ight)
ight| אזי a\in\mathbb{Z} ויהי m\in\mathbb{N} ויהי m\in\mathbb{N}
                                                                                                                  \pi_{m,a}\left(\infty
ight) \leq 1 אזי (m,a)>1 באשר a\in\mathbb{Z} ויהי m\in\mathbb{N} טענה: יהי
                                                             משפט דיריכלה: יהי m\in\mathbb{N} ויהי a\in\mathbb{Z} באשר a\in\mathbb{Z} אזי a\in\mathbb{Z}. לא הוכח בקורס
                                משפט דה-לה-ואלה-פוסן/המספרים הראשוניים בסדרות חשבוניות: יהי m\in\mathbb{N} ויהי באשר באשר האוי משפט דה-לה-ואלה-פוסן/המספרים הראשוניים בסדרות חשבוניות: יהי
                                                                                                                                                                      לא הוכח בקורס .\pi_{m,a}\left(x
ight)\simrac{x}{arphi\left(m
ight)\cdot\log\left(x
ight)}
                                                                                             \pi_{m,a}\left(x
ight)\simrac{1}{arphi(m)}{
m Li}\left(x
ight) איי (a,m)=1 באשר a\in\mathbb{Z} מסקנה: יהי
\pi_{m,a}(x)=rac{1}{\wp(m)}{
m Li}(x)+\mathcal{O}(\sqrt{x}\cdot\log(x)) אזי איי (a,m)=1 באשר a\in\mathbb{Z} ויהי m\in\mathbb{N} יהי (GRH): יהי
לכל MillerRabinPrimalityTest (N;a)= True)\Longleftrightarrow (N\in\mathbb{P}_+ מתקיים N\in\mathbb{N}_+ עבורו לכל c>0 אז קיים C>0 משפט: אם GRH משפט:
                                                                                                                                                                                     לא הוכח בקורס.(a < c \log^2(N)
                                                   \tilde{\mathcal{O}}\left(n^4
ight) אז קיים אלגוריתם דטרמיניסטי לבדיקת לבדיקת אוניות בעל היים אלגוריתם דטרמיניסטי אלגוריתם לבדיקת אז קיים אלגוריתם דטרמיניסטי
                                                                                                                        f=0 אזי f\in\mathbb{Z}\left[x_1,\ldots,x_n
ight] ויהי ויהי n\in\mathbb{N} אזי אזי
                                                          \mathrm{sols}_{\mathbb{Z}}\left(f=0
ight)=arnothing אזי \mathrm{sols}_{\mathbb{Z}_{N}}\left(f=0
ight)=arnothing באשר N\in\mathbb{N}_{\geq2} ויהי f\in\mathbb{Z}\left[x_{1},\ldots,x_{n}
ight] איזי
                                                                                                \{\langle f 
angle \mid (f \in \mathbb{Z}\left[x_1,\ldots,x_n
ight]) \land (\operatorname{sols}_{\mathbb{Z}}\left(f=0
ight) 
eq arnothing)\} 
otin \mathcal{R} משפט מטיאסביץ':
         a\in S^n עבורם a\in R^{n+1} וקיים הומוגני בשני משתנים: יהי a\in R חוג אזי וf\in R עבורו קיים f\in R עבורו אזי ואיי
                                                                                                 f=0 הומוגני אזי f\in\mathbb{Z}\left[x,y
ight] היהי בשני משתנים: יהי
                                                 .(f(\lambda x,\lambda y)=\lambda^{\deg(f)}\cdot f(x,y) מתקיים x,y,\lambda\in\mathbb{R} טענה: יהי f\in\mathbb{Z}[x,y] אזי לכל
                                                 .f\left(rac{a}{(a,b)},rac{b}{(a,b)}
ight)=0 אאי f\left(a,b
ight)=0 באשר a,b\in\mathbb{Z}\backslash\left\{0
ight\} הומוגני ויהיו f\in\mathbb{Z}\left[x,y
ight] איזי f\left(a,b
ight)=0 הומוגני ויהיו f\left(a,b
ight)=0 הומוגני אאי f\left(a,b
ight)\in\mathbb{Z}^{2} הומוגני היי f\left(a,b
ight)=0 הומוגני הומוגני היי הומוגני איי
                                                                                               f=\sum_{i=0}^n \zeta_i x^i y^{n-i} טענה: יהי f\in\mathbb{Z}[x,y] הומוגני ויהי הומוגני יהי
                                                                                     \operatorname{sols}_{\mathbb{Z}}(f=0) = \{(da,db) \mid (d \in \mathbb{Z}) \land (f=0)  פתרון פרימיטיבי של (a,b)) •
                                                                                                                    a|\zeta_n וכן a|\zeta_0 מתקיים f=0 של (a,b) וכן •
                                                                                                                                      f=0 אזי f\in\mathbb{Z}\left[x
ight] אזי במשתנה אחד: יהי
