```
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 מענה: \mathbb{Z}
         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) באיי פרידיקט מעל מסקנה עיקרון האינדוקציה: יהי
                                                                                                                                                   .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 אוי a\in\mathbb{Z} אזי 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} מתקיים
                                                                                                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 יהי יהי יהי 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 a,b\in\mathbb{Z} ויהי סימון: יהיו
                                                                                                      (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) המחשב כפל מספרים בסיבוכיות ריצה NaiveMul טענה: קיים אלגוריתם
                                                                                            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
                                                                                .
(Karatsuba<br/>Mult ((a)_2\,,(b)_2))_{10}=abאזי a,b\in\mathbb{N}יהיו יהי<br/>וa,b\in\mathbb{N}
                                                                                  \mathcal{O}\left(n^{\log_2(3)}\right) הינה KaratsubaMult טענה: סיבוכיות הריצה של
                             \mathcal{O}(n\log(n)) מענה קולי־טוקי: קיים אלגוריתם CooleyTukeyMul 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 אוי k\in\mathbb{N}_+ יסענה: יהי
                                                              \mathcal{O}\left(n\log^2\left(n\right)\right) בסיבוכיות ריצה FastGCD טענה: קיים אלגוריתם
                                                               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
                              \mathrm{lcm}\,(a_1\ldots a_n)=d אזי a_1\ldots a_n של המשותפת המזערית של הכפולה הכפולה הכפולה ויהי ויהי d\in\mathbb{N} ויהי
                                                                                      [a_1\ldots a_n]=\mathrm{lcm}\,(a_1\ldots a_n) אזי [a_1\ldots a_n\in\mathbb{Z}] יהיו
                                                                                     a_i | \mathrm{lcm}\,(a_1 \ldots a_n) אזי a_1 \ldots a_n \in \mathbb{Z} לכל
                                                               .\mathrm{lcm}\,(a_1\ldots a_n)\,|m| אזי i\in[n] לכל a_i|m באשר a_1\ldots a_n, m\in\mathbb{Z} אזי יהיו
                                               \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}ackslash\left\{0
ight\}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\mathbb{Z} ויהיו p\in\mathbb{P} אזי p|ab אזי a,b\in\mathbb{Z} טענה: יהי
                                                      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 \le N do
A_{i+2j} = \text{False}
     return \{i \in [N] \mid A_i = \text{True}\}
                                                                                    .EratosthenesSieve (N)=\{p\in\mathbb{P}\mid p\leq N\} אזי N\in\mathbb{N}_+ יהי יהי איזי N\in\mathbb{N}_+
                      \mathcal{O}\left(\left(\sum_{p\in\mathbb{P}_{\leq N}}\frac{1}{p}\right)\cdot N\right) הינה EratosthenesSieve (N) אזי סיבוכיות הריצה של N\in\mathbb{N}_+ הינה איז איז סיבוכיות הריצה של N\in\mathbb{N}_+ לכל N\in\mathbb{N}_+ וכן N\in\mathbb{N}_+ רץ בסיבוכיות ריצה \mathcal{O}\left(N\right) טענה אטקין־ברנסטיין: קיים אלגוריתם \mathcal{A} עבורו
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\{m\in\mathbb{N}\mid (p^m|n)\} אזי p\in\mathbb{R} ויהי n\in\mathbb{N}_+ יהי יהי n\in\mathbb{N}_+
                                                                                                                           p^{e_p(n)} \| n אזי p \in \mathbb{P} ויהי n \in \mathbb{N}_+ אזי יהי
                                                                                                                             n=\prod_{n\in\mathbb{P}}p^{e_p(n)} אזי n\in\mathbb{N}_+ יהי 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}_{+} מסקנה: 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
                                                                                  [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}_+ מסקנה: 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{N} אזי קיים p\in N באשר באשר p\in \mathbb{N} השערה פתוחה הראשוניים התאומים:
                                                                                                                            .\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} המקיים p\in\mathbb{P} ראשוני סופי ז'רמן: ראשוני חופי 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 $n\in\mathbb{N}$ יהי של היהי $\pi:\mathbb{Z} o\mathbb{Z}/n\mathbb{Z}$ העתקת המנה ויהי $\pi\in\mathbb{N}$ שארית החלוקה של π

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

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

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

[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} מודולו: יהיn \in \mathbb{N}
                               (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 חכn\in\mathbb{N}_+ יהי
                                                          .(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} אזי \alpha, r \in \mathbb{N}_+ טענה: יהיו
     a+b\equiv c+d\mod n אזי אb\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 \mod n) + (b \mod n) = ((a+b) \mod n) אזי(a,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 יהי
                                                                              הערה: אלא אם כן נאמר אחרת חוג הינו חוג אבלי בעל יחידה.
                                                                                                                           טענה: יהי\mathbb{Z}/n\mathbb{Z} אזי n\in\mathbb{N}_+ חוג.
                                                                                                           \mathbb{Z}/n\mathbb{Z} אזי n\in\mathbb{N}_+ חוג השאריות מודולו: יהי
                                                                                                   (n\in\mathbb{P})שדה) שדה n\in\mathbb{N}_+ טענה: יהיn\in\mathbb{N}_+ אזי טענה:
                                                        a,(a,n)=(b,n) אזיa\equiv b \mod n באשר באשר n\in\mathbb{N}_+ יהיn\in\mathbb{N}_+ למה: יהי
                                              .((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
                                                        i\mapsto (i\mod n) כך \{0,\dots,n-1\}\stackrel{\checkmark}{\hookrightarrow}\mathbb{Z}/n\mathbb{Z} אזי נשכן n\in\mathbb{N}_+ יהי יהי
                                    אלגוריתם הופכי בחבורת שאריות החלוקה: יהי n\in\mathbb{N}_+ ויהי a\in\mathbb{Z} באשר אלגוריתם הופכי
```

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
```

```
.Inverse\mathrm{Mod}\,(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})^	imes=\{(i\mod p)\mid i\in\{0,\dots,p-1\}\} איי p\in\mathbb{P} טענה: יהי p\in\mathbb{P} איי איילר: נגדיר \varphi:\mathbb{N}_+	o\mathbb{N} כך \varphi:\mathbb{N}_+	o\mathbb{N} פונקציית 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} ראשוני עבורו קיים n\in\mathbb{N}_+ המקיים p\in\mathbb{P} אזי p\in\mathbb{P} ראשוני סופי 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 a באשר a\in\mathbb{Z} ויהי ויהי p\in\mathbb{P} משפט הקטן של פרמה: יהי
                                                                  a^p \equiv a \mod p אזי a \in \mathbb{Z} ויהי ויהי p \in \mathbb{P}
                   a_i,j\in[n] לכל (a_i,a_j)=1 המקיימים a_1\dots a_n\in\mathbb{Z} מספרים זרים בזוגות:
                                          [a_1,\ldots,a_n]=\prod_{i=1}^n a_i איים באוגות זיי a_1\ldots a_n\in\mathbb{Z} יהיי
 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 (גדיר n\in\mathbb{N}_+ יהי יהי
                      משפט השאריות הסיני: יהיוa_1 \ldots a_n \in \mathbb{Z} ארים בזוגות ויהיוm_1 \ldots m_n \in \mathbb{N}_+ אזי
```

- $\mathbb{1}^n s \equiv a \mod m$ 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
                              .1^n\cdot 	ext{ModEquationSys}\equiv a\mod m אזי אזי a_1\ldots a_n\in \mathbb{Z} זרים בזוגות ויהיו m_1\ldots m_n\in \mathbb{N}_+ איזי
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} אירים בזוגות זירים m_1\dots m_n\in\mathbb{N}_+ 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 באשר לכל כפליות באשר לכל לכל באשר לכל לכל היינה
                                                                  . 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
                              \operatorname{ord}\left(g^d
ight)=rac{n}{(n,d)} אזי איז g\in G יוצר איזי חבורה ציקלית מסדר חבורה אזי חבורה G אהיו n,d\in\mathbb{N}_+ יהיו
                             \{a\in G\mid G\mid G טענה: יהיa\}=\{g^d\mid (d,n)=1\} יוצר מסדר מסדר עלקלית מסדר a\}=\{g^d\mid (d,n)=1\} יוצר של
                                                     |\{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 d,n\in\mathbb{N}_+
                \|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_{d\in\mathbb{N}_+}arphi\left(d
ight)=n אזי n\in\mathbb{N}_+ יהי יהי מסקנה: יהי n\in\mathbb{N}_+ אזי חותהא G\leq\mathbb{F}^	imes טופית אזי G ציקלית.
                                                                        \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. \left|\left\{g\in[n-1]\mid \langle g\mod n
angle=(\mathbb{Z}/n\mathbb{Z})^	imes
ight.
ight.
ight.
ight.
ight.באשר קיים שורש פרימיטיבי מודולו n אזי וואי איזי n\in\mathbb{N}_+ באשר קיים שורש פרימיטיבי בי מודולו אזי וואיי
                                                                  \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 p\in\mathbb{P}
                                                                                                  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{R} אזי q \in G אזי q \in \mathbb{R} מתקיים q \in \mathbb{R} מתקיים ויהי
                                                                                                           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,\dots,2^{k-2}\} וכן lpha\in \{0,1\} ויהי אזי קיימים ויחידים a\in \mathbb{Z}_{\mathrm{odd}} איזי 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} וכן המקיים a\in\mathbb{Z} אזי אזי a\in\mathbb{Z} אזי n\in\mathbb{N} אזי ריבועית: יהי
                                                                                                                               \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 \; \mathsf{ווולו} \; n אי־שארית איי איי a \} איי אזי n \in \mathbb{P} איי יהי
                                                      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
                                                                                                                                               a,b\in\mathbb{Z} ויהיו a,b\in\mathbb{Z} ויהיו p\in\mathbb{P}_{>2} אזי מסקנה: 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
                                                                                                                              |\operatorname{sols}ig(x^2=aig)|=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} וכך S\cap (-S)=\varnothing באשר באשר S\subseteq (\mathbb{Z}/p\mathbb{Z})^{	imes} ויהי p\in \mathbb{P}_{\geq 2} אזי יהי p\in \mathbb{P}_{\geq 2}
                                                                                                                                                       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} עבורו לכל
                                                                                           \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 \in \mathbb{Z} טענה: יהיו n,m \in \mathbb{N}_{	ext{odd}} ויהיn,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 המקיים p\in\mathbb{P} המקיים (m\equiv a^2\mod n עבורו a\in\mathbb{Z} אזי (קיים m\in\mathbb{Z} המקיים האזי m\in\mathbb{N}_{\mathrm{odd}} המקיים אזי (m,n) אזי (היים m\in\mathbb{N}_{\mathrm{odd}}
                                                                                                                            (\frac{-1}{n})=(-1)^{\frac{n-1}{2}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מטקנה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מטקנה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} טענה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מטקנה: יהי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} אזי n\in\mathbb{N}_{\mathrm{odd}} מטקנה: יהי 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)
                                                                                                       .
Jacobi<br/>Symbol (m,n)=\left(\frac{m}{n}\right) אזי m\in\mathbb{Z} ויהי <br/> n\in\mathbb{N}_{\mathrm{odd}} יהי יהי
                                                                                                                          \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 באשר a\in\mathbb{Z} אזי (קיימים x,y\in\mathbb{Z} אזי (קיימים a\in\mathbb{Z} ויהי p
eq \mathbb{Z} ויהי ויהי p\in\mathbb{P}_{>2}
                                                                                                                                                                            |\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 יהי שלם אזי n\in\mathbb{Z} יהי
                                                                            a \in \mathbb{Z} אזי n = \square אזי n \in \mathbb{N}_{\mathrm{odd}} \setminus \{1\} אזי n \in \mathbb{N}_{\mathrm{odd}} \setminus \{1\} טענה: יהי
                                                                                            a\in\mathbb{Z} טענה: יהי n
eq n באשר באשר n\in\mathbb{N}_{\mathrm{odd}}ackslash\{1\} טענה: יהי
                                                                          \left. \left| \left\{ x \in \left( \mathbb{Z}/n\mathbb{Z} \right)^{	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}_{	ext{odd}} \setminus \{1\} טענה: יהי
                                                                                                                                                                            |\mathbb{P}\cap (5\mathbb{N}-1)|=\aleph_0 טענה:
  \mathcal{A}\left(N,a,m
ight)=(a^{m}\mod N) מתקיים a,m\in[N-1] ולכל אלגוריתם N,m\in\mathbb{N}_{+} עבורו לכל עבורו לכל
                                   אזי a \in R ויהי ויהי m_0 \dots m_k \in \{0,1\} יהיו אלגוריתם כפל מעל A אחוג יהי ויהי R חוג יהי אלגוריתם ריבוע איטרטיבי:
Algorithm IteratedSquaring<sub>R</sub> [\mathcal{A}] (a, m):
       \begin{array}{l} a_0 \leftarrow a \\ r \leftarrow a_0^{m_0} \end{array}
      for i \in [1, ..., k] do
\begin{vmatrix} a_i \leftarrow \mathcal{A}(a_{i-1}, a_{i-1}) \\ \text{if } m_i = 1 \text{ then } r \leftarrow \mathcal{A}(r, a_i^{m_i}) \end{vmatrix}
                               .ModIteratedSquaring (N,a,m)= IteratedSquaring_{\mathbb{Z}/N\mathbb{Z}}(a,m) אזי a\in\mathbb{Z}/N\mathbb{Z} ויהי N,m\in\mathbb{N} ויהי איז N,m\in\mathbb{N}
                                                    .ModIteratedSquaring (N,a,(m)_2)=(a^m \mod N) אזי a\in \mathbb{Z}/Nענה: יהיו N,m\in \mathbb{N} ויהי N,m\in \mathbb{N}
```

