

**פעולה בינארית:** תהא  $A$  קבוצה אזי  $*$  :  $A \times A \rightarrow A$

**סימון:** תהא  $*$  פעולה בינארית אזי  $a * b = *(\langle a, b \rangle)$

**חבורה:** תהא  $G$  קבוצה ותהא  $*$  פעולה בינארית אזי  $\langle G, * \rangle$  המקיימת

• אסוציאטיביות/קיבוציות:  $\forall a, b, c \in A. a * (b * c) = (a * b) * c$

• איבר יחידה:  $\exists e \in A. \forall g \in G. e * g = g * e = g$

• איבר הופכי/נגדי:  $\forall g \in G. \exists h \in A. g * h = h * g = e_G$

**סימון:** תהא  $G$  חבורה אזי איבר היחידה של  $G$  הינו  $e_G$

**סימון:** תהא  $G$  חבורה ויהי  $a \in G$  אזי האיבר ההופכי של  $a$  הינו  $a^{-1}$

**חוג:** תהא  $R$  קבוצה ויהיו  $+$ ,  $*$  :  $R^2 \rightarrow R$  אזי  $\langle R, *, + \rangle$  המקיימת

•  $\langle R, + \rangle$  חבורה אבלית.

• אסוציאטיביות/קיבוציות:  $a * (b * c) = (a * b) * c$

• איבר יחידה לכפל:  $\exists e_* \in R. \forall g \in R. e_* * g = g * e_* = g$

• חוק הפילוג:  $((b + c) * a = b * a + c * a) \wedge (a * (b + c) = a * b + a * c)$

**שדה:** תהא  $\mathbb{F}$  קבוצה ויהיו  $+$ ,  $*$  :  $\mathbb{F}^2 \rightarrow \mathbb{F}$  אזי  $\langle \mathbb{F}, +, * \rangle$  המקיים

•  $\langle \mathbb{F}, +, * \rangle$  חוג.

•  $\langle \mathbb{F} \setminus \{e_*\}, * \rangle$  חבורה אבלית.

•  $e_+ \neq e_*$

**חזקה מושלמת:**  $n \in \mathbb{N}$  עבורו קיימים  $a \in \mathbb{N}_+$  וכן  $b \in \mathbb{N}_{>1}$  המקיימים  $n = a^b$

**מקדם בינומי:** יהיו  $k, n \in \mathbb{N}$  כאשר  $k \leq n$  אזי  $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

**סימון:** יהיו  $k, n \in \mathbb{N}$  אזי  $S_n^{(k)} = \sum_{i=1}^n i^k$

**טענה:**  $S_n^{(2)} = \frac{n(n+1)(2n+1)}{6}, S_n^{(1)} = \frac{n(n+1)}{2}, S_n^{(0)} = n$

**הבינום של ניוטון:** יהיו  $x, y \in \mathbb{R}$  וכן  $n \in \mathbb{N}$  אזי  $(x + y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$

**טענה:**  $S_n^{(k)} = \frac{1}{k+1} \left( n^{k+1} - \sum_{t=0}^{k-1} (-1)^{k-t} \binom{k+1}{t} S_n^{(t)} \right)$

**מסקנה:**  $S_n^{(3)} = \frac{n^4 + 2n^3 + n^2}{4}$

**חוג חלקי ל- $\mathbb{C}$ :** קבוצה  $A \subseteq \mathbb{C}$  המקיימת

•  $\langle A, + \rangle$  חבורה.

• סגירות לכפל:  $\forall a, b \in A. ab \in A$

•  $1 \in A$

**טענה:** יהי  $A$  חוג חלקי ל- $\mathbb{C}$  אזי  $A$  חוג.

**טענה:**  $\mathbb{Z}$  חוג חלקי ל- $\mathbb{C}$ .

**הגדרה:**  $\mathbb{Z}[\alpha] = \bigcup_{n=0}^{\infty} \{ \sum_{i=0}^n k_i \alpha^i \mid k \in \mathbb{Z}^n \}$

**טענה:** יהי  $m \in \mathbb{Z}$  עבורו  $\sqrt{m} \notin \mathbb{Q}$  אזי  $\{1, \sqrt{m}\}$  בת"ל מעל  $\mathbb{Q}$ .

**טענה:** יהי  $m \in \mathbb{Z}$  עבורו  $\sqrt{m} \notin \mathbb{Q}$  אזי  $\mathbb{Z}[\sqrt{m}]$  חוג חלקי ל- $\mathbb{C}$ .