       a|\zeta_n וכן a|\zeta_0 אזי a|\zeta_0 אזי a|\zeta_0 אזי וכן a|\zeta_0 אזי a|\zeta_0 וכן a|\zeta_0 וכן וכן a|\zeta_0 יהי a|\zeta_0 אזי a|\zeta_0 באשר a|\zeta_0 באשר a|\zeta_0 וכן וכן a|\zeta_0
                                                   m|\zeta_0 אזי f\left(m
ight)=0 באשר m\in\mathbb{Z} ויהי f=\sum_{i=0}^n\zeta_ix^i באשר באשר f\in\mathbb{Z}[x] אזי f\in\mathbb{Z}[x]
                                                                                                             f=0 אזי f\in\mathbb{Z}_{\leq 1}\left[x,y
ight] יהי ששתנים: יהי לינארית בשני משתנים:
          (\operatorname{sols}_{\mathbb{Z}}(ax+by=c) \neq \varnothing) \iff ((a,b)|c) איזי (a,b,c \in \mathbb{Z}) איזי (ax+by=c) = \left\{\left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) \ \middle| \ m \in \mathbb{Z}\right\} איזי (\alpha,\beta) \in \operatorname{sols}_{\mathbb{Z}}(ax+by=c) איזי (a,b,c \in \mathbb{Z}) היהי (ax+by=c) = \left\{\left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) \ \middle| \ m \in \mathbb{Z}\right\} איזי (ax+by=c) = \left\{\left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) \ \middle| \ m \in \mathbb{Z}\right\} איזי (ax+by=c) = \left\{\left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) \ \middle| \ m \in \mathbb{Z}\right\} איזי (ax+by=c) = \left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) איזי (ax+by=c) = \left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) איזי (ax+by=c) = \left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right) איזי (ax+by=c) = \left(\alpha + \frac{m \cdot b}{(a,b)}, \beta - \frac{m \cdot a}{(a,b)}\right)
                                                                                                             f=0 אזי f\in\mathbb{Z}_{\leq 2}\left[x,y
ight] אזי משוואה דיופנטית ריבועית בשני משתנים: יהי
                                                                               טענה: יהי מהבאים מהבאים עבורם lpha,eta,\gamma,\delta,arepsilon,\zeta\in\mathbb{Q} אזי קיימים f\in\mathbb{Z}_{<2}\left[x,y
ight] יהי
                                                                                                            f(\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \zeta) = y - x^2 מתקיים x, y \in \mathbb{Z} לכל
                                                f(\alpha x + \beta y + \gamma, \delta x + \varepsilon y + \zeta) = x^2 - dy^2 - a מתקיים x, y \in \mathbb{Z} עבורם לכל a, d \in \mathbb{Z}
                                                                                                                                                           \operatorname{sols}_{\mathbb{Z}}\left(y=x^{2}\right)=\left\{ \left(m,m^{2}\right)\mid m\in\mathbb{Z}
ight\} :טענה
                                                                                                                                   (\operatorname{sols}_{\mathbb{Z}}(x^2=a)\neq\varnothing)\Longleftrightarrow (a=\square) אזי a\in\mathbb{Z} טענה: יהי
                                                                                                                         \mathrm{sols}_{\mathbb{Z}}\left(x^{2}=a
ight)=\{\pm\sqrt{a}\} אזי a=\square באשר a\in\mathbb{Z} יהי מסקנה: יהי
 \operatorname{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\{\pm1\}\right)\wedge\left(-\sqrt{\left|\frac{a}{d}\right|}\leq y\leq\sqrt{\left|\frac{a}{d}\right|}
ight)
ight\} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0} אזי d\in\mathbb{Z}_{<0}
                           \operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=0
ight)=\left\{\left(sm\cdot\sqrt{d},rm
ight)\,\Big|\,\left(s,r\in\{\pm1\}
ight)\wedge\left(m\in\mathbb{Z}
ight)
ight\} אזי d=\square באשר של באשר מסקנה: יהי d\in\mathbb{N}_+ אזי
                                        \operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=a
ight)=igcup_{\substack{(u,v)\in\mathbb{Z}^2\ a=uv}}\operatorname{sols}_{\mathbb{Z}}\left(\left\{egin{array}{l} x-\sqrt{d}y=u\ x+\sqrt{d}y=u \end{array}
ight) אזי d=\square אזי a\in\mathbb{Z} ויהי a\in\mathbb{Z} ויהי a\in\mathbb{Z} ויהי a\in\mathbb{Z}
```

```
d = 1 אזי d \neq d = 1 באשר d \in \mathbb{N}_+ משוואת פל: יהי
                                                                                                                     a^2-dy^2=a אזי d