הינה ModIteratedSquaring איז סיבוכיות איז איז ויהיי איז ויהיו איז מספרים מספרים אלגוריתם כפל מספרים ויהיו איז יהי

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

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

```
\mathcal{O}(\log(m) \cdot \log(N) \log \log(N) \log \log \log \log(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
                                                              N \in \mathbb{N}_+ אזי (TrialDivision N = \text{True}) אזי (N \in \mathbb{P}) אזי N \in \mathbb{N}_+ טענה: יהי
                                                                             \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 [A] (N; a):
    if A(N, a, N - 1) = 1 then return True
    return False
                           \mathcal{O}\left(n^3\right) הינה FermatPrimalityTest [ModIteratedSquaring [NaiveMul]] אינה: סיבוכיות הריצה של
                           הינה FermatPrimalityTest [ModIteratedSquaring [CooleyTukeyMul]] סענה: סיבוכיות הריצה של
                                                                                                            \mathcal{O}\left(n^2\log\left(n\right)\log\log\left(n\right)\right)
                                                    \mathbb{P}_{a\leftarrow [N-1]} (FermatPrimalityTest (N;a)=\mathrm{True})=1 אזי N\in\mathbb{P} סענה: יהי
                       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]}\left(\mathrm{FermatPrimalityTest}\left(N;a\right)=\mathrm{False}\right)>rac{1}{2} אינו מספר קרמייקל אזי N\in\mathbb{N}_{+} פריק באשר N\in\mathbb{N}_{+}
                                                                       .FermatPrimalityTest (F_k; 2) = \text{True} אזי 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
             מספר קרמייקל. (6k+1)\cdot (12k+1)\cdot (18k+1)\cdot (18k+1) אזי 6k+1,12k+1,18k+1\in \mathbb{P} מספר קרמייקל.
                                                          השערה פתוחה .|\{k\in\mathbb{N}\mid 6k+1, 12k+1, 18k+1\in\mathbb{P}\}|=leph_0 השערה:
                                           משפט אלפורד־גרנוויל־פומרנץ: N\}|=leph_0: מספר קרמייקל אלפורד־גרנוויל־פומרנץ: משפט אלפורד
 משפט אלפורד־גרנוויל־פומרנץ: החל ממקום מסויים לכל x\in\mathbb{N} מתקיים x\in\mathbb{N} מספר קרמייקל N<1. לא הוכח בקורס
                                                           משפט ארדוש: קיים c>0 עבורו החל ממקום מסויים לכל מתקיים מתקיים
                                               לא הוכח בקורס .|\{N < x \mid  קרמייקל N\}| < x \cdot \exp\left(rac{-c \cdot \log(x) \cdot \log\log\log(x)}{\log\log(x)}
ight)
                           אזי a\in [N-1] אזי ויהי N\in \mathbb{N}_+ אזי מבחן סולובאי־סטראסן: יהי A אלגוריתם חזקה מודולרית יהי
Algorithm SolovayStrassenPrimalityTest [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 (A(N, a, \frac{N-1}{2}) = (s \mod N)) then
     | return True
    return False
                \mathcal{O}\left(n^3\right) אינה SolovayStrassenPrimalityTest [ModIteratedSquaring [NaiveMul] הינה היצה של
                              אזי SolovayStrassenPrimalityTest (N;a)=True המקיים a\in[N-1] ויהי N\in\mathbb{N}_+ ויהי N\in\mathbb{N}_+
```

.FermatPrimalityTest (N; a) = True

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

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

```
\mathbb{P}_{a\leftarrow[N-1]} (SolovayStrassenPrimalityTest (N;a)=\mathrm{False})>\frac{1}{2} אזי N\in\mathbb{N}_+ יהי אלגוריתם מבחן מילר־רבין: יהי A\in\mathbb{N}_{< N} אזי אלגוריתם מבחן מילר־רבין: יהי A\in\mathbb{N}_{< N} אזי
```

```
for i \in [1, \dots, e_2(N-1)] do
         \alpha_i \leftarrow \mathcal{A}(N, \alpha_{i-1}, 2)
         if \alpha_i = -1 then return True
          if \alpha_i \neq 1 then return False
    return True
                         \mathcal{O}\left(n^3\right) הינה MillerRabinPrimalityTest [ModIteratedSquaring [NaiveMul]] אענה: סיבוכיות הריצה של
                                                         \mathbb{P}_{a\leftarrow\mathbb{N}_{\leq N}} (MillerRabinPrimalityTest (N;a)=\mathrm{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
                                              \mathbb{P}_{a\leftarrow\mathbb{N}_{\leq N}} (MillerRabinPrimalityTest (N;a)=\mathrm{False})>rac{3}{4} צריק אזי N\in\mathbb{N} מסקנה: יהי
                                                                                                   טענה: יהיk \in \mathbb{N}_{	ext{odd}} באשר אזי k \in \mathbb{N}_{	ext{odd}} אזי
                     . \left| \left\{ a \in \mathbb{N}_{<(2k+1)\cdot(4k+1)} \mid \text{MillerRabinPrimalityTest} \left( (2k+1)\cdot(4k+1); a \right) = \text{True} \right\} \right| = \frac{\varphi((2k+1)\cdot(4k+1))}{4}
                                          אזי MillerRabinPrimalityTest (N;a)= True מענה: יהי N\in\mathbb{N}_+ ויהי N\in\mathbb{N}_+ ויהי אזי
                                                                                                     .SolovayStrassenPrimalityTest (N; a) = True
באשר r:\mathbb{N}	o\{2^{n-1},\ldots,2^n\}	imes\mathbb{N}^k ותהא הייצור מספרים יהי אלגוריתם חזקה מודולרית יהיו אלגוריתם לייצור מספרים ראשוניים: יהי
                                                                                        אזי i \in \{2,\ldots,k+1\} ולכל 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 \text{True}
          for i \in [2, \ldots, 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
     end
                .2^{n-1}< 	ext{PrimeGenerator}\left(n,k;r
ight)< 2^n עוצר אזי PrimeGenerator (n,k;r) עבורו n,k\in\mathbb{N}_+ טענה: יהיו n,k\in\mathbb{N}_+ אוהי n,k\in\mathbb{N}_+
             \mathbb{E}_r [Time (PrimeGenerator [ModIteratedSquaring [NaiveMul]] (n,k;r))] = \mathcal{O}(kn^4) איי n,k\in\mathbb{N}_+ יהיי n,k\in\mathbb{N}_+ איי
                                                                    \mathbb{P}_r\left(\mathrm{PrimeGenerator}\left(n,k;r\right)\in\mathbb{P}\right)\geq 1-\frac{1}{4^k} אזי n,k\in\mathbb{N}_+ יהיי יהיי n,k\in\mathbb{N}_+
                                                                                            q\equiv 1\mod p אזי q|2^p-1 באשר p,q\in\mathbb{P} אזי יהיו
                                                      . פריק. p=2p+1 אזי p\equiv 3 \mod 4 באשר p,q\in \mathbb{P}_{>3} אזי p\equiv 2 פריק.
                                                                                                             M_n=2^n-1 אזי n\in\mathbb{N} מספר מרסן: יהי
                                                                  p=a^n-1 המקיימים a,n\in\mathbb{N}_+ עבורו קיימים עבורו אשוני מרסן: ראשוני p\in\mathbb{P}
                                                                                 p=2^q-1 עבורו q\in\mathbb{P} טענה: יהי p\in\mathbb{P} ראשוני מרסן אזי קיים
                                                                                             מסקנה: יהי p \in \mathbb{P} ראשוני מרסן אזי p \in \mathbb{P} מסקנה:
                                                                                 . מושלם 2^{n-1}\cdot (2^n-1) אזי ראשוני אזי n\in\mathbb{N} מושלם מענה: יהי
```

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

if $(N < 2) \lor (2 \mid N)$ then return False

if N=2 then return True

 $\alpha_0 \leftarrow \mathcal{A}(N, a, \frac{N-1}{2^{e_2(N-1)}})$

```
Algorithm LucasLehmer [\mathcal{A}, \mathcal{B}] (n, 2^n - 1):
           if A(n) = \text{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)=\mathrm{True})\Longleftrightarrow (2^n-1\in\mathbb{P}) אזי n\in\mathbb{N} יהי משפט: יהי
                                                 \mathcal{O}\left(n^3\right) הינה LucasLehmer [TrialDivision, ModIteratedSquaring [NaiveMul]] הינה הריצה של
                                                  טענה: סיבוכיות הריצה של [CooleyTukeyMul] הינה LucasLehmer [TrialDivision, ModIteratedSquaring
                                                                                                                                                                                                                                                                                   \mathcal{O}\left(n^2\log\left(n\right)\log\log\left(n\right)\right)
                                                                                                                                                                                                                                                                                   2^{136276841}-1\in\mathbb{P} :טענה
                                                                                                                                                                                        .	ilde{\mathcal{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) בסיבוכיות בעל בסיבוכיות ריצה AKS משפט אגרוול־קיאל־סקסנה: קיים אלגוריתם דטרמיניסטי
                               E(E,D) אזי p,k\in\mathbb{F}_2^n לכל D\left(E\left(p,k
ight),k
ight)=p באשר באשר E,D:\mathbb{F}_2^n	imes\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 k_e,k_d\in\mathbb{F}_2^m יהיו n,m\in\mathbb{N} יהיו יהיו
i\in[k] בעיית הפירוק: יהי p_i\in\mathbb{P} אזי וכן p_i\in\mathbb{P} באשר p_i=N באשר p_i=1 וכן וכן p_i=1 וכן p_i=1 אזי ווּך p_i=1 באשר p_i=1 באשר p_i=1 וכן p_i=1 וכן p_i=1 אזי ווּך p_i=1 בעיית הפירוק: יהי p_i=1 אזי ווּך p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 אזי ווּך באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 בעיית המספרים: קיים p_i=1 עבורו קיים אלגוריתם p_i=1 בעיית הפירוק בעל סיבוכיות ריצה p_i=1 בענות המספרים: קיים p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 בעיית הפירוק: יהי p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 בעיית הפירוק: יהי p_i=1 בענות המספרים: יהי p_i=1 באשר p_i=1 באשר p_i=1 באשר p_i=1 בעיית הפירוק: יהי p_i=1 בעיית הפירוק: יהי p_i=1 בענות המספרים: יהי p_i=1 באשר p_i=1 באשר p_i=1 בענות המספרים: יהי p_i=1
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 ed\equiv 1\mod arphi(n)
                                                                                                                                                                                              A(A, A, (pq, e), (pq, d)) אזי A(c, (M, a)) = c^a \mod M
                                                                          . אינ (M,M,k_e,k_d) הינה הצפנה אסימטרית. (M,M,k_e,k_d) ותהא (M,M,k_e,k_d) הצפנת הצפנה אסימטרית.
                                                                                                        \operatorname{KSA} טענה: יהיו p,q\in\mathbb{P} ותהא (M,M,k_e,k_d) הצפנת אזי (M,M,k_e,k_d) ותהא
משפט: יהיו (קיים אזי (קיים אזי (איים אזי (אp,q\in\mathbb{P} משפט: יהיו אזי (איים אזי (אp,q\in\mathbb{P} הצפנת אזי (איים אזי (אווים אזי (איים אזי (אווים) אזי (אווים) אזי (אווים) אווים אזי (אווים) אווים איני (אווים) אזי (אווים) אזי (אווים) אווים 
                            .(\mathcal{A}^{M(\cdot,k_e)}\left(1^n
ight)=\mathrm{IFP}\left(N
ight) המקיים \mathcal{\tilde{O}}\left(T
ight) המקיים (מיים יריב \mathcal{A}^M בעל כוח חישובי (\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 ויהי שורש פרימיטיבי מודולו p ויהי שורש מימיטיבי יהי ויהי p\in \mathbb{P} אזי מיסקרטי:
a טענה: יהי p\in\mathbb{P} יהי a שורש פרימיטיבי מודולו a יהי a\in (\mathbb{Z}/p\mathbb{Z})^{	imes} ויהיו a\in (\mathbb{Z}/p\mathbb{Z})^{	imes} יהי a\in \mathbb{Z} יהי שורש פרימיטיבי מודולו
x\in\mathbb{N}_{\leq p} באשר \mathrm{DLP}\left(p,q,a
ight)=x אזי a\in\left(\mathbb{Z}/p\mathbb{Z}
ight)^{	imes} ויהי p\in\mathbb{P} יהי p\in\mathbb{P} יהי יהי p\in\mathbb{P} יהי מודולו
                                                                                                                                                                                                                     g בבסיס g מודולו g בבסיס הינו הלוגריתם הדיסקרטי
טענה נפת שדות המספרים: קיים ל בעל סיבוכיות באשר לכל באשר לכל באשר בעל סיבוכיות ריצה בעל סיבוכיות ריצה c>0 מתקיים כי
                                                                                                                                                                                                                                                            \mathcal{O}\left(\exp\left(c\cdot\log^{\frac{1}{3}}\left(p\right)\cdot\log^{\frac{2}{3}}\left(p\right)\right)\right)
פרוטוקול תקשורת דיפי־הלמן: יהי p\in\mathbb{P} ויהי שורש פרימטיבי מודולו p אזי נגדיר פרוטוקול תקשורת בעל מפתחות פרטיים
                                                                                                                                                                                                                                                                                                                      כך \Pi_{\text{DiffieHellman}}
Communication Protocol \Pi_{\text{DiffieHellman}}(p, g):
           A draws x \in [p-1]
            A sends (g^x \mod p) as K_A
```

```
A draws x \in [p-1]

A sends (g^x \mod p) as K_A

B draws y \in [p-1]

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
```