**חוג השלמים של גאוס:**  $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$

**מסקנה:**  $\mathbb{Z}[i]$  חוג חלקי ל- $\mathbb{C}$ .

**חבורת ההפיכים:** יהי  $A$  חוג חלקי ל- $\mathbb{C}$  אזי  $A^* = \{a \in A \mid \exists b \in A. ab = 1\}$

**טענה:** יהי  $A$  חוג חלקי ל- $\mathbb{C}$  אזי  $\langle A^*, * \rangle$  חבורה.

**מחלק**: יהי  $A$  חוג חלקי ל- $\mathbb{C}$  ויהי  $b \in A$  אזי  $a \in A \setminus \{0\}$  המקיים  $\frac{b}{a} \in A$ .

**סימון**: יהי  $b \in A$  ויהי  $a \in A \setminus \{0\}$  מחלק אזי  $a \mid b$ .

**טענה**: יהיו  $a, b, c \in A$  עבורם  $a \mid b$  וכן  $b \mid c$  אזי  $a \mid c$ .

**טענה**: יהיו  $a, b, c \in A$  עבורם  $a \mid b$  וכן  $a \mid c$  אזי  $a \mid ub + vc$   $\forall u, v \in A$ .

**יחס חברות**:  $\sim$  יחס על  $A$  המקיים  $(\exists \varepsilon \in A^*. b = \varepsilon a) \iff (a \sim b)$ .

**טענה**: יחס החברות הינו יחס שקילות.

**טענה**: יהיו  $a, b \in A$  אזי  $(a \mid b) \wedge (b \mid a) \iff ((a \mid b) \wedge (b \mid a))$ .

**טענה**: יהי  $m \in \mathbb{Z}$  אזי חבריו של  $m$  הם  $\pm m$ .

**טענה**: יהי  $z \in \mathbb{Z}[i]$  אזי חבריו של  $z$  הם  $\{\pm z, \pm iz\}$ .

**אי פריק (א"פ)**:  $a \in A \setminus A^*$  המקיים  $(a = bc) \implies (b \in A^*) \vee (c \in A^*)$   $\forall b, c \in A$ .

**ראשוני**:  $a \in A \setminus (A^* \cup \{0\})$  המקיים  $(a \mid bc) \implies (a \mid b) \vee (a \mid c)$   $\forall b, c \in A$ .

**טענה**: יהי  $a \in A$  ראשוני אזי  $a$  "פ".

**טענה**: בחוג  $\mathbb{Z}[\sqrt{-5}]$  מתקיים כי 2 "פ" אך אינו ראשוני.

**תחום פריקות**:  $A$  חוג חלקי של  $\mathbb{C}$  המקיים לכל  $a \in A \setminus (A^* \cup \{0\})$  קיימים  $q_1 \dots q_n \in A$  "פ" המקיימים  $a = \prod_{i=1}^n q_i$ .

**משפט פירוק לאי פריקים מעל  $\mathbb{Z}$** : תחום פריקות.

**פונקציית הצמוד**: יהי  $\alpha \in \mathbb{Z}$  עבורו  $\sqrt{\alpha} \notin \mathbb{Q}$  נגדיר  $\sigma : \mathbb{Z}[\sqrt{\alpha}] \rightarrow \mathbb{Z}[\sqrt{\alpha}]$  כך  $\sigma(a + b\sqrt{\alpha}) = a - b\sqrt{\alpha}$ .