eq\square באשר באשר d\in\mathbb{N}_+ ויהי a\in\mathbb{Z}\setminus\{0\} אזי משוואת פל מוכללת: יהי
                                                                                                                                                                                 \mathbb{Z}\left[\sqrt{d}
ight]=\mathbb{Z}+\sqrt{d}\cdot\mathbb{Z} אזי d
eq\square באשר באשר d\in\mathbb{Z} יהי יהי
                                                                                                                                                                                                                 טענה: יהי\mathbb{Z}\left[\sqrt{d}
ight] אזי d
eq \square חוג. d\in\mathbb{Z}
                                                               lpha=\delta וכן lpha=\gamma אזי lpha+eta\sqrt{d}=\gamma+\delta\sqrt{d} באשר lpha,eta,\gamma,\delta\in\mathbb{Z} ויהיו d
eq\square אזי מענה: יהי d\in\mathbb{Z}
                                                                   -arphi\left(lpha+eta\sqrt{d}
ight)=(lpha,eta) כך כך arphi: \mathbb{Z} באשר באשר שאי נגדיר d
eq \square אזי נגדיר d
eq \square
                                                                                                                                       ע ועל. \varphi מסקנה: יהי d \in \mathbb{Z} באשר ותהא d \neq \square ותהא לא יהי באשר ותהי יהי
                                                                                                                  (lpha,eta)\mapsto lpha+eta\sqrt{d} כך \mathbb{Z}\left[\sqrt{d}
ight] כדערה: יהי d
eq\square באשר באשר לשכן את משרה d\in\mathbb{Z}
                                                                                                                                        \overline{a}, \overline{a}, \overline{b}, \overline{d} = \alpha - \beta \sqrt{d} אזי \alpha, \beta \in \mathbb{Z} ויהיו d 
eq \square באשר באשר מיה: יהי d \in \mathbb{Z}
                                                               \overline{lphaeta}=\overline{lpha}\cdot\overline{eta} וכן \overline{lpha+eta}=\overline{lpha}+\overline{eta} וכן \overline{(\overline{lpha})}=lpha ויהיו d
eq \mathbb{Z} ויהיו d
eq \mathbb{Z} ויהיו d
eq \mathbb{Z}
                                                                                                                                    (\overline{lpha}=lpha)\Longleftrightarrow (lpha\in\mathbb{Z}) אזי lpha\in\mathbb{Z} ויהי d
eq\square ויהי ויהי d
eq\square אזי d\in\mathbb{Z}
                                                . מסקנה: יהי f אזי f אזי f הינו אוטומורפיזם חוגים. f:\mathbb{Z}\left[\sqrt{d}
ight]	o\mathbb{Z}\left[\sqrt{d}
ight] ונגדיר ונגדיר d
eq \square אזי d\in\mathbb{Z} אזי d\in\mathbb{Z} מסקנה: יהי
                                        N(lpha)=lpha\cdot\overline{lpha} כך N:\mathbb{Z}\left[\sqrt{d}
ight]	o\mathbb{Z} אזי נגדיר lpha\in\mathbb{Z}\left[\sqrt{d}
ight] כך מורמה בחוג d
eq \mathbb{Z} יהיd\in\mathbb{Z} יהי
                                                                                                                        N\left(lphaeta
ight)=N\left(lpha
ight)N\left(eta
ight) אזי lpha,eta\in\mathbb{Z}\left[\sqrt{d}
ight] ויהיו d
eq\square באשר באשר ל
                                                                                                                     \mathbb{Z}\left[\sqrt{d}
ight]^{	imes}=\left\{lpha\in\mathbb{Z}\left[\sqrt{d}
ight]\;\middle|\;N\left(lpha
ight)\in\{\pm1\}
ight\} אזי d
eq\square באשר של d\in\mathbb{Z} יהי d\in\mathbb{Z}
                                                                                                                                                                                          \mathbb{Z}ig[\sqrt{d}ig]^	imes = \left\{egin{array}{ll} \{\pm 1, \pm i\} & d=-1 \ \{\pm 1\} & d<-1 \end{array}
ight. אזי d\in\mathbb{Z}_{<0} מסקנה: יהי
\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=a
ight)=\left\{g\in\mathbb{Z}\left[\sqrt{d}
ight]\,\Big|\,\,N\left(g
ight)=a
ight\} אזי d
eq\mathbb{Z} אזי d\in\mathbb{Z} וכן d\in\mathbb{Z} וכן d\in\mathbb{Z} אזי a,b\in\mathbb{Z}\setminus\{0\} אזי a,b\in\mathbb{Z}\setminus\{0\} אזי a,b\in\mathbb{Z}\setminus\{0\} וכן a,b\in\mathbb{Z}\setminus\{0\} אזי