 $K_{AB}=K_{BA}$ אזי $\Pi_{ ext{DiffieHellman}}\left(p,g
ight)=\left(K_{AB},K_{BA}
ight)$ באשר באשר $K_{AB}=K_{BA}$ אזי שורש פרימטיבי מודולו p ויהיו

```
\mathcal{O}(T) סענה: יהי p\in\mathbb{P} יהי p\in\mathcal{A} יהי שורש פרימטיבי מודולו p\in\mathbb{N} תהא p\in\mathbb{N} חשיבה בזמן עבורה קיים יריב
                                             \mathcal{B}(p,q,q^x \mod p,q^y \mod p) = q^{xy} \mod p המקיים המקיים יריב \mathcal{B} בעל כוח חישובי \tilde{\mathcal{O}}(T) המקיים \tilde{\mathcal{O}}(T)
                                                   כך E,D:\mathbb{F}_2^*	imes\mathbb{F}_2^*	o\mathbb{F}_2^* ונגדיר יהי x\in\mathbb{N}_{< p} יהי ווערש פרימטיבי שורש פרימטיבי מודולו x\in\mathbb{N}_{< p} יהי וונגדיר יהי p\in\mathbb{P} יהי וונגדיר יהי פרימטיבי מודולו
                                                                                                                                 E(c,(\alpha,\beta,\gamma)) = ((c\cdot\gamma^y) \mod \alpha,\beta^y \mod \alpha) אזי y\in\mathbb{N}_{< p} •
                                                                                                                                                                                         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
טענה: יהי \{(x,y)\in\mathbb{R}^2\mid y^2=f\left(x
ight)\} אינה חד־מימדית אוי \deg\left(f\right)=3 באשר באשר f\in\mathbb{R}\left[x
ight] אינה אוי
עקום אַליפטי: יהי \mathbb F שדה באשר f\in \mathbb F[x] ויהי ויהי \operatorname{char}(\mathbb F)
eq 1 באשר בעל שורשים פשוטים מעל \mathbb F
                                                                                                                                                                                                                                 \{(x,y) \in \mathbb{F}^2 \mid y^2 = f(x)\} \cup \{\infty\}
                                                                                                                             E/\mathbb{F} אזי אור אונפטי מעל \mathbb{F} אזי עקום אליפטי מעל ויהי ויהי רhar (\mathbb{F}) \neq 2 אזי
                                                                                                                                                   . יריעה חד־מימדית חלקה אזי E \setminus \{\infty\} עקום אליפטי אזי E \setminus \mathbb{R} יריעה חד־מימדית חלקה.
                                                                                                                                                                                            אז P \in E אז עקום אליפטי ותהא איפוף: יהי יהי
                                                                                                                                                                                                                                           -P=P אזי P=\infty סר
                                                                                                                                                                                                                   -P = (x, -y) אזי P = (x, y) •
                                                                                                                                           A-(-P)=P וכן A-P\in E אזי אליפטי ויהי אליפטי ויהי אזי אזי דיהי עקום אליפטי ויהי
                                                             (\mathrm{line}_{P,Q}\setminus\{P,Q\})\cap E
eq \varnothing אזי איזי איזי איזי אינה P,Q\in E\setminus\{\infty\} טענה: יהי ליפטי ותהיינה
                                                             (T_P\left(Eackslash\{\infty\}
ight)ackslash\{P\}
ight)\cap E
eqarnothing אזי P
eq -P באשר באשר P\in Eackslash\{\infty\} עקום אליפטי ותהא
                                                                                                                                                                                 אז P,Q \in E אז עקום אליפטי ותהיינה אינה E יהי הגדרה חיבור:
                                                                                                                                                                                                                     P+Q=\infty אזי \infty\in\{P,Q\} אם
                                                                                                                                                                                  P+Q=\infty אזי P=-Q וכן \infty \notin \{P,Q\} אם
                                                                                         P+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 \Phi
                                          P+Q=-R אזי R\in ((T_P(E\backslash \{\infty\})\backslash \{P\})\cap E) אחז P\neq -Q וכן P=Q וכן 0
                                                                                                                                                   P+Q=Q+P אזי אזי איננה: יהי P,Q\in E טענה: יהי אליפטי ותהיינה
                                                                                                        P,Q,R\in E טענה: יהי Q,R\in P עקום אליפטי ותהיינה P,Q,R\in E טענה: יהי
                                                                                                                                                                                     . תבורה אבלית עקום אליפטי אזי (E,+) חבורה אבלית עקום אליפטי ההי
                                                                        |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
\|\sum_{x\in\mathbb{F}_p}\left(rac{f(x)}{p}
ight)\|\leq 2\sqrt{p} אוי \overline{\mathbb{F}_p} אויהי f\in\mathbb{F}_p באשר f\in\mathbb{F}_p וכן f\in\mathbb{F}_p וכן שורשים פשוטים מעל f\in\mathbb{F}_p אויהי ויהי
                                                                                                 p+1-2\sqrt{p} \leq |E| \leq p+1+2\sqrt{p} אזי אזי אליפטי אזי p \in \mathbb{P}_{>2} יהי מסקנה: יהי יהי
                   \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} האזי קיים אלגוריתם אוי חיבור נקודות p\in\mathbb{P}_{>2}
טענה: יהי \mathbb{F}_p ויהי \mathbb{F}_p אאי קיים אלגוריתם \mathcal{A} המחשב הכפלת נקודה על עקום אליפטי מעל p\in\mathbb{P}_{>2} יהי י
                                                                                                                                                                                                                                                                    \mathcal{O}\left(\log\left(n\right)\cdot\log^2\left(p\right)\right)
                                    ניהי B\in\mathbb{N}_+ יהי וההי G\in E עקום אליפטי יהי E/\mathbb{F}_v יהי יהי יהי אליפטיים: יהי אליפטיים: יהי
                                                                                                                                                                                                                                                    ECDLP(p, E, G, nG) = n
                                                                   \mathcal{O}\left(\sqrt{p}
ight) באשר לכל בעל סיבוכיות כי \mathcal{A} מתקיים כי בצל באשר לכל באשר לבאשר לבא
אזי G\in Eackslash\{\infty\} ויהי ליפטי המוגדר על אליפטי אליפטי E/\mathbb{F}_p יהי יהי אליפטיים: יהי אליפטיים: יהי אליפטי המוגדר אליפטי אליפטיים: יהי אליפטיים: ירי אליפטיים: ירי אליפטיים: ירי אליפטיים: ירי אליפטיים: ירי אליפטיים: ירי 
                                                                                                                                                                      כך \Pi^{\text{EC}}_{\text{DiffieHellman}} פרטיים מפתחות בעל מפתחות נגדיר נגדיר בעל
Communication Protocol \Pi^{\mathrm{EC}}_{\mathrm{DiffieHellman}}(p,f,G):
          A draws x \in [p-1]
          A sends xG as K_A
          B draws y \in [p-1]
          B sends yG as K_B
          A calculates K_{BA} \leftarrow x \cdot K_{B}
         B calculates K_{AB} \leftarrow y \cdot K_A
```

```
טענה: יהי p\in\mathbb{P} שורש פרימטיבי מודולו p\in\mathbb{P} תהא p\in\mathbb{P} חשיבה בזמן עבורה קיים יריב p\in\mathbb{P} בעל כוח חישובי
                                                                          \mathcal{B}(p,f,G,xG,yG)=xyG המקיים המקיים בעל כוח חישובי \mathcal{\tilde{O}}(T) בעל כוח חישובי
                                                                                                                                   \pi\left(x
ight)=|\mathbb{P}_{\leq x}| כך \pi:\mathbb{R}_{+}	o\mathbb{N} פונקציית ספירת הראשוניים: נגדיר
                                                                                                          \lim_{x	o\infty}rac{f(x)}{g(x)}=1 המקיימות f,g:\mathbb{R}	o\mathbb{R} פונקציות אסימפטוטיות: פונקציות פונקציות המקיימות
                                                                                                                                                             f,g:\mathbb{R} 	o \mathbb{R} אזי אזי f,g:\mathbb{R} 	o \mathbb{R} סימון: תהיינה
                                                                 \lim\sup_{x	o\infty}rac{f(x)}{g(x)}\leq 1 המקיימת g:\mathbb{R}	o\mathbb{R} אזי f:\mathbb{R}	o\mathbb{R} האי תהא
                                                                                                       f, f \lesssim g אזי אזי על ידי אסימפטוטית אסימ באשר f, g: \mathbb{R} 	o \mathbb{R} סימון: תהיינה
                                                            .(f\lesssim g)\Longleftrightarrow \left(\liminf_{x	o\infty}rac{g(x)}{f(x)}\geq 1
ight) אזי f,g:\mathbb{R}	o\mathbb{R} טענה: תהיינה f,g:\mathbb{R}	o\mathbb{R} אזי f,g:\mathbb{R}	o\mathbb{R} טענה: תהיינה f,g:\mathbb{R}	o\mathbb{R} אזי f,g:\mathbb{R}	o\mathbb{R} אזי f,g:\mathbb{R}	o\mathbb{R}
                                                                                                                             .(f\sim g)\Longleftrightarrow ((f\lesssim g)\wedge (g\lesssim f)) אזי f,g:\mathbb{R}	o\mathbb{R} טענה: תהיינה
                                                                                                                                                                                                                       \log = \ln הערה: בקורס זה
                                                                                                                                                     \log = \min אוי הערה: הערה: בעוו ט אוי הואפן איז הערה: איז איז חום פוסו.  \pi\left(2n\right) - \pi\left(n\right) \leq \frac{\log(4) \cdot n}{\log(n)}  איז n \in \mathbb{N}_+ איז \pi\left(x\right) \lesssim \frac{\log(4) \cdot x}{\log(x)}  מסקנה: \sum_{p \in \mathbb{P}_{\leq x}} \log\left(p\right) \lesssim \log\left(4\right) \cdot x  מסקנה: (2n) \geq \frac{4^n}{2n+1}  איז n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ למה: יהי n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ למה: יהי n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ למה: יהי n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ איז n \in \mathbb{N}_+ למה: יהי n \in \mathbb{N}_+ איז 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
                                                                                                                                                                           \sigma=\sigma + \frac{1}{n}טענה: יהיn\in\mathbb{N}_+ אזי n\in\mathbb{N}_+טענה: יהי
                                                                                                                                                                                                             \pi\left(x
ight)\gtrsimrac{\log\left(2
ight)\cdot x}{\log\left(x
ight)} משפט צ'בישב:
                                  מתקיים n\in\mathbb{N}_{\geq 2} עבורם לכל eta\in\mathbb{R}_{\geq 1} וקיים lpha\in(0,1] מתקיים סדר אזי קיים n\in\mathbb{N}_{+}	o \mathbb{N}
                                                                                                                                                                                                       .\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 אבל: יהי
                                                                                                     \sum_{n \in \mathbb{N}_{\leq x}} \left( a_n \cdot f \left( n \right) \right) = \left( \sum_{n \in \mathbb{N}_{\leq x}} a_n \right) \cdot f \left( x \right) - \int_1^x \left( \sum_{n \in \mathbb{N}_{\leq t}} a_n \right) \cdot f' \left( t \right) dt
                                                                                                                                                                                                \log(n!) = n \cdot \log(n) + O(n) למה:
                                                                                                                                                                        \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 K>0 משפט: קיים K>0 עבורו לכל \sigma עבורו לכל \sigma מסקנה: קיים \sigma עבורו לכל \sigma
                                                                                                                                                    \log\log(n) טענה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ מסקנה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ מסקנה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ טענה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ טענה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ טענה: n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+ אזי n \in \mathbb{N}_+
                                                                                                                                                                                                                  n! = \Theta\left(\left(rac{n}{e}
ight)^n \cdot \sqrt{n}
ight) טענה:
                                                                                                                                             \gamma=1-\int_{1}^{\infty}rac{t-\lfloor t
floor}{t^{2}}\mathrm{d}t כך כך גגדיר נגדיר נגדיר נגדיר אויילר־מסקרוני: נגדיר
                                                                                                                                                                                .\gamma = \lim_{n 	o \infty} \left( \left( \sum_{i=1}^n rac{1}{i} 
ight) - \log\left(n
ight) 
ight) טענה:
                                                                                                                                               משפט מרטנס: \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\geq 1 אז אי אם c\in\mathbb{R} אז אי אכונה: יהי
                                                                                                                                                                   c \leq 1 אז \pi\left(x
ight) \gtrsim rac{c \cdot x}{\log(x)} אזי אם c \in \mathbb{R} טענה: יהי
                                                                                                                                                                c=1 אז או\pi\left(x
ight)\simrac{c\cdot x}{\log(x)} אזי אם c\in\mathbb{R} מסקנה: יהי
                                                                                                                                              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 היי
                                                                                                                  .artheta\left(x
ight)=\sum_{p\in\mathbb{P}_{\leq x}}\log\left(p
ight) כך כך artheta: נגדיר נגדיר artheta:
```

```
\lim_{x 	o \infty} rac{\vartheta(x)}{x} = 1 משפט:
                                                                                                           \mathrm{Li}\left(x
ight)=\int_{2}^{x}rac{1}{\log(t)}\mathrm{d}t כך בו \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)} מסקנה:
                                                                                                        .\operatorname{Li}(x) = \sum_{k=0}^m \frac{(m-1)! \cdot x}{\log^m(x)} + \mathcal{O}\left(\frac{x}{\log^{m+1}(x)}\right) אזי m \in \mathbb{N} טענה: יהי m \in \mathbb{N}
                  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 לא הוכח בקורס משפט אדמר־דה-לה-ואלה-פוסן:
                                                                                                                                      \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 (x)=\mathrm{Li}\,(x)+\mathcal{O}\left(x\cdot\exp\left(-\log^{rac{2}{3}+arepsilon}(x)
ight)
ight) אזי (x)=\mathrm{Li}\,(x)+\mathcal{O}\left(x\cdot\exp\left(-\log^{rac{2}{3}+arepsilon}(x)
ight)
ight). לא הוכח בקורס
                                                                                                 השערה פתוחה \pi\left(x\right) \doteq \mathrm{Li}\left(x\right) + \mathcal{O}\left(\sqrt[r]{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}
                                                                                                         .\pi_{m,a}\left(\infty
ight)=\lim_{x	o\infty}\pi_{m,a}\left(x
ight) אזי a\in\mathbb{Z} ויהי m\in\mathbb{N} יהי 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 הוכח בקורס משפט דיריכלה: יהי
                              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) אזי (a,m)=1 באשר a\in\mathbb{Z} ויהי m\in\mathbb{N} מסקנה: יהי
\pi_{m,a}(x)=rac{1}{\omega(m)}\mathrm{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 יהי (GRH): השערת רימן המוכללת
Miller Rabin Primality Test (N;a) = True) \Longleftrightarrow (N \in \mathbb{P}) מתקיים N \in \mathbb{N}_+ עבורו לכל משפט: אם GRH משפט: אם
                                                                                                                                                                  לא הוכח בקורס.(a < c \log^2(N)
                                              	ilde{\mathcal{O}}\left(n^4
ight) אז קיים אלגוריתם דטרמיניסטי \mathcal{A} לבדיקת ראשוניות בעל בסיבוכיות ריצה GRH מסקנה:
                                                                                                            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}}\,(f=0)=arnothing אזי \mathrm{sols}_{\mathbb{Z}_N}\,(f=0)=arnothing באשר N\in\mathbb{N}_{\geq 2} ויהי f\in\mathbb{Z}\,[x_1,\ldots,x_n] טענה: יהי
                                                                                      \{\langle f \rangle \mid (f \in \mathbb{Z}\left[x_1,\ldots,x_n
ight]) \wedge (\mathrm{sols}_{\mathbb{Z}}\left(f=0
ight) 
eq \varnothing)\} 
otin \mathcal{R} משפט מטיאסביץ':
        a\in S^n עבורם a\in R^{n+1} וקיים a\in R^{n+1} וקיים a\in R^{n+1} עבורו אזי וקיים f\in R עבורו אזי f\in R עבורו אזי וקיים הומוגני בשני משתנים: יהי
                                                                                        f=0 משוואה דיופנטית הומוגנית בשני משתנים: יהי f\in\mathbb{Z}\left[x,y
ight] הומוגני אזי
                                             (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 אי מהמוגני)
                                            f\left(rac{a}{(a,b)},rac{b}{(a,b)}
ight)=0 אזי f\left(a,b
ight)=0 טענה: יהי f\left(a,b
ight)=0 הומוגני ויהיו a,b\in\mathbb{Z}\setminus\{0\} באשר f\left(a,b
ight)=0 וכן f\left(a,b
ight)=0 פתרון מצומצם/פרימיטיבי: יהי f\left(a,b
ight)=0 הומוגני אזי f\left(a,b
ight)=0 באשר f\left(a,b
ight)=0 וכן f\left(a,b
ight)=0
                                                                                      טענה: יהי f=\sum_{i=0}^n \zeta_i x^i y^{n-i} באשר \zeta\in\mathbb{Z}^{n+1} הומוגני ויהי הומוגני יהי
                                                                           \operatorname{sols}_{\mathbb{Z}}(f=0) = \{(da,db) \mid (d \in \mathbb{Z}) \land (f=0) \neq (a,b)\} פתרון פרימיטיבי של (a,b)
                                                                                                        b|\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,b) וכן a|\zeta_0 אזי a|\zeta_0 אזי וכן a|\zeta_0 אזי a|\zeta_0 וכן a,b)=1 ויהי וכן a,b)=1 ויהי וכן באשר באשר באשר באשר באשר לa,b)=1 ויהי וכן a|\zeta_0 אזי a|\zeta_0 אזי a|\zeta_0
                                              m|\zeta_0 אזי f(m)=0 באשר m\in\mathbb{Z} ויהי f=\sum_{i=0}^n\zeta_ix^i באשר באשר f\in\mathbb{Z}[x] אזי יהי f\in\mathbb{Z}[x]
                                                                                                  f=0 אאי f\in\mathbb{Z}_{\leq 1}\left[x,y
ight] יהי משתנים: יהי לינארית בשני משתנים:
                                                                                                 .(\mathrm{sols}_{\mathbb{Z}}\left(ax+by=c
ight)
eqarnothing)\Longleftrightarrow\left(\left(a,b
ight)|c
ight) אזי a,b,c\in\mathbb{Z} טענה: יהיו
       \operatorname{sols}_{\mathbb{Z}}\left(ax+by=c\right)=\left\{\left(lpha+rac{m\cdot b}{(a,b)},eta-rac{m\cdot a}{(a,b)}
ight)\,\Big|\,\,m\in\mathbb{Z}
ight\}אזי (lpha,eta)\in\operatorname{sols}_{\mathbb{Z}}\left(ax+by=c
ight) ויהי a,b,c\in\mathbb{Z} ויהי a,b,c\in\mathbb{Z} אזיי (lpha,eta)\in\operatorname{sols}_{\mathbb{Z}}\left(ax+by=c
ight) אזיי (a,b)\in\mathbb{Z} ויהי a,b,c\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z} אזיי (a,b)\in\mathbb{Z}
```