**טענה**: יהיו  $z, w \in \mathbb{Z}[\sqrt{\alpha}]$  מתקיים

- $\sigma(z + w) = \sigma(z) + \sigma(w)$
- $\sigma(zw) = \sigma(z)\sigma(w)$
- $\sigma(\sigma(z)) = z$
- $\sigma$  חח"ע ועל.

**נורמה**: יהי  $\alpha \in \mathbb{Z}$  עבורו  $\sqrt{\alpha} \notin \mathbb{Q}$  נגדיר  $N : \mathbb{Z}[\sqrt{\alpha}] \rightarrow \mathbb{Z}$  כך  $N(z) = z\sigma(z)$ .

**למה**: יהיו  $z, w \in \mathbb{Z}[\sqrt{\alpha}]$  מתקיים

- $N(zw) = N(z)N(w)$
- $(N(z) = 0) \iff (z = 0)$

**טענה**: יהי  $\alpha \in \mathbb{Z}$  עבורו  $\sqrt{\alpha} \notin \mathbb{Q}$  אזי  $\mathbb{Z}[\sqrt{\alpha}]^* = \{z \in \mathbb{Z}[\sqrt{\alpha}] \mid N(z) \in \{\pm 1\}\}$ .

**משפט פירוק לאי פריקים מעל  $\mathbb{Z}[\sqrt{\alpha}]$** : יהי  $\alpha \in \mathbb{Z}$  עבורו  $\sqrt{\alpha} \notin \mathbb{Q}$  אזי  $\mathbb{Z}[\sqrt{\alpha}]$  תחום פריקות.

**תחום פריקות יחידה**:  $A$  תחום פריקות המקיים לכל  $a \in A \setminus (A^* \cup \{0\})$  קיימים  $q_1 \dots q_n \in A$  "פ" יחידים המקיימים  $a = \prod_{i=1}^n q_i$  עד כדי שינוי סדר הגורמים וחברות.

**משפט**: יהי  $A$  תחום פריקות אזי  $(A$  תחום פריקות יחידה)  $\iff$  (כל  $a \in A$  "פ" הינו ראשוני).

**מסקנה**:  $\mathbb{Z}[\sqrt{-5}]$  אינו תחום פריקות יחידה.

**משפט חלוקה עם שארית ב- $\mathbb{Z}$** : יהיו  $a, b \in \mathbb{Z}$  באשר  $a > 0$  אזי קיימים ויחידים  $q, r \in \mathbb{Z}$  באשר  $0 \leq r < a$  המקיימים  $b = qa + r$ .

**שארית חלוקה**: יהיו  $a, b \in \mathbb{Z}$  באשר  $a > 0$  ויהיו  $q, r \in \mathbb{Z}$  באשר  $0 \leq r < a$  המקיימים  $b = qa + r$  אזי  $r$  שארית החלוקה של  $b$  ב- $a$   $a \bmod b = r$ .

**סימון**: יהיו  $a, b \in \mathbb{Z}$  ויהי  $r \in \mathbb{Z}$  שארית החלוקה של  $b$  ב- $a$  אזי  $a \bmod b = r$ .

**טענה**: יהיו  $a, b \in \mathbb{Z}$  באשר  $a > 0$  אזי (שארית החלוקה של  $b$  ב- $a$  היא 0)  $\iff (a \mid b)$ .

**מחלק משותף**: יהיו  $a, b \in \mathbb{Z}$  באשר  $(a, b) \neq 0$  אזי  $d \in \mathbb{Z}$  המקיים  $(d \mid a) \wedge (d \mid b)$ .

**מחלק משותף מקסימלי (ממ"מ):** יהיו  $a, b \in \mathbb{Z}$  באשר  $(a, b) \neq 0$  אזי  $\max \{d \in \mathbb{Z} \mid (d \mid a) \wedge (d \mid b)\}$ .