                                                                                                                                                                                                                                                .(\alpha \gamma + d\beta \delta)^{2} - d(\alpha \delta + \beta \gamma)^{2} = ab
                                                                       כך \mathrm{SG}:\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1
ight)^2	o\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1
ight) כך איי גאדיה באשר d\in\mathbb{Z} איי נגדיר d
eq \mathbb{Z}
                                                                                                                                                                                                                         .SG((\alpha,\beta),(\gamma,\delta)) = (\alpha\gamma + d\beta\delta,\alpha\delta + \beta\gamma)
\operatorname{SG}\left(\left(lpha,eta
ight),\left(\gamma,\delta
ight)
ight)=\left(lpha+eta\sqrt{d}
ight)\left(\gamma+\delta\sqrt{d}
ight)אזי \left(lpha,eta
ight),\left(\gamma,\delta
ight)\in\operatorname{sols}_{\mathbb{Z}}\left(x^{2}-dy^{2}=1
ight) טענה: יהי d
eq\square באשר באשר ש
                                                                                                                           . חבורה אבלית (sols_{\mathbb{Z}}\left(x^2-dy^2=1
ight),\mathrm{SG}
ight) אזי אזי d
eq\square באשר שבלית יהי
                                                                                                                             \mathbb{Z}\left[\sqrt{d}
ight]^{	imes}=\left\{lpha\in\mathbb{Z}\left[\sqrt{d}
ight]\mid N\left(lpha
ight)=1
ight\} אזי d
eq\square באשר של d\in\mathbb{N} יהי מה יהי
                                                                                                                                                 \mathbb{Z}^{1} .sols\mathbb{Z}\left(x^2-dy^2=1
ight)=\mathbb{Z}\left[\sqrt{d}
ight]^	imes אזי d
eq \square אזי d\in\mathbb{N} מסקנה: יהי
                                                                                                                                 \mathbb{Z}\left[\sqrt{d}
ight]_{1+}^{	imes}=\left\{lpha\in\mathbb{Z}\left[\sqrt{d}
ight]_{1}^{	imes}\midlpha>0
ight\} איי d
eq\square באשר של d\in\mathbb{N} יהי להי
                a=seta עבורם s\in\{\pm 1\} וקיים ויחיד eta\in\mathbb{Z}\left[\sqrt{d}
ight]_{1+}^{	imes} אזי קיים ויחיד a
eq \mathbb{Z}\left[\sqrt{d}
ight]_{1}^{	imes} עבורם a\in\mathbb{N} טענה: יהי a\in\mathbb{Z}
                                                                                                                                                      \mathbb{Z}\left[\sqrt{d}
ight]_1^	imes\simeq\mathbb{Z}\left[\sqrt{d}
ight]_{1+}^	imes \{\pm 1\} אזי d
eq\square באשר d\in\mathbb{N} יהי מסקנה: יהי
                                                                                                                                                                                                                                                               [lpha]=lpha אזי lpha\in\mathbb{R} סימון: יהי
     [a_0,\dots,a_n]=a_0+rac{1}{[a_1,\dots,a_n]} איז a_1\dots a_n\in\mathbb{R}_+ ויהיו a_0\in\mathbb{R} ויהיו a_0\in\mathbb{R}_+ איז a_1\dots a_n\in\mathbb{R}_+ ויהיו a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ איז a_0\in\mathbb{R}_+ איז a_0\in\mathbb{R}_+ למה: יהי a_0\in\mathbb{R}_+ יהיו a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ איז a_0\in\mathbb{R}_+ איז a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ יהיו a_0\in\mathbb{R}_+ יהיו a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ איז a_0\in\mathbb{R}_+ וועדיר a_0\in\mathbb{R}_+ וועדי
                              טענה: יהיa_0\in\mathbb{R} יהיי a_0\in\mathbb{R} יהיי a_0\in\mathbb{R} ונגדיר a_1\ldots a_n\in\mathbb{R} ונגדיר a_1\ldots a_n\in\mathbb{R} אזי a_1\ldots a_n\in\mathbb{R} אזי a_1\ldots a_n\in\mathbb{R}
                                                                                                                                                                                          .rac{p_k}{q_k}=[a_0,\ldots,a_k] מתקיים k\in\mathbb{N}_{\leq n} לכל .inom{p_k}{q_k}rac{p_k}{q_{k-1}}=\prod_{i=0}^kinom{a_i}{1}{0} מתקיים k\in\mathbb{N}_{\leq n} לכל .