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

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

טענה: יהי מהבאים מהבאים עבורם $lpha,eta,\gamma,\delta,arepsilon,\zeta\in\mathbb{Q}$ אזי קיימים אזי אזי יהי $f\in\mathbb{Z}_{<2}\left[x,y
ight]$ אזי קיימים

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

```
.(\mathrm{sols}_{\mathbb{Z}}\,(x^2=a)
eq\varnothing)\Longleftrightarrow(a=\square) אזי a\in\mathbb{Z} יהי מענה: יהי a\in\mathbb{Z}
                                                                                                                     \operatorname{sols}_{\mathbb{Z}}\left(x^{2}=a
ight)=\{\pm\sqrt{a}\} אזי a=\square באשר a\in\mathbb{Z} יהיa\in\mathbb{Z}
\mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=a
ight)\subseteq\left\{\left(s\cdot\sqrt{a+dy^2},y
ight)\,\Big|\,\left(s\in\{\pm1\}
ight)\wedge\left(-\sqrt{\left|rac{a}{d}
ight|}\le y\le\sqrt{\left|rac{a}{d}
ight|}
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}
                          \mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=0
ight)=\left\{\left(sm\cdot\sqrt{d},rm
ight)\;\middle|\;(s,r\in\{\pm1\})\land(m\in\mathbb{Z})
ight\} אזי d=\square באשר שר d\in\mathbb{N}_+ יהי יהי d\in\mathbb{N}_+ יהי
                                      \operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right)=igcup_{\substack{(u,v)\in\mathbb{Z}^2\\a=uv}}\operatorname{sols}_{\mathbb{Z}}\left(\left\{egin{array}{ll} x-\sqrt{dy}=u\\x+\sqrt{dy}=v\end{array}
ight) אזי d=\square אזי d\in\mathbb{N}_+ יהי a\in\mathbb{Z} יהי a\in\mathbb{Z} יהי a\in\mathbb{Z} אזי a\in\mathbb{Z} אזי a\in\mathbb{Z} אזי a\in\mathbb{Z} אזי a\in\mathbb{Z}
                                                                                  a^2-dy^2=a אזי d
eq\square באשר באשר d\in\mathbb{N}_+ ויהי a\in\mathbb{Z}\backslash\{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 d \in \mathbb{Z} באשר שור d \neq d אוי d \neq d באשר מענה: יהי
                                             eta=\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 d\in\mathbb{Z} אזי מענה: יהי
                                               -arphi\left(lpha+eta\sqrt{d}
ight)=(lpha,eta) כך כך arphi:\mathbb{Z}\left[\sqrt{d}
ight]	o\mathbb{Z}^2 אזי נגדיר d
eq\square אזי נגדיר d
eq\square כד
                                                                                               ע ועל. \varphi אזי איז היי של באשר d 
eq \square ותהא ותהא א העתקת המקדמים א באשר ועל. ועל.
                                                                                 (lpha,eta)\mapsto lpha+eta\sqrt{d} כך \mathbb{Z}\left|\sqrt{d}
ight| כדער משכן את שכן משכן d
eq\square באשר להיי יהיd\in\mathbb{Z}
                                                                                                \overline{lpha+eta\sqrt{d}}=lpha-eta\sqrt{d} אזי lpha,eta\in\mathbb{Z} ויהיו d
eq\square באשר באשר מהי יהי לבמדה: יהי
                                             \overline{lphaeta}=\overline{lpha}\cdot\overline{eta} וכן \overline{lpha+eta}=\overline{lpha}+\overline{eta} וכן \overline{(\overline{lpha})}=lpha ויהיי a,eta\in\mathbb{Z}\left[\sqrt{d}
ight] ויהיי d
eq \square באשר ש
                                                                                             \alpha=lphaטענה: יהי\alpha=lpha lpha באשר lpha=d ויהי lpha\in\mathbb{Z} אזי lpha\in\mathbb{Z} טענה: יהי lpha
                                  . 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} הינו אוטומורפיזם חוגים.
                                                                                       N\left(lpha
ight)=lpha\cdot\overline{lpha} כך N:\mathbb{Z}\left[\sqrt{d}
ight]	o\mathbb{Z} אזי נגדיר d
eq\square באשר מדרה: יהי d\in\mathbb{Z}
                                                                                     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 שנה: יהי d\in\mathbb{Z} אזי d\in\mathbb{Z}
                                                                                                                                    \mathbb{Z}\left[\sqrt{d}
ight]^	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\} איי d
eq\mathbb{Z} וכן d\in\mathbb{Z} וכן a\in\mathbb{Z}\setminus\{0\} איי a,b\in\mathbb{Z}\setminus\{0\} איי a,b\in\mathbb{Z}\setminus\{0\} וכן a,b\in\mathbb{Z}\setminus\{0\} איי a,b\in\mathbb{Z}\setminus\{0\} וכן יהיו
                                                                                                                                                                         (\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 אזי נגדיר d
eq\square אזי נגדיר d
eq\square
                                                                                                                                                         .SG \left(\left(\alpha,\beta\right),\left(\gamma,\delta\right)\right)=\left(\alpha\gamma+d\beta\delta,\alpha\delta+\beta\gamma\right)
\mathrm{SG}\left(\left(lpha,eta
ight),\left(\gamma,\delta
ight)
ight)=\left(lpha+eta\sqrt{d}
ight)\left(\gamma+\delta\sqrt{d}
ight) איי \left(lpha,eta
ight),\left(\gamma,\delta
ight)\in\mathrm{sols}_{\mathbb{Z}}\left(x^{2}-dy^{2}=1
ight) יסענה: יהי d
eq \mathbb{Z} באשר d\in\mathbb{Z} יהיי
                                                                                     \left(\operatorname{sols}_{\mathbb{Z}}\left(x^{2}-dy^{2}=1\right),\operatorname{SG}
ight) אזי d
eq\square חבורה אבלית. מסקנה: יהי d\in\mathbb{Z}
                                                                                        \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\mathbb{D} אזי d\in\mathbb{N}
                                                                                                     \mathrm{sols}_{\mathbb{Z}}\left(x^2-dy^2=1
ight)=\mathbb{Z}\left[\sqrt{d}
ight]^{	imes} אזי d
eq \square באשר שר 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\} אוי d
eq \square באשר של d\in\mathbb{N} הגדרה: יהי
            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\perp}}^	imes \{\pm 1\} אזי d
eq \square באשר שר d\in\mathbb{N} יהי
                                                                                                                                                                                    [lpha]=lpha אזי lpha\in\mathbb{R} סימון: יהי
   טענה: יהיa_0\in\mathbb{R} יהיו a_1\ldots a_n\in\mathbb{R} יהיו a_1\ldots a_n\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}
```