**סימון:** יהיו  $a, b \in \mathbb{Z}$  אזי המחלק המשותף המקסימלי שלהם  $\gcd(a, b)$ .

**משפט:** יהיו  $a, b \in \mathbb{Z}$  אזי  $\gcd(a, b) = ma + nb$   $\exists m, n \in \mathbb{Z}$ .

**מסקנה:** יהיו  $a, b \in \mathbb{Z}$  ויהי  $d \in \mathbb{Z}$  מחלק משותף אזי  $d \mid \gcd(a, b)$ .

**טענה:** יהיו  $a, b \in \mathbb{Z}$  ויהי  $d \in \mathbb{Z}$  מחלק משותף אזי (לכל מחלק משותף  $r \in \mathbb{Z}$  מתקיים  $(r \mid d) \iff (d = \gcd(a, b))$ ).

**מחלק משותף מקסימלי (ממ"מ):** יהיו  $a_1 \dots a_n \in \mathbb{Z}$  באשר  $(a_1 \dots a_n) \neq 0$  אזי  $\max \{d \in \mathbb{Z} \mid \forall i \in [n]. (d \mid a_i)\}$ .

**סימון:** יהיו  $a_1 \dots a_n \in \mathbb{Z}$  אזי המחלק המשותף המקסימלי שלהם  $\gcd(a_1 \dots a_n)$ .

**משפט:** יהיו  $a_1 \dots a_n \in \mathbb{Z}$  אזי  $\gcd(a_1 \dots a_n) = \sum_{i=1}^n u_i a_i$   $\exists u_1 \dots u_n \in \mathbb{Z}$ .

**אלגוריתם אוקלידס:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  ויהי  $b \in \mathbb{N}$  אזי

**function** EuclideanAlgorithm ( $a, b$ )

```

| if  $b = 0$ 
|   return  $a$ 
| else
|   return EuclideanAlgorithm ( $b, a \bmod b$ )

```

**משפט:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  ויהי  $b \in \mathbb{N}$  אזי  $\text{EuclideanAlgorithm}(a, b) = \gcd(a, b)$ .

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

**מסקנה:** יהיו  $a, b \in \mathbb{Z}$  זרים אזי  $ma + nb = 1$   $\exists m, n \in \mathbb{Z}$ .

**משפט:** יהי  $a \in \mathbb{Z}$  "א"פ אזי ראשוני.

**המשפט היסודי של האריתמטיקה:**  $\mathbb{Z}$  תחום פריקות יחידה.

**משפט אוקלידס:** קיימים אינסוף ראשוניים ב- $\mathbb{Z}$ .

**טענה:** בסדרה  $\{4n + 3\}_{n=0}^{\infty}$  ישנם אינסוף ראשוניים.

**משפט דיריכלה:** יהיו  $a, b \in \mathbb{N}_+$  זרים אזי בסדרה  $\{bn + a\}_{n=0}^{\infty}$  ישנם אינסוף ראשוניים.

**טענה:** תהא  $\{p_n\}_{n=1}^{\infty}$  סדרת הראשוניים אזי  $p_n \leq 2^{2^n}$ .

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

**השערת התאומים הראשוניים:** קיימים אינסוף  $p \in \mathbb{P}$  עבורם  $p + 2 \in \mathbb{P}$ . השערה פתוחה

**פונקציית ספירת ראשוניים:**  $\pi(x) = |\{p \in \mathbb{P} \mid p \leq x\}|$ .

**אלגוריתם הנפה של ארטוסטנס :** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  אזי

**function** SieveOfEratosthenesAlgorithm ( $n$ )

```
|  $A \leftarrow [\text{true}, \text{true}, \dots, \text{true}]$ 
| for  $i \leftarrow 2 \dots n$ 
|   | if  $A[i] = \text{true}$ 
|   |   |  $j \leftarrow 1$ 
|   |   | while  $ij \leq n$ 
|   |   |   |  $A[ij] = \text{false}$ 
|   |   |   |  $j \leftarrow j + 1$ 
| return  $A$ 
```

**משפט :** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  אזי כל אינדקס שמסומן כ-true בתשובת SieveOfEratosthenesAlgorithm ( $n$ ) הינו ראשוני.