                                                                                                                                   a_k=a_kq_{k-1}+q_{k-2} וכן p_k=a_kp_{k-1}+p_{k-2} מתקיים k\in\mathbb{N}_{\leq n} לכל
                                                                                                                                                                                 .p_kq_{k-1}-q_kp_{k-1}=(-1)^{k+1} מתקיים k\in\mathbb{N}_{\leq n} לכל \bullet
                                          . מונוטונית עולה. [a_0,\ldots,a_{i-1},x,a_{i+1},\ldots a_n] אזי i\in\mathbb{N}_{\mathrm{even}}\cap\mathbb{N}_{\leq n} ויהי a_1\ldots a_n\in\mathbb{R}_+ יהיי a_0\in\mathbb{R} יהי
```

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

טענה: יהי $a_0,\ldots,a_{i-1},x,a_{i+1},\ldots a_n$ ויהי $a_0\in\mathbb{R}$ ויהי $a_1,\ldots,a_n\in\mathbb{R}$ מונוטונית יורדת. $a_1,\ldots,a_n\in\mathbb{R}$

```
.Cycling (x)=rac{1}{x-|x|} כך Cycling : \mathbb{R}\setminus\mathbb{Q} 	o (1,\infty)\setminus\mathbb{Q} גלגול: נגדיר
                                                                                                      lpha=[a] המקיים [a] המקיים אינסופי שבר משולב משפט: יהי lpha\in\mathbb{R}\setminus\mathbb{Q} האזי קיים ויחיד שבר
                                                                                                                                                                    אלגוריתם שבר משולב פשוט אינסופי למספר אי־רציונלי: ...
(rac{p_k}{q_k})=\left(\prod_{i=0}^k\left(egin{smallmatrix}a_i&1\1&0\end{smallmatrix}
ight)\left(egin{smallmatrix}1&0\0&0\end{smallmatrix}
ight) כך p,q:\mathbb{Z}_{\geq -1}	o \mathbb{Z} ייצוג שברי של שבר משולב פשוט אינסופי: יהי[a] שבר משולב פשוט אינסופי
                                                                                                                                                                                                                                                                                (p,q) אזי
                  .rac{p_k}{q_k}=[a_0,\ldots,a_k] שבר משולב פשוט אינסופי ויהי (p,q) ייצוג שברי של [a] אזי לכל k\in\mathbb{N} מתקיים k\in\mathbb{N} מתקיים k\in\mathbb{N} שבר משולב פשוט אינסופי ויהי (p,q) ייצוג שברי של k\in\mathbb{N} אזי k\in\mathbb{N} אזי k\in\mathbb{N} וכן k\in\mathbb{N} וכן k\in\mathbb{N} יהי k\in\mathbb{N} ייצוג שברי של k\in\mathbb{N} ויהי k\in\mathbb{N} ייצוג שברי של k\in\mathbb{N} אזי לכל k\in\mathbb{N} משפט קירוב דיופנטי: יהי k\in\mathbb{N} ויהי k\in\mathbb{N} ייצוג שברי של k\in\mathbb{N} אזי לכל k\in\mathbb{N} מתקיים k\in\mathbb{N} מתקיים k\in\mathbb{N}
            \left| lpha - rac{\zeta}{\xi} 
ight| > \left| lpha - rac{p_n}{q_n} 
ight| ייצוג שברי של lpha יהי lpha \in \mathbb{R} ויהי lpha \in \mathbb{R} \setminus \mathbb{Q} יהי lpha \in \mathbb{R} \setminus \mathbb{Q} יהי lpha \in \mathbb{R} \setminus \mathbb{Q} יהי
עבורו n\in\mathbb{N} אזי קיים |lpha-rac{\zeta}{\xi}|<rac{1}{2\xi^2} באשר \xi\in\mathbb{N} ויהי \zeta\in\mathbb{Z} יהי lpha ייצוג שברי של lpha ייצוג שברי של lpha יהי lpha יהי אזי קיים lpha
                                                                                                                                                                                                                                                         q_n = \xi וכן p_n = \zeta
                           a_n=a_{n+T} המקיימת a:\mathbb{N}	o\mathbb{R} אזי פונקציה איז פונקציה מסווים: יהיו איזי יהיו מסויים: יהיו
                                 a_0\dots a_{N-1}\overline{a_N\dots a_{N+T-1}}=a אזי מראור מרא מחזור מחזור מחזורית בעלת מחזור a:\mathbb{N}	o\mathbb{R} ותהא N,T\in\mathbb{N}