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

- $.rac{p_k}{q_k}=[a_0,\ldots,a_k]$ מתקיים $k\in\mathbb{N}_{\leq n}$ לכל $.inom{p_k}{q_k}rac{p_k}{q_{k-1}}ig)=\prod_{i=0}^kinom{a_i}{1}$ מתקיים מקיים $k\in\mathbb{N}_{\leq n}$ לכל .
- $a_k = a_k q_{k-1} + q_{k-2}$ וכן $p_k = a_k p_{k-1} + p_{k-2}$ מתקיים $k \in \mathbb{N}_{\leq n}$ לכל
 - $p_k q_{k-1} q_k p_{k-1} = (-1)^{k+1}$ מתקיים $k \in \mathbb{N}_{\leq n}$ לכל

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

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

 $[a_0,\ldots,a_n]$ אזי $a_1\ldots a_n\in\mathbb{N}_+$ ויהיו $a_0\in\mathbb{Z}$ יהי $n\in\mathbb{N}$ אזי יהי

טענה: יהיו $[a_0,\ldots,a_n]=[b_0,\ldots,b_m]$ באשר $[a_0,\ldots,a_n]=[b_0,\ldots,b_m]$ אזי אחד מהבאים נכון מהבאים נכון יהיו $a_0,b_0\in\mathbb{Z}$ יהי יהיו

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

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 $lpha\in\mathbb{Q}$ $.\alpha = [a_0, \ldots, a_n]$

אזי $b\in\mathbb{Z}ackslash\{0\}$ ויהי $a\in\mathbb{Z}$ יהי משולב פשוט למספר רציונלי: יהי

Algorithm RationalContinuedFraction (a, b):

if b = 0 then return $(q, r) \leftarrow \text{RemainderDiv}(a, b)$ return $[q] \parallel RationalContinuedFraction(b, r)$

.RationalContinuedFraction $(a,b)=rac{a}{b}$ אזי $b\in\mathbb{Z}\setminus\{0\}$ ויהי $a\in\mathbb{Z}$ ויהי $a\in\mathbb{Z}$

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

. סענה: תהא $i\in\mathbb{N}_+$ לכל $a_i\geq 1$ באשר $a:\mathbb{N} o\mathbb{R}$ אזי מענה:

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

. 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 $lpha\in\mathbb{R}\backslash\mathbb{Q}$ אזי קיים ויחיד שבר

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

Algorithm IrrationalContinuedFraction (n, α) :

if n = 0 then return

return $[|\alpha|] \parallel \text{IrrationalContinuedFraction}(n-1, \text{Cycling}(\alpha))$

 $\lim_{n \to \infty}$ Irrational
ContinuedFraction $(n, \alpha) = \alpha$ אזי $\alpha \in \mathbb{R} \backslash \mathbb{Q}$ יהי

 $(rac{p_k}{q_k})=\left(\prod_{i=0}^k\left(egin{smallmatrix}a_i&1\\1&0\end{smallmatrix}
ight)
ight)(rac{1}{0})$ 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 $k\in\mathbb{N}$ מחקנים $k\in\mathbb{N}$ מחקנים $k\in\mathbb{N}$ שבר משולב פשוט אינסופי ויהי (p,q) ייצוג שברי של $k\in\mathbb{N}$ אזי $k\in\mathbb{N}$ ויהי $k\in\mathbb{N}$ 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 $k\in\mathbb{R}$ ויהי $k\in\mathbb{N}$ ייצוג שברי של $k\in\mathbb{N}$ אזי לכל $k\in\mathbb{N}$ מתקיים $k\in\mathbb{R}$ מתקיים $k\in\mathbb{R}$

 $\left| lpha - rac{\zeta}{\xi}
ight| > \left| lpha - rac{p_n}{q_n}
ight|$ ייצוג שברי של lpha יהי $lpha \in \mathbb{R}$ ויהי $eta \in \mathbb{R} \setminus \mathbb{Q}$ יהי $lpha \in \mathbb{R} \setminus \mathbb{Q}$ יהי $lpha \in \mathbb{R} \setminus \mathbb{Q}$ יהי עבורו $n\in\mathbb{N}$ אזי קיים $|lpha-rac{\zeta}{arepsilon}|<rac{1}{2arepsilon^2}$ באשר $\xi\in\mathbb{N}$ ויהי $\zeta\in\mathbb{Z}$ ויהי $\zeta\in\mathbb{Z}$ אזי קיים lpha אזי קיים lpha $q_n = \xi$ וכן $p_n = \zeta$

 $i\in[d]$ אזי קיים $q\in[N^d]$ וקיים $q\in[N^d]$ ויהי אזי קיים $d,N\in\mathbb{N}_+$ עבורם לכל לקירוב אופנטי: יהיו אזי קיים $\left|v_i-rac{1}{q}u_i
ight|<rac{1}{qN}$ מתקיים

 $a_n=a_{n+T}$ המקיימת $a:\mathbb{N} o\mathbb{R}$ לכל אזי פונקציה מחזורית החל ממקום מסויים: יהיו אזי הייו $N,T\in\mathbb{N}$ אזי פונקציה מחזורית החל ממקום מסויים: יהיו $a_0\dots a_{N-1}\overline{a_N\dots a_{N+T-1}}=a$ אזי N אזי $a:\mathbb{N} o\mathbb{R}$ מחזורית בעלת מחזורית החל מNשבר משולב פשוט מחזורית החל ממקום מסויים. [a] עבורו [a] עבורי מחזורי. שבר משולב פשוט אינסופי

```
A,B\in (0,\sqrt{d}) וכן A\in (0,d) ריבועי מצומצם אזי A,B\in \mathbb{Z} וכן B^2\equiv d\mod A באשר אוכן A,B\in \mathbb{Z} ויהיי A\in \mathbb{N}
                                                                                    \left|\left\{lpha\in\mathbb{Q}\left(\sqrt{d}
ight)\ \middle|\ מסקנה: יהי d\in\mathbb{N} אזי a
                                             a_n=a_{n+T} המקיימת a:\mathbb{N}	o \mathbb{R} לכל T\in \mathbb{N} אזי פונקציה a_n=a_{n+T} המקיימת
                                                            שבר משולב פשוט מחזורי מחזורי טהור: שבר משולב פשוט מחזורי [a] עבורו שבר מחזורי טהורה.
                               (ריבועי מצומצם). איי (קיים שבר משולב פשוט מחזורי טהור 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 אאי קיים מסקנה: יהי
עבורו a_m עבורו אזי קיים m\in\mathbb{N} אזי קיים a_{n+1}=\operatorname{Cycling}(a_n) וכן a_0=lpha כך a:\mathbb{N}	o\mathbb{R}\setminus\mathbb{Q} ריבועי נגדיר lpha\in\mathbb{R}\setminus\mathbb{Q} מסקנה: יהי
                                                                                                                                     mמצומצם וכן a מחזורית החל מ
                                                   (\alpha) אוי (קיים שבר משולב פשוט מחזורי [a] עבורו שבר משרט: יהי \alpha \in \mathbb{R} \setminus \mathbb{Q} אוי (קיים שבר משולב משפט: יהי
יצוג (p,q) ייצוג \sqrt{d}=[a] באשר באשר n=1 באשר n=1 משפט: יהי n=1 באשר n=1 ייצוג n=1 ייצוג n=1 ייצוג מחזור n=1 ייצוג
                                                                                                       .p_{kn-1}^2-dq_{kn-1}^2=(-1)^{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 מחזור מחזור מחזור a:\mathbb{N}\to\mathbb{N} תהא תהא n\in\mathbb{N} יהי ויהי d
eq \square באשר באשר מחזור ייצוג
                                                                                                     (\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) = (p_{n-1}, q_{n-1}) איז n \in \mathbb{N}_{\operatorname{odd}} שנו
יצוג (p,q) ייצוג \sqrt{d}=[a] יהי d \in \mathbb{N} יהי d \in \mathbb{N} יהי ויהי d \in \mathbb{N} יהי יצוג d \in \mathbb{N} יהי יצוג
                                                                                                                                                               שברי של [a] אזי
                                                                                                        \operatorname{sols}_{\mathbb{Z}}(x^2 - dy^2 = 1) \setminus \{(1,0), (-1,0)\} \neq \emptyset \bullet
                                                 \min_{\pi_2} \left( \operatorname{sols}_{\mathbb{N}} \left( x^2 - dy^2 = 1 \right) \setminus \left\{ (1,0), (-1,0) \right\} \right) = (p_{n-1}, q_{n-1}) אם n \in \mathbb{N}_{\text{even}} שנ
                                               \min_{\pi_2} \left( \operatorname{sols}_{\mathbb{N}} \left( x^2 - dy^2 = 1 \right) \setminus \left\{ (1,0), (-1,0) \right\} \right) = (p_{2n-1}, q_{2n-1}) אם n \in \mathbb{N}_{\operatorname{odd}} סי
                         \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 באשר d \in \mathbb{N} הפתרון היסודי למשוואת פל: יהי
                                             arepsilon=u+v\sqrt{d} אזי x^2-dy^2=1 שלי של הפתרון היסודי d
eq\square אזי איזי מימון: יהי ל
                                             \langle arepsilon 
angle = \mathbb{Z} \left[ \sqrt{d} 
ight]_{1+}^	imes אזי x^2 - dy^2 = 1 שלי הפתרון היסודי של d 
otin \mathbb{N} אזי משפט: יהי d 
otin \mathbb{N} באשר ויהי
n\in\mathbb{Z} מסקנה: יהי d
eq \log_{\mathbb{Z}}(x^2-dy^2=1) יהי של d\in\mathbb{N} יהי מסקנה: יהי d
eq \square יהי אזי קיים d\in\mathbb{N} אזי קיים
                                                                                                                        \alpha + \beta \sqrt{d} = s \cdot \varepsilon^n עבורם s \in \{\pm 1\} וקיים
```

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

 $eta = \delta$ טענה: יהי $eta = \gamma$ אזי $eta = \gamma + \delta \sqrt{d} = \gamma + \delta \sqrt{d}$ באשר $eta = \alpha, \beta, \gamma, \delta \in \mathbb{Q}$ ויהיו $a \in \mathbb{R}$ אזי $a \in \mathbb{R}$ באשר $a \in \mathbb{R}$ העתקת המקדמים: יהי $a \in \mathbb{R}$ באשר $a \in \mathbb{R}$ אזי נגדיר $a \in \mathbb{R}$ העתקת המקדמים: 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 $\sqrt{d}
otin \mathbb{Q}$ ונגדיר 0 באשר 0 באשר 0 באשר 0 באשר 0 באשר 0 ונגדיר 0 באשר 0 ונגדיר 0 באשר 0 באשר 0 באשר 0 ונגדיר 0 וונגדיר 0 וונגדי

 $A,B\in\mathbb{Z}$ מסקנה: יהי $A,B\in\mathbb{Z}$ אזי (lpha ריבועי) אזי (קיים $a\in\mathbb{N}$ עבורו $a\in\mathbb{N}$ אזי (alpha ריבועי) אזי ($alpha^2+blpha+c=0$ עבורם $a\in\mathbb{Z}\setminus\{0\}$ עבורם ($alpha^2+blpha+c=0$).