                                                                               . שבר משולב פשוט מחזורית a עבורו a עבורו שבר משולב שבר שבר משולב שב משולב שבר משולב שב משולב שב משולב שב משולב שבר משולב שב משולב ב מש
                                                                                                                                                                                       \mathbb{Q}\left(\sqrt{d}
ight)=\mathbb{Q}+\sqrt{d}\cdot\mathbb{Q} אזי d\in\mathbb{R} הגדרה: יהי
                                                                                                                                                                                                                  . שדה \mathbb{Q}\left(\sqrt{d}
ight) אזי d\in\mathbb{R} טענה: יהי
                                                  eta=\delta וכן lpha=\gamma אזי lpha+eta\sqrt{d}=\gamma+\delta\sqrt{d} באשר lpha,eta,\gamma,\delta\in\mathbb{Q} ויהיו a=\gamma וכן באשר a=\gamma אזי יהי וכן
                                                   -\omega(lpha+eta\sqrt{d})=(lpha,eta) כך arphi:\mathbb{Q}\left(\sqrt{d}
ight)	o\mathbb{Q}^2 אזי נגדיר \sqrt{d}
otin\mathbb{Q} באשר d\in\mathbb{R} העתקת המקדמים: יהי
                                                                                                                 (ועל. \sigma באשר \sigma באשר \sigma ותהא \sigma העתקת המקדמים אזי \sigma חח"ע ועל. d\in\mathbb{R}
                                                                                                                                                       lpha+eta\sqrt{d}=lpha-eta\sqrt{d} אזי lpha,eta\in\mathbb{Q} ויהיו d\in\mathbb{R} הצמדה: יהי
                                      טענה: יהי f אזי f אזי f אזי f כך f:\mathbb{Q}\left(\sqrt{d}\right) 	o \mathbb{Q}\left(\sqrt{d}\right) ונגדיר ענהי ונגדיר d\in\mathbb{R} כך יהי
                                                                                                                                      lpha \in \mathbb{Q}\left(\sqrt{d}
ight) מספר ריבועי: מספר lpha \in \mathbb{R} עבורו קיים lpha \in \mathbb{R}
                          . ריבועי Cycling\left(lpha
ight) עד להיות אוי ריבועי אוי ריבועי אוי ריבועי אוי אוי ריבועי אוי להיות מריבועי אוי להיות מריבועי אוי d\in\mathbb{Q} עד להיות מענה: יהי lpha\in\mathbb{R}
                                                                                      .(lpha=rac{B+\sqrt{d}}{A} עבורם A,B\in\mathbb{Z} וקיימים d\in\mathbb{N} וקיים אזי (איזי lpha\in\mathbb{R} אזי lpha\in\mathbb{R}
                                              .(lpha=rac{B+\sqrt{d}}{A} עבורם A,B\in\mathbb{Z} וקיימים d
eq \mathbb{N} עבורו (קיים a) אזי אזי lpha\in\mathbb{R}\setminus\mathbb{Q} אזי lpha\in\mathbb{R}\setminus\mathbb{Q}
                                                             (alpha^2+blpha+c=0\, עבורם b,c\in\mathbb{Z} וקיימים a\in\mathbb{Z}\setminus\{0\} (קיים (קיים lpha) אזי lpha\in\mathbb{R} אזי lpha\in\mathbb{R}
                                       .(lpha=rac{B+\sqrt{d}}{A} וכן B^2\equiv d\mod A עבורם A,B\in\mathbb{Z} וקיימים וקיים (קיים A,B\in\mathbb{R} וכן lpha\in\mathbb{R}
                                                                                                                                           \overline{lpha} \in (-1,0) המקיים lpha \in \mathbb{R}_{>1} מספר ריבועי מצומצם: מספר ריבועי
                                                                                                                                              מסקנה: יהי d\in\mathbb{N} באשר d
eq d אזי d
eq d ריבועי מצומצם.