.($lpha=rac{B+\sqrt{d}}{A}$ וכן $B^2\equiv d\mod A$ עבורם $A,B\in\mathbb{Z}$ וקיימים $d\in\mathbb{N}$ וכן $A,B\in\mathbb{Z}$ טענה: יהי $lpha\in\mathbb{R}$ אזי $lpha\in\mathbb{R}$

 $Cycling\left(lpha
ight)$ עד להיות Cycling (lpha) ריבועי וכן $d\in\mathbb{Q}$ עד להיות עד להיות היהי $\alpha\in\mathbb{R}$ ריבועי יהי $\alpha\in\mathbb{R}$

(עועל. φ חח"ע וועל. q העתקת המקדמים אזי איז חח"ע וועל. מסקנה: יהי ל $d\in\mathbb{R}$ האי

 $A,B\in\mathbb{Z}$ מסקנה: יהי $A,B\in\mathbb{Z}$ אזי (קיים לקיים) אזי (קיים מסקנה: יהי $lpha\in\mathbb{R}$ אזי (מסקנה: יהי

lpha=eta אזי $\operatorname{Cycling}\left(lpha
ight)=\operatorname{Cycling}\left(eta
ight)$ אזי מענה: יהיו $lpha,eta\in\mathbb{R}$ ריבועיים מצומצמים באשר

 $lpha+eta\sqrt{d}=lpha-eta\sqrt{d}$ אזי $lpha,eta\in\mathbb{Q}$ ויהיו $d\in\mathbb{R}$ הצמדה: יהי

 $lpha \in \mathbb{Q}\left(\sqrt{d}
ight)$ מספר ריבועי: מספר $lpha \in \mathbb{R}$ עבורו קיים מספר מספר

 $\overline{lpha}\in(-1,0)$ מספר ריבועי אומצם: מספר ריבועי מצומצם: מספר באיר מספר ריבועי מצומצם: מסקנה: יהי $d\in\mathbb{N}$ באשר באשר באשר $d\in\mathbb{N}$ ריבועי מצומצם. ריבועי מצומצם אזי $\alpha\in\mathbb{R}$ ריבועי מצומצם מענה: יהי $\alpha\in\mathbb{R}$

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

```
אזי \operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=a\right) 
eq \varnothing באשר a\in\mathbb{Z}\setminus\{0\} ויהי d
eq \square באשר באשר a\in\mathbb{N} אזי יהי
                                                                                           \left(\frac{a}{p}\right)\in\{0,1\} מתקיים p|d המקיים p\in\mathbb{P}_{>2} •
                                                                                                                  a \mod 4 \in \{0,1\} אז 4|d אם •
                                                                                                              a \mod 8 \in \{0,1,4\} אם a \mod 8 \in \{0,1,4\} אם a \mod 8
(lpha,eta)\in\operatorname{sols}_{\mathbb{Z}}\left(x^2-dy^2=a
ight) יהי a\in\mathbb{Z}\setminus\{0\} יהי x^2-dy^2=1 יהי של a\in\mathbb{Z}\setminus\{0\} יהי a\in\mathbb{Z}\setminus\{0\} יהי משפט: יהי
         a+eta\sqrt{d}=s\cdotarepsilon^n\cdot\left(z+w\sqrt{d}
ight) איי קיימים s\in\{\pm 1\} באשר z+w\sqrt{d}<\sqrt{|a|}arepsilon וקיים s\in\{\pm 1\} וקיים איי
                                                                                  \{\langle f \rangle \mid (f \in \mathbb{Z}_{\leq 2}[x,y]) \land (\operatorname{sols}_{\mathbb{Z}}(f=0) \neq \varnothing)\} \in \mathcal{R} מסקנה:
                                                                                                                         \mathbb{Q}\left(i
ight)=\mathbb{Q}+i\cdot\mathbb{Q} מספרי גאוס:
                                                                                                                                         מסקנה: \mathbb{Q}(i) שדה.
                                                                                                                            \mathbb{Z}\left[i
ight]=\mathbb{Z}+i\cdot\mathbb{Z} שלמי גאוס:
                                                                                                                       מסקנה: \mathbb{Z}[i] חוג אבלי בעל יחידה.
                                                   a,b=0 עבורו לכל a,b\in A המקיימים a,b\in A מתקיים A עבורו לכל
                                                                     A^{	imes}=\{a\in A\mid \exists h\in A.ah=ha=1\} הגדרה: יהי A תחום שלמות אזי
                                         ac=ac אינבר מחלק איבר: יהי a\in A תחום שלמות ויהי a\in A אזי אינר מחלק איבר: יהי ac=ac
                                                                        a|b אזי אולק את מחלק באשר a באשר a,b\in A ויהיו
                                                                                                       טענה: יהי A תחום שלמות ויהיו A אזי
                                                                                                                             a|c אם a|b וכן a|b אז
                                                                                        a|ab+ec מתקיים d,e\in A אז לכל a|c וכן
                                                                                                                                           a|0 וכן 1|a
                                                                                                     (\exists u \in A^{\times}.a = bu) \iff ((b|a) \land (a|b)) \bullet
                                                                                  a|a וכן a|b וכן a,b\in A המקיימים a|b וכן הברים: יהי
                                                                                       a\sim b אזי חברים a,b\in A ויהיו שלמות ויהיו A תחום אזי
                                                                                                        . טענה: יהי A תחום שלמות אזי יחס שקילות.
                                                         ac \sim bd אזי a \sim b וכן a \sim b באשר a,b,c,d \in A אזי שלמות ויהיו
                                                                                                                 N\left(lpha
ight)=\left|lpha
ight|^{2} אזי lpha\in\mathbb{Z}\left[i
ight] טענה: יהי
                                                                                             (N\left(lpha
ight)=0)\Longleftrightarrow (lpha=0) אזי lpha\in\mathbb{Z}\left[i
ight] יהי יהי
וכן N\left(
ho
ight) < N\left(eta
ight) המקיימים \kappa, 
ho \in \mathbb{Z}\left[i\right] אזי קיימים \beta \in \mathbb{Z}\left[i\right] \setminus \{0\} ויהי \alpha \in \mathbb{Z}\left[i\right] ויהי שארית בשלמי גאוס: יהי
יכן |N\left(\rho
ight)|<|N\left(eta
ight)| יהי d\in\{2,-2,3\} יהי המקיימים \kappa,
ho\in\mathbb{Z}\left[\sqrt{d}\right]\setminus\{0\} יהי היהי \alpha\in\mathbb{Z}\left[\sqrt{d}\right] יהי
                                                                                  נורמה N:A \to \mathbb{N} אזי שלמות אוי A המקיימת נורמה אוקלידית: יהי
                                                                                              (a=0) \Longleftrightarrow (N(a)=0) מתקיים a \in A לכל
```

 $a\in\mathrm{QR}_d\cup\{0\}$ אזי $\mathrm{sols}_\mathbb{Z}\left(x^2-dy^2=a
ight)
eq \emptyset$ באשר באשר $a\in\mathbb{Z}\setminus\{0\}$ ויהי ויהי $d
eq \mathbb{D}$ באשר באשר מענה: יהי

- $N\left(a
 ight) \leq N\left(b
 ight)$ מתקיים a|b המקיימים $b \in A \setminus \{0\}$ ולכל $a \in A$
- $A \in A \setminus \{0\}$ וכן a = qb + r המקיימים a = qb + r המקיימים $a \in A \setminus \{0\}$ ולכל $a \in A$

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

 $\mathbb{Z}\left[i\right]$ טענה: N הינה נורמה אוקלידית מעל וורמה N טענה: ענה: יהי אוקלידית מעל וורמה וורמה וורמה $d\in\{2,-2,3\}$ טענה: יהי

 $N:A \to \mathring{\mathbb{N}}$ תחום אוקלידי: תחום שלמות A עבורו קיימת נורמה אוקלידיו: תחום שלמות

.dA=aA+bA עבורו $d\in A$ סענה: יהי $a,b\in A$ ויהיו ויהיו A

 $(aA=bA) \Longleftrightarrow (a\sim b)$ אזי $a,b\in A$ ויהיו אוקלידי ויהיו A תחום אוקלידי ויהיו

 $\operatorname{Gcd}\left(a,b\right)=\left\{d\in A\mid dA=aA+bA
ight\}$ אזי $a,b\in A$ ויהיו אוקלידי ויהיו A תחום אוקלידי ויהיו

 $\gcd(a,b)\in \mathrm{Gcd}\,(a,b)$ המקיימת $\gcd:A^2 o A$ אזי אוקלידי אוי תחום אוקלידי היA מחלק משותף מירבי: יהי

 $(a,b)=\gcd{(a,b)}$ אזי $a,b\in A$ ויהיו אוקלידי ויהיו A תחום אוקלידי

 $\gcd(a,b)|b$ וכן $\gcd(a,b)|a$ אזי $a,b \in A$ ויהיו אוקלידי ויהיו A תחום אוקלידי ויהיו

```
\gcd(a,b)=na+mb עבורם n,m\in A אזי קיימים a,b\in A אוי ויהיו A
                                                            |c| \gcd(a,b) אזי |c| וכן |c| אזי |c| אזי ויהיו |c| אזי ויהיו |c| אזי ויהיו
a,b \in A עבורו לכל a,b \in A מתקיים שלמות אזי a,b \in A עבורו לכל a,b \in A עבורו לכל איבר אי־פריק: יהי a,b \in A מתקיים אזי a,b \in A
             p(a) \lor (p|a) \lor (p|b) מתקיים a,b \in A עבורו לכל p \in A \lor (A^{	imes} \cup \{0\}) מתקיים מתקיים a,b \in A עבורו לכל
                                                                       .(יבריק)\iff תחום אוקלידי ויהי a \in A אזי ויהי a \in A ראשוני).
                                                                                     תחום בעל פריקות יחידה לראשוניים: תחום שלמות A המקיים
                                             .a \sim \prod_{i=1}^k p_i עבורם ראשוניים p_1 \dots p_k \in Aוקיימים ווקיים k \in \mathbb{N}_+ קיים a \in A \backslash \left\{0\right\} לכל
עבורה \sigma\in S_k וכן קיימת k=\ell מתקיים \prod_{i=1}^{\hat{k}}p_i\sim\prod_{i=1}^\ell q_i עבורה ראשוניים באשר p_1\dots p_k,q_1\dots q_\ell\in A ולכל
                                                                                                                           i \in [k] לכל p_i \sim q_{\sigma(i)}
                                                                                                        אזי p,q\in A אזי אוקלידי ויהיו A תחום אוקלידי
                                                                                                                        .(ראשוני) (q) \leftarrow (p) ראשוני).
                                                                                                                    (q) \Leftrightarrow (q) \Leftrightarrow (q) אי־פריק).
                                                  (a\sim b)\Longleftrightarrow ((N\,(a)=N\,(b))\wedge (a|b)) אזי a,b\in A ויהיו אוקלידי ויהיו A
                                                                       משפט: יהי A תחום אוקלידי אזי A תחום בעל פריקות יחידה לראשוניים.
                                                                                             מסקנה: \mathbb{Z}\left[i
ight] הינו תחום בעל פריקות יחידה לראשוניים.
. תחום אוקלידי). באשר \mathbb{Z}\left[\sqrt{d}
ight] מתקיים (\left[\sqrt{d}
ight] תחום בעל פריקות יחידה לראשוניים) אז לכל לבל שנט משפט: אם d 
eq \mathbb{Z} מתקיים לבל מתקיים (d \neq \mathbb{Z} מתקיים ווא לכל מתקיים).
                                                                                                                                            לא הוכח בקורס
                                                                                   (a \mod n) = a + nA אזי n, a \in A מודולו: יהי A חוג ויהי
                                  a,b\in A איברים שקולים תחת מודולו: יהיA חוג ויהיA אוג ויהיA איברים שקולים תחת מודולו: יהי
                                                            a\equiv b \mod n אזי מודולו מודולו a,b\in A ויהיו ויהיו n\in A חוג יהי A חוג יהי
                                                                    (n|(a-b)) \Longleftrightarrow (a \equiv b \mod n) אזי n,a,b \in A חוג ויהי A חוג ויהי
                         a+b\equiv c+d\mod n אזי b\equiv d\mod n וכן a\equiv c\mod n באשר a,b,c,d\in\mathbb{Z} אזי a+b\equiv c+d\mod n
                                    (a \mod n) + (b \mod n) = ((a+b) \mod n) אזי a,b \in A ויהיו n \in A ויהיו n \in A ויהיו
                                 ab\equiv cd\mod n אזי אb\equiv d\mod n וכן a\equiv c\mod n באשר n,a,b,c,d\in\mathbb{Z} אזי חוג ויהיו
                                        (a \mod n) \cdot (b \mod n) = ((a \cdot b) \mod n) אזי a,b \in A ויהיו n \in A חוג יהי n \in A חוג יהי
                                                                                                          טענה: יהי A חוג ויהי n \in A אזי A/n חוג.
                                                                                             A/nאזי n\in A חוג ויהי n\in A אזי n\in A
                                                                .(ראשוני) אזי אוקלידי ויהי A/n שדה) שדה אוזי אזי ויהי חום אוקלידי ויהי אוקלידי ויהי ויהי n \in A \setminus \{0\}
                                                                              \mathbb{P}_A = \{a \in A \mid A \; | \; A סימון: יהי A תחום שלמות אזי שלמות אזי מעל
                                                          \left\{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid0\in\left\{\operatorname{Re}\left(\pi
ight),\operatorname{Im}\left(\pi
ight)
ight\}
ight\}=\left\{p\in\mathbb{P}\mid p\equiv3\mod4
ight\}\cdot\mathbb{Z}\left[i
ight]^{	imes} טענה:
                                                                                                                      .\overline{\pi} \in \mathbb{P}_{\mathbb{Z}[i]} אזי \pi \in \mathbb{P}_{\mathbb{Z}[i]} למה: יהי
                                        N\left(\left\{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid\left(0
otin\{\operatorname{Re}\left(\pi
ight),\operatorname{Im}\left(\pi
ight)
ight\}
ight)\wedge\left(\pi
ot\sim1+i
ight)
ight\}
ight)=\left\{p\in\mathbb{P}\mid p\equiv1\mod4
ight\}טענה:
                                                         a,b \in \mathbb{Z} מסקנה: יהי p \equiv a,b \in \mathbb{Z} באשר p \equiv 1 \mod 4 באשר p \in \mathbb{P} מסקנה: יהי
                                                                        אזי p\equiv 1\mod 4 באשר p\in\mathbb{P} אזי יהי ראשוני כסכום ריבועיים: יהי
Algorithm SumSquaresPrime(p):
    c \leftarrow \text{QNR}_p
    t \leftarrow c^{\frac{p-1}{4}} \bmod p
     a + ib \leftarrow \text{EuclidGCD}_{\mathbb{Z}[i]}(p, t + i)
     return (a, b)
             \sum_{i=1}^2 \left( \operatorname{SumSquaresPrime}\left(p 
ight) \right)_i^2 = p וכך SumSquaresPrime (p) \in \mathbb{Z}^2 אזי p \equiv 1 \mod 4 באשר p \in \mathbb{P} סענה: יהי
                                                                                     \{\pi\in\mathbb{P}_{\mathbb{Z}[i]}\mid\pi\sim1+i\}=\{\pi\in\mathbb{Z}\left[i
ight]\mid\pi\sim1+i\} טענה:
```

שונים באשר $p_1\dots p_r,q_1\dots q_s\in\mathbb{P}$ קיימים איז $k,r,s\in\mathbb{N}$ שונים באשר אזי (קיימים $a,b\in\mathbb{Z}$ עבורם $a,b\in\mathbb{Z}$

. $(n=2^k\cdot\prod_{i=1}^r p_i^{e_i}\cdot\prod_{i=1}^s q_i^{2f_i}$ עבורם $e_1\dots e_r,f_1\dots f_s\in\mathbb{N}_+$ וקיימים $q_j\equiv 3\mod 4$

 $\mathbb{Z}[i]/lpha\mathbb{Z}[i]$ אזי $lpha=[i]/lpha\mathbb{Z}[i]$ מערכת נציגים של אזי $lpha\in\mathbb{Z}[i]$ מערכת מיה: יהי $lpha\in\mathbb{Z}[i]$

```
lpha^{p^2-1}\equiv 1\mod p אזי lpha\in\mathbb{Z}[i] ויהי p\equiv 3\mod 4 באשר p\in\mathbb{P} יהי יהי \mathbb{Z}[i]: יהי
                           f=\sum_{i=0}^n\zeta_{i+1}x^i וכן \zeta_{n+1}
eq 0 וכן המקיים \zeta\in\mathbb{F}^{n+1} וקיים וכן f:\mathbb{F}	o\mathbb{F} וכן המקיים לינום: יהי
                                                                                                                            \mathbb{F}[x]=\{f:\mathbb{F}	o\mathbb{F}\mid פולינום f\} שדה אזי \mathbb{F} שדה אזי פולינום ויהי
                                                                                                                                                     . טענה: יהי \mathbb{F}\left[x
ight] שדה אזי \mathbb{F}\left[x
ight] הינו חוג אבלי בעל יחידה
                                                                                                                                                            \alpha\mapsto \lambda x.\alpha כך \mathbb{F}\hookrightarrow\mathbb{F}[x] הערה: יהי \mathbb{F} אזי נשכן
                                                 \deg\left(\sum_{i=0}^n\zeta_{i+1}x^i
ight)=n אזי \zeta_{n+1}
eq 0 באשר באשר \gamma\in\mathbb{F}^{n+1} ויהי ויהי \gamma\in\mathbb{F} שדה יהי שדה יהי ויהי
                                                                                                                                                                               \deg\left(0
ight)=-\infty שדה אזי \mathbb{F} יהי יהי הגדרה: יהי
                                                  \mathrm{lc}\left(\sum_{i=0}^n\zeta_{i+1}x^i
ight)=\zeta_{i+1} אזי אזי \zeta_{n+1}
eq 0 באשר באשר \gamma\in\mathbb{F}^{n+1} ויהי \gamma\in\mathbb{F} ויהי המקדם המוביל: יהי
                                                                                                                                                                                          .\mathrm{lc}\left(0
ight)=0 אזי שדה \mathbb{F} יהי יהי
                                                         \mathrm{lc}\left(fg
ight)=\mathrm{lc}\left(f
ight)\mathrm{lc}\left(g
ight) וכך \mathrm{deg}\left(fg
ight)=\mathrm{deg}\left(f
ight)+\mathrm{deg}\left(g
ight) אזי f,g\in\mathbb{F}\left[x
ight] וכך שדה ויהיו
                                                                                                                                                                               \mathbb{F}[x]^{\times} = \mathbb{F} \setminus \{0\} טענה: יהי \mathbb{F} שדה אזי
                                                                                                           (f\sim g)\Longleftrightarrow (\exists c\in\mathbb{F}.f=cg) אזי f,g\in\mathbb{F}[x] אדה ויהיו שדה ויהיו
                                                                                                                                      \mathrm{.lc}\,(f)=1 המקיים f\in\mathbb{F}\left[x
ight] שדה אזי שדה המקיים f\in\mathbb{F}\left[x
ight]
                                                                                                    \mathbb{F}^{[x]}/\sim טענה: יהי \mathbb{F} שדה אזי \{f\in\mathbb{F}[x]\mid מתוקן f\}\cup\{0\} מערכת נציגים של
f=qg+r וכן \deg\left(r
ight)<\deg\left(r
ight)< שדה יהי f\in\mathbb{F}\left[x
ight] ויהי g\in\mathbb{F}\left[x
ight]\setminus\left\{ 0
ight\} איז קיימים ויחידים ויחידים q,r\in\mathbb{F}\left[x
ight] המקיימים q,r\in\mathbb{F}\left[x
ight] וכן
                                                       \mathbb{F}^{[x]}/f\mathbb{F}[x] מערכת נציגים של \{r\in\mathbb{F}\left[x
ight]\mid \deg\left(r
ight)<\deg\left(f
ight)\} אזי f\in\mathbb{F}\left[x
ight] מערכת נציגים של
      \mathbb{F}\left[x
ight] אוי F אוי 
                                                                                                                                                                      \mathbb{F}[x] מסקנה: יהי \mathbb{F} שדה אזי \mathbb{F}[x] תחום אוקלידי.
d\in\mathrm{Gcd}\,(f,g) באשר \gcd(f,g)=d כך \gcd:\mathbb{F}\left[x
ight]^2	o\mathbb{F}\left[x
ight] שדה אזי נגדיר שדה אזי נגדיר
                                                                                     \mathcal{D}\left(\sum_{i=0}^n\zeta_ix^i
ight)=\sum_{i=1}^ni\zeta_ix^{i-1} כך כך \mathcal{D}:\mathbb{F}[x]	o\mathbb{F}[x] שדה אזי נגדיר שדה \mathcal{E}
                                                                                                                                                           f' = D(f) אזי f \in \mathbb{F}[x] שדה ויהי
                                                                                                                                                           טענה: יהי \mathbb{F} שדה יהיו f,g\in\mathbb{F}\left[x
ight] ויהי שדה יהי
                                                                                                                                                         (f-g)' = f' - g' וכך (f+g)' = f' + g'
                                                                                                                                                                                                          .(fg)' = f'g + fg' \bullet
                                                                                                                                                                                                  (cf)' = cf' וכן c' = 0
                                                                                       p^2 
mid f מתקיים p \in \mathbb{P}_{\mathbb{F}[x]} עבורו לכל f \in \mathbb{F}[x] מתקיים \mathfrak{F} שדה אזי שדה איזי
                                                                  . טענה \gcd(f,f')=1 המקיים f\in\mathbb{F}[x] שזה f חסר ריבועים \gcd(f,f')=1
                                                                                                             השערה פתוחה השערה: \{\langle n \rangle \mid (n \in \mathbb{N}) \land (מספר מספר מספר מספר n)\} \in \mathcal{P}
                                                 כך \operatorname{mindef}: X \times \mathcal{P}\left(X\right) 	o X מינימום דיפולטי: תהא X קבוצה ויהי 	ou יחס סדר טוב על X אזי נגדיר
                                                                                                                                                                .mindef (x,\emptyset)=x מתקיים x\in X •
                                                                                                 .mindef (x, A) = \min(A) מתקיים A \in \mathcal{P}(X) \setminus \{\emptyset\} ולכל x \in X
                                                                                                \operatorname{char}\left(\mathbb{F}\right)=\operatorname{mindef}\left(0,\left\{n\in\mathbb{N}_{+}\mid n\cdot 1_{\mathbb{F}}=0\right\}\right) מציין של שדה: יהי \mathbb{F} שדה אזי
                                                                                                                                             \operatorname{char}\left(\mathbb{F}\right)\in\mathbb{P} אזי \operatorname{char}\left(\mathbb{F}\right)
eq0 שדה באשר \mathbb{F} יהי יהי
        arphiטענה: יהי arphi \in \mathbb{F} שדה באשר arphi = p ונגדיר arphi : \mathbb{Z}/p\mathbb{Z} 	o \mathbb{F} כך ונגדיר arphi : \mathbb{Z}/p\mathbb{Z} 	o \mathbb{F} מונומורפיזם שדות.
                                                                                                                                                                                             \mathbb{F}_p=\mathbb{Z}/p\mathbb{Z} אזי p\in\mathbb{P} סימון: יהי
                                                                          (n \mod p)\mapsto n\cdot 1_{\mathbb F} כך \mathbb F_p\hookrightarrow \mathbb F איי נשכן \operatorname{char}\left(\mathbb F\right)=p ויהי באשר p\in \mathbb P יהי יהי יהי
                                                                                                                                                                            \operatorname{char}\left(\mathbb{F}
ight)\in\mathbb{P} טענה: יהי \mathbb{F} שדה סופי אזי
                                                                                                                                                       \mathbb{F}_n טענה: יהי \mathbb{F} שדה סופי אזי \mathbb{F} מרחב וקטורי מעל
```

 $|\mathbb{Z}[i]/lpha\mathbb{Z}[i]|=N\left(lpha
ight)$ אזי $lpha\in\mathbb{Z}\left[i
ight]$ מסקנה: יהי

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

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

 $\mathbb{F}^{ imes}$ אזי $\mathbb{F}^{ imes}$ ציקלית.