                                                                                                                                              . ריבועי מצומצם ריבועי היי ar{\operatorname{Cycling}}\left(lpha
ight) אזי מצומצם ריבועי מצומצם lpha\in\mathbb{R}
                                                                                           lpha=eta אזי \operatorname{Cycling}\left(lpha
ight)=\operatorname{Cycling}\left(eta
ight) אזי מענה: יהיו lpha,eta\in\mathbb{R} ריבועיים מצומצמים באשר
                   A,B\in \left(0,\sqrt{d}
ight) וכן A\in (0,d) ויהיו A\in \mathbb{N} ויהיו A,B\in \mathbb{Z} וכן B^2\equiv d\mod A באשר אויהיו ויהיו A,B\in \mathbb{Z}
                                                                          . \left|\left\{lpha\in\mathbb{Q}\left(\sqrt{d}
ight)\;\middle|\;מסקנה: יהי d\in\mathbb{N} אזי a אזי a ריבועי מצומצם a ריבועי מצומצם a אזי פונקציה a המקיימת a אזי פונקציה a לכל a
```

 $i \in \mathbb{N}_{\leq n}$ לכל $a_i = b_i$ וכן n = m

אלגוריתם שבר משולב פשוט למספר רציונלי: ...

. סענה: תהא $i\in\mathbb{N}_+$ אזי $a:\mathbb{N} o\mathbb{R}$ אזי $a:\mathbb{N} o\mathbb{R}$ סענה: תהא

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

 $a:\mathbb{N} \to \mathbb{N}$ אזי $i\in\mathbb{N}_+$ לכל $a_i\in\mathbb{N}_+$ באשר $a:\mathbb{N} \to \mathbb{Z}$ אזי $a_i\in\mathbb{N}_+$ אזי

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

עבורם $a_n>1$ באשר $a_1\ldots a_n\in\mathbb{N}_+$ וכן קיימים ויחידי $a_0\in\mathbb{Z}$ וכן קיים ויחיד ווחיד אזי קיים ויחיד מענה: יהי $lpha\in\mathbb{Q}$

```
.(ביועי מצומצם). איי (קיים שבר משולב פשוט מחזורי טהור [a] עבורו משפט: יהי lpha\in\mathbb{R}\setminus\mathbb{Q} איי (קיים שבר משולב פשוט מחזורי טהור
                 \sqrt{d}=[a_0,\overline{a_1,\ldots,a_{n-1},2a_0}] עבורם a_0\ldots a_{n-1}\in\mathbb{N} וקיימים n\in\mathbb{N} אזי קיים d
eq \square אזי קיים מסקנה: יהי
עבורו a_m ריבועי m\in\mathbb{N} אזי קיים a_{n+1}=\operatorname{Cycling}(a_n) וכן a_0=lpha כך a:\mathbb{N}	o\mathbb{R}\backslash\mathbb{Q} עבורו lpha\in\mathbb{R}\backslash\mathbb{Q}
                                                                                                                          mמצומצם וכן a מחזורית החל מ
                                               (\alpha) אזי (קיים שבר משולב פשוט מחזורי [a] עבורו שבר משרט: יהי \alpha \in \mathbb{R} \setminus \mathbb{Q} אזי (קיים שבר משולב משרט: יהי
ייצוג (p,q) ייהי d = [a] ייהי החל מ־1 באשר 1 באשר 0 = a: \mathbb{N} \to \mathbb{N} מחזורית בעלת מחזור a: \mathbb{N} \to \mathbb{N} ייהי ויהי
                                                                                              p_{kn-1}^2-dq_{kn-1}^2=\left(-1
ight)^{kn} מתקיים k\in\mathbb{N} לכל
                                                                                   .sols_{\mathbb{N}} (x^2 - dy^2 \in \{\pm 1\}) = \{(p_{kn-1}, q_{kn-1}) \mid k \in \mathbb{N}\} \bullet
יצוג (p,q) ייצוג \sqrt{d}=[a] באשר בשר 1 באשר n באשר n באשר n\in\mathbb{N} יהי ויהי n\in\mathbb{N} יהי יצוג d\in\mathbb{N} ייצוג
                                                                                                                                                 שברי של [a] אזי
                                                                                             (\operatorname{sols}_{\mathbb{Z}}(x^2 - dy^2 = -1) \neq \emptyset) \iff (n \in \mathbb{N}_{\operatorname{odd}}) \bullet
                                                                     \min_{\pi_2} \left( \operatorname{sols}_{\mathbb{N}} \left( x^2 - dy^2 = -1 \right) \right) = \left( p_{n-1}, q_{n-1} \right) אז n \in \mathbb{N}_{\operatorname{odd}} שו
```

יצוג (p,q) ייצוג $\sqrt{d}=[a]$ באשר בשר 1 באשר n באשר n באשר $n\in\mathbb{N}$ יהי ויהי $n\in\mathbb{N}$ יהי יצוג $d\in\mathbb{N}$ ייצוג

$$.sols_{\mathbb{Z}}(x^2 - dy^2 = 1) \setminus \{(1,0), (-1,0)\} \neq \emptyset \bullet$$

$$\min_{\pi_2}\left(\mathrm{sols}_{\mathbb{N}}\left(x^2-dy^2=1
ight)\setminus\left\{\left(1,0
ight),\left(-1,0
ight)
ight\}
ight)=\left(p_{n-1},q_{n-1}
ight)$$
 אם $n\in\mathbb{N}_{\mathrm{even}}$ אם \bullet

$$\min_{\pi_2}\left(\operatorname{sols}_{\mathbb{N}}\left(x^2-dy^2=1
ight)\setminus\left\{\left(1,0
ight),\left(-1,0
ight)
ight\}
ight)=\left(p_{2n-1},q_{2n-1}
ight)$$
 אם $n\in\mathbb{N}_{\operatorname{odd}}$ אם $n\in\mathbb{N}_{\operatorname{odd}}$

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

$$arepsilon=u+v\sqrt{d}$$
 אזי אזי $x^2-dy^2=1$ סימון: יהי של ויהי ויהי שוהי ויהי ויהי ויהי ויהי של באשר ויהי ויהי ויהי ויהי אזי ויהי ויהי ויהי

$$\langle arepsilon
angle = \mathbb{Z} \left[\sqrt{d}
ight]_{1+}^ imes$$
 אזי אזי $x^2 - dy^2 = 1$ משפט: יהי ויהי של ויהי ויהי לוהי ויהי ויהי ויהי לוהי הפתרון היסודי של

 $n\in\mathbb{Z}$ אזי קיים $(lpha,eta)\in\mathrm{sols}_\mathbb{Z}$ $(x^2-dy^2=1)$ ויהי $x^2-dy^2=1$ אזי הפתרון היסודי של $d\in\mathbb{N}$ אזי קיים $d\in\mathbb{N}$ $\alpha + \beta \sqrt{d} = s \cdot \varepsilon^n$ עבורם $s \in \{\pm 1\}$ וקיים

$$a\in\mathrm{QR}_d\cup\{0\}$$
 אזי $a\in\mathbb{Z}\setminus\{0\}$ אזי $a\in\mathbb{Z}\setminus\{0\}$ ויהי $a\in\mathbb{Z}\setminus\{0\}$ אזי $a\in\mathbb{R}$ טענה: יהי $a\in\mathbb{R}$

$$\operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2
ight)
eqarnothing$$
 באשר $a\in\mathbb{Z}ackslash\left\{0
ight\}$ ויהי $d
eq\square$ באשר באשר $d\in\mathbb{N}$ אזי

$$.\left(\frac{a}{p}\right)\in\{0,1\}$$
 מתקיים $p|d$ המקיים $p\in\mathbb{P}_{>2}$ לכל •

$$a \mod 4 \in \{0,1\}$$
 אז $4|d$ אם 4

$$a \mod 8 \in \{0,1,4\}$$
 אם $a \mod 8 \in \{0,1,4\}$ אם •

 $(lpha,eta)\in\operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=a
ight)$ ויהי $a\in\mathbb{Z}\setminus\{0\}$ יהי $x^2-dy^2=1$ יהי של יהי $a\in\mathbb{Z}\setminus\{0\}$ יהי של יהי $a\in\mathbb{Z}\setminus\{0\}$ יהי $z+a\sqrt{d}=s\cdotarepsilon^n\cdot\left(z+w\sqrt{d}
ight)$ עבורם $s\in\{\pm 1\}$ וקיים ו $s\in\mathbb{Z}$ וקיים ו $z+w\sqrt{d}<\sqrt{|a|}$ באשר $z,w\in\mathbb{N}$ $\{\langle f \rangle \mid (f \in \mathbb{Z}_{\leq 2} \left[x, y \right]) \land (\operatorname{sols}_{\mathbb{Z}} \left(f = 0 \right) \neq \varnothing) \} \in \mathcal{R}$ מסקנה:

$$\mathbb{Q}\left(i
ight)=\mathbb{Q}+i\cdot\mathbb{Q}$$
 מספרי גאוס:

.טענה: $\mathbb{O}(i)$ שדה

 $\mathbb{Z}\left[i
ight]=\mathbb{Z}+i\cdot\mathbb{Z}$ שלמי גאוס:

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