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

 $\| \mathbb{Z}[\sqrt{d}]/_{lpha}\mathbb{Z}[\sqrt{d}] \| = |N\left(lpha
ight)|$ אזי $lpha \in \mathbb{Z}\left[\sqrt{d}
ight]$ ויהי $d
eq \square$ אזי $d \in \mathbb{Z}$ באשר $d \in \mathbb{Z}$

```
\mathbb{F}\simeq \mathbb{F}[x]/f\cdot\mathbb{F}[x] אזי \deg(f)=n יהי p\in\mathbb{P} יהי \mathbb{F}=p^n ויהי ויהי \mathbb{F}=p^n ויהי p\in\mathbb{F} יהי יהי
                                                                                      \mathbb{F} \simeq \mathbb{K} אזי |\mathbb{K}|=p^n וכן |\mathbb{F}|=p^n אזי שדות באשר n\in\mathbb{N}_+ יהי p\in\mathbb{P} יהי מסקנה: יהי
                                                                                                                                                  |\mathbb{F}_{p^n}|=p^n שדה המקיים \mathbb{F}_{p^n} אזי n\in\mathbb{N}_+ ויהי p\in\mathbb{P} יהי
                                                   \|\mathbb{F}_q[x]/f\cdot\mathbb{F}_q[x]\|=q^{\deg(f)} שדה וכן \|\mathbb{F}_q[x]/f\cdot\mathbb{F}_q[x]\| שדה ויהי \|\mathbb{F}_q[x]/f\cdot\mathbb{F}_q[x]\| שדה ויהי \|\mathbb{F}_q[x]/f\cdot\mathbb{F}_q[x]\|
                                                                                             |f|=q^{\deg(f)} כך כך |\cdot|:\mathbb{F}_q\left[x
ight]	o\mathbb{N} גודל של פולינום: יהי q\in\mathbb{N} באשר באשר אזי נגדיר
                                                                                                                             \mathbb{F}_{a}\left[x\right] שדה אוקלידית נורמה אוקלידית שדה \left|\cdot\right| שדה אזי q\in\mathbb{N}יהי יהי יהי מסקנה: יהי
                                                                                                                               |f|=|\mathbb{F}_q[x]/f\cdot\mathbb{F}_q[x]| אזי f\in\mathbb{F}_q[x] שדה ויהי \mathbb{F}_q שדה מסקנה:יהי q\in\mathbb{N}
                                                                                                                              |f\cdot g|=|f|\cdot |g| אזי f,g\in \mathbb{F}_q\left[x
ight] שדה ויהיו שדה g\in \mathbb{F}_q אזי g\in \mathbb{F}_q
                                                                                                     \mathbb{F}_q\left[x
ight] אזי חסר ריבועים מעל x^{q^n}-x אזי n\in\mathbb{N}_+ שדה יהי \mathbb{F}_q שדה יהי q\in\mathbb{N} יטענה: יהי
                                           \mathbb{F}_q\left[x
ight] שעל \gcd\left(x^{q^n}-x,x^{q^m}-x
ight)=x^{q^{\gcd(n,m)}}-x אזי n,m\in\mathbb{N}_+ שדה יהיו \mathbb{F}_q שדה יהיו q\in\mathbb{N} מעל
                                                    \operatorname{Fr}_p(a)=a^p כורפיזם פרובניום: יהי \mathbb{K}	o\mathbb{K} ויהי \mathbb{K} שדה המקיים \operatorname{char}(\mathbb{K})=p איי נגדיר p\in\mathbb{F} כורפיזם פרובניום: יהי
                                                                     \mathbb Kאוטומורפיזם של Fr_p אויהי p\in\mathbb P ויהי p\in\mathbb R אויה אוי הות פרובניוס: יהי ויהי p\in\mathbb R ויהי
                                                           g\left(x
ight)^{p^n}=g\left(x^{p^n}
ight) אזי n\in\mathbb{N}_+ ויהי f\in\mathbb{F}[x] יהי f\in\mathbb{F}[x] יהי באשר שדה באשר p\in\mathbb{P} אזי יהי p\in\mathbb{P}
                                          P(x^{q^n}-x) \iff (\deg(P)|n) איזי אזי P\in \mathbb{F}_q[x] ויהי ויהי n\in \mathbb{N}_+ שדה יהי \mathbb{F}_q שדה יהי n\in \mathbb{N}_+ ויהי
                                       \mathcal{P}_{q,n}=\{f\in\mathbb{F}_q\left[x
ight]\mid (\deg\left(f\right)=n)\wedge (יימון: יהי q\in\mathbb{N}_+ שדה ויהי n\in\mathbb{N}_+ אזי n\in\mathbb{N}_+ אזי q\in\mathbb{N} יהי q\in\mathbb{N} באשר מיטון: יהי
                                                                                                                 \pi_q\left(n
ight)=|\mathcal{P}_{q,n}| כך \pi_q:\mathbb{N}_+	o\mathbb{N} באשר \mathbb{F}_q שדה אזי נגדיר \pi_q:\mathbb{N}_+	o\mathbb{N} כך
                                                                              \mathbb{F}_q\left[x
ight] מעל x^{q^n}-x=\prod_{\substack{d\in\mathbb{N}\down}}\prod_{f\in\mathcal{P}_{q,d}}f אזי n\in\mathbb{N}_+ מעל שדה ויהי q\in\mathbb{N} מעל יהי q\in\mathbb{N}
                                                                                                                         q^n=\sum_{\substack{d\in\mathbb{N}\dln}}^{a\mid n}(d\cdot\pi_q\left(d
ight)) אזי n\in\mathbb{N}_+ שדה ויהי \mathbb{F}_q שדה ויהי q\in\mathbb{N}
                                                                         \pi_{q}\left(n
ight)=rac{1}{n}\left(q^{n}-\sum_{\substack{d\in\mathbb{N}_{< n}\d|n}}\left(d\cdot\pi_{q}\left(d
ight)
ight)
ight) אזי n\in\mathbb{N}_{+} אזי q\in\mathbb{N} באשר q\in\mathbb{N} באשר מסקנה: יהי
                                                                                              rac{q^n}{n}-rac{q}{q-1}\cdotrac{q\left\lfloorrac{n}{2}
ight
floor}{n}\leq\pi_q\left(n
ight)\leqrac{q^n}{n} אזי n\in\mathbb{N}_+ אזי q\in\mathbb{N} באשר q\in\mathbb{N} באשר q\in\mathbb{N} שדה אזי \pi_q\left(n
ight)\simrac{q^n}{n} שדה אזי \pi_q\left(n
ight)\simrac{q^n}{n} שדה אזי \pi_q\left(n
ight)
                                                                                                                                                   \pi_q\left(n
ight)>0 אזי n\in\mathbb{N}_+ שדה ויהי \mathbb{F}_q שדה q\in\mathbb{N} אזי מסקנה: יהי
\mu\left(\prod_{i=1}^k p_i^{e_i}
ight) = \left\{egin{array}{ll} (-1)^k & e=1 \ 0 & 	ext{else} \end{array}
ight. בונקציית מוביוס: יהי k\in\mathbb{N} יהיי k\in\mathbb{N} יהיי שונים ויהי p_1\dots p_k\in\mathbb{N} שונים ויהי
                                                                                                                                                                                        \sum_{\substack{d\in\mathbb{N}\d|n}}\mu\left(d
ight)=\{egin{array}{ccc} 1&n=1\0&n>1 \end{array} אזי n\in\mathbb{N}_+ יהי
                                   f(n)=\sum_{\substack{d\in\mathbb{N}\\d\mid n}}\left(\mu\left(d
ight)\cdot\left(\sum_{\substack{a\in\mathbb{N}\\a\midrac{n}{d}}}f\left(a
ight)
ight)
ight) אזי n\in\mathbb{N}_{+} אזי f:\mathbb{N}_{+}	o\mathbb{C} אחלי מוביוס: תהא
                                                                                                       .\pi_q^{'a}(n)=\stackrel{`}{1}_n\stackrel{`}{\sum}_{\substack{d\in\mathbb{N}\\d|n}}\left(\mu\left(rac{n}{d}
ight)\cdot q^d
ight) אזי n\in\mathbb{N}_+ שדה ויהי p_q שדה ויהי q\in\mathbb{N}
לכל (f)=n אזי (f)=f ווכן אזי (f)=n וויהי וויהי (f)=n אזי וויהי וויהי וויהי וויהי (f)=n אזי וויהי וויהי
                                                                                                                                                                                                        .(gcd \left(f,x^{q^\ell}-x\right)=1 מתקיים \ell\in\mathbb{N}_{< n}
אלגוריתם מבחן ראשוניות לפולינום: היי q\in\mathbb{N} באשר q\in\mathbb{N} יהי לפולינום: היי לפולינום: אלגוריתם מבחן באשר q\in\mathbb{N} יהי לפולינום: אלגוריתם מבחן ראשוניות לפולינום: אלגוריתם מבחן ראשוניות לפולינום:
                                                                                                                                                             אזי \mathbb{F}_q\left[x
ight] מעל \gcd ויהי \mathcal{B} אלגוריתם \gcd אלגוריתם ויהי \mathbb{F}_q\left[x
ight]/f\cdot\mathbb{F}_q\left[n
ight]
Algorithm PolynomialPrimality [A, B] (q, n, f):
         L \in (\mathbb{F}_q[x]/f \cdot \mathbb{F}_q[x])^n;
                                                                   L_1 \leftarrow (x^q \mod f)
         for i \in [2, \ldots, n] do
                   L_i \leftarrow \mathcal{A}\left(f, L_{i-1}, q\right)
          if L_n \neq (x \mod f) then return False
         for d \in [1, ..., n-1] do
             if \mathcal{B}(L_d - x, f) \neq 1 then return False
          end
```

 \iff אזי $\deg(f)=n$ באשר $f\in\mathbb{F}_q[x]$ אויהי $n\in\mathbb{N}_+$ שדה יהי $f\in\mathbb{F}_q[x]$ אזי $g\in\mathbb{N}$ באשר רביט באשר $g\in\mathbb{N}$ באשר (Polynomial Primality g(q,n,f)= True)

return True

```
\mathcal{O}\left(\left(n\cdot\log\left(q\right)\right)^3\right) הינה PolynomialPrimality [IteratedSquaring [NaiveMul] , EuclidGCD] אענה: סיבוכיות הריצה של
                         סענה: סיבוכיות הריצה של PolynomialPrimality [IteratedSquaring [CooleyTukeyMul] , FastGCD] סענה: סיבוכיות הריצה של
                                                                                                                                              \tilde{\mathcal{O}}\left(\left(n \cdot \log\left(q\right)\right)^2\right)
                                                   (g'=0)\Longleftrightarrow (\exists h\in\mathbb{F}_{p^r}\left[x
ight].g=h^p) אזי g\in\mathbb{F}_{p^r}\left[x
ight] ויהי r\in\mathbb{N}_+ יהי p\in\mathbb{P} יהי יהי
                              אזי \mathbb{F}_{p^r} אזי חזקה חזקה אלגוריתם שורש מעל שדה סופי: יהי p\in\mathbb{P}_+ יהי יהי p\in\mathbb{P}_+ אזי אלגוריתם שורש מעל א
                                                                                                           .FiniteFieldRoot [A](p,r,a) = A(a,p^{r-1})
                                                             .
FiniteFieldRoot (p,r,a)=\sqrt[p]{a} אזי a\in\mathbb{F}_{p^r} יהי r\in\mathbb{N}_+ יהי p\in\mathbb{P} יהי יהי
.
FiniteFieldPolynomialRoot [$\mathcal{A}$] (p,r,a) = \sum_{i=0}^{\frac{n}{p}} \text{FiniteFieldRoot} \left[\mathcal{A}\right] (a_{pi}) \, x^i חזקה מעל \mathbb{F}_{p^r} אזי
                                       .
FiniteFieldPolynomialRoot (p,r,f)=\sqrt[p]{f} אזי f\in\mathbb{F}_{p^r}[x] יהי r\in\mathbb{N}_+ יהי p\in\mathbb{P} יהי יהי p\in\mathbb{P}
                                                . (מסר ריבועים) אזי (\gcd(f,f')=1) אזי f\in \mathbb{F}_q\left[x
ight] שדה ויהי שדה f\in \mathbb{F}_q\left[x
ight] שדה ויהי
אלגוריתם \gcd יהי f\in \mathbb{F}_{p^r}[x] יהי f\in \mathbb{F}_{p^r}[x] יהי יהי f\in \mathbb{F}_{p^r}[x] יהי יהי ויהי מעל מעל p\in \mathbb{P} מעל
                                                                                                                              אזי \mathbb{F}_{p^r} אזי אלגוריתם חזקה מעל
Algorithm PolyFactorNoSquare [A, B] (p, r, f):
     G \leftarrow \mathcal{A}\left(f, f'\right)
     if G = 1 then return \{(f, 1)\}
     if f' \neq 0 then
          A \leftarrow \texttt{PolyFactorNoSquare}[\mathcal{A}, \mathcal{B}] (p, r, G)
          B \leftarrow \texttt{PolyFactorNoSquare}\left[\mathcal{A}, \mathcal{B}\right]\left(p, r, \frac{f}{C}\right)
          return A + B
     g \leftarrow \text{FiniteFieldPolynomialRoot} [\mathcal{B}] (p, r, f)
     S \leftarrow \texttt{PolyFactorNoSquare}[\mathcal{A}, \mathcal{B}](p, r, g)
     return \{(q, n + p) \mid (q, n) \in S\}
                                                                                                      טענה: יהי f \in \mathbb{F}_{p^r}\left[x
ight] ויהי r \in \mathbb{N}_+ אזי p \in \mathbb{P} אזי
                                                                                                           . \prod PolyFactorNoSquare (p, r, f) = f \bullet
                                                                          . מתקיים q \in \operatorname{PolyFactorNoSquare}(p, r, f) לכל
f\in\mathbb{F}_{p^r}[x] אלגוריתם פירוק פולינום חסר ריבועים לפולינומים בעלי פירוק לראשוניים בעלי אותה דרגה: יהי p\in\mathbb{P} יהי יהי
                                                    אזי \mathbb{F}_{p^r}[x] אזי חזקה חזקה אלגוריתם \mathcal{B} ויהי \mathcal{B} ויהי אלגוריתם \gcd אלגוריתם מעל
Algorithm PolyFactorSameDeg [\mathcal{A}, \mathcal{B}] (p, r, f):
     S \leftarrow \varnothing
     for d \in [1, \ldots, \deg(f)] do
         f_d \leftarrow \mathcal{A}\left(\mathcal{B}\left(x, q^d\right) - x, f\right)
if f_d \neq 1 then S \leftarrow S \cup \{f_d\}
```

.power $(r,n)=r^n$ כך power : $R imes\mathbb{N} o R$ פונקציית חזקה: נגדיר

.(\prod power (PolyFactorSameDeg (p,r,f))) | f

טענה: יהי $p\in\mathbb{F}_{p^r}\left[x
ight]$ ויהי ויהי $p\in\mathbb{F}_{p^r}\left[x
ight]$ יהי יהי יהי

return S

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

$$.\mathbb{F}_{q}\left[x\right] \text{ אמ } x^{q^{d}}-x=\left(\left(x+a\right)^{\frac{q^{d}-1}{2}}-1\right)\left(\left(x+a\right)^{\frac{q^{d}-1}{2}}+1\right)\left(x+a\right) \text{ (} x+a) \text{ (} x+a) + 2 \nmid q \text{ (} a \mid x+a) + 2 \mid q \text{ (} a \mid x+a) \mid x+a \mid$$

למה: יהי $P=\prod_{i=1}^d\left(x-a^{q^i}
ight)$ עדה יהי $P\in\mathbb{F}_{q^d}\left[x
ight]$ ונגדיר $f\left(a
ight)=0$ באשר $a\in\mathbb{F}_{q^d}$ יהי $d\in\mathbb{N}_+$ יהי $d\in\mathbb{N}_+$ שזי $P\in\mathbb{F}_q\left[x
ight]$ וכן $P\in\mathbb{F}_q\left[x
ight]$ וכן $P\in\mathbb{F}_q\left[x
ight]$

חסר $f\in\mathbb{F}_{p^r}\left[x
ight]$ יהי $p\in\mathbb{P}_+$ יהי יהי $p\in\mathbb{P}$ יהי אלגוריתם פירוק פירוק בעל פירוק בעל פירוק לראשוניים בעל אותה אווי יהי $q\in\mathbb{F}_{p^r}\left[x
ight]$ יהי רבועים עבורו לכל $Q\in\mathbb{F}_{p^r}\left[x
ight]$ מתקיים Q מתקיים עבורו לכל עבורו לכל ראשוני המקיים בעל פירוק מתקיים ולכל וויים עבורו לכל ראשוני המקיים וויים אוויים בעל מתקיים וויים עבורו לכל ראשוני המקיים וויים וויים בעל מתקיים וויים בעל פירוק מתקיים וויים בעל פירוק מתקיים וויים בעל פירוק מתקיים וויים בעל פירוק וויים בעל פירוק פירוק

•••