**טענה :**  $\pi(x) > \log \log(x)$

**סימון :** יהיו  $f, g \in \mathbb{R} \rightarrow \mathbb{N}$  המקיימות  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$  אזי  $f \sim g$

**משפט :**  $\pi(x) \sim \frac{x}{\log(x)}$

**למה :** יהי  $x \in \mathbb{R}$  אזי  $[2x] - 2[x] \in \{0, 1\}$

**למה :** יהי  $p \in \mathbb{P}$  ויהי  $n, r \in \mathbb{N}_+$  עבורם  $p^r \leq n < p^{r+1}$  אזי  $\sum_{i=1}^r \left\lfloor \frac{n}{p^i} \right\rfloor = \max \{m \in \mathbb{N} \mid (p^m \mid n!)\}$

**משפט צ'בישב :**  $\exists a \in (0, 1). \exists b \in (1, \infty). \forall x \geq 2. \left( a \frac{x}{\log(x)} < \pi(x) < b \frac{x}{\log(x)} \right)$

**מסקנה :**  $\exists \alpha, \beta > 0. \forall n \in \mathbb{N} \setminus \{0, 1\}. (\alpha n \log(n) < p_n < \beta n \log(n))$

**משפט השערת ברטרנד :** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  אזי  $n < p < 2n$

**הגדרה :** נגדיר  $\text{Li} : \mathbb{R} \rightarrow \mathbb{R}$  כך  $\text{Li}(x) = \int_2^x \frac{1}{\log(t)} dt$

**טענה :**  $\text{Li}(x) \sim \frac{x}{\log(x)}$

**מסקנה :**  $\text{Li}(x) \sim \pi(x)$

**פונקציית זטא של רימן :** נגדיר  $\zeta : \mathbb{R} \rightarrow \mathbb{R}$  כך  $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$

**השערת רימן :**  $\forall \beta > \frac{1}{2}. \exists x_0 \in \mathbb{R}_+. \forall x \geq x_0. |\pi(x) - \text{Li}(x)| \leq x^\beta$  השערה פתוחה

**משפט :** (השערת רימן נכונה)  $\iff \left( \text{sols}_{\mathbb{C}}(\zeta(s) = 0) \setminus \{-2n \mid n \in \mathbb{N}_+\} \subseteq \left\{ z \in \mathbb{C} \mid \text{Re}(z) = \frac{1}{2} \right\} \right)$

**מספרי פרמה :** יהי  $n \in \mathbb{N}$  אזי  $F_n = 2^{2^n} + 1$

**טענה :** יהיו  $x, y \in \mathbb{R}$  ויהי  $t \in \mathbb{N}_+$  אזי  $x^t - y^t = (x - y) \sum_{i=0}^{t-1} x^i y^{t-i-1}$

**טענה :** יהיו  $m, n \in \mathbb{N}$  באשר  $m \neq n$  אזי  $\gcd(F_n, F_m) = 1$

**מספרי מרסן :** יהי  $p \in \mathbb{P}$  אזי  $M_p = 2^p - 1$

**מספר מושלם :**  $n \in \mathbb{N}_+$  המקיים  $\sum_{\substack{d|n \\ d < n}} d = n$

**פונקציית סכום המחלקים :** יהי  $n \in \mathbb{N}_+$  אזי  $\sigma(n) = \sum_{d|n} d$

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $(n \text{ מושלם}) \iff (\sigma(n) = 2n)$ .

**פונקציה כפלית:**  $f: \mathbb{N} \rightarrow \mathbb{C}$  המקיימת לכל  $n, m \in \mathbb{N}$  זרים מתקיים  $f(nm) = f(n)f(m)$ .

**טענה:** תהא  $f$  פונקציה כפלית ויהי  $n \in \mathbb{N}$  עם פירוק לראשוניים  $n = \prod_{m=1}^k p_m^{r_m}$  אזי  $f(n) = \prod_{i=1}^k f(p_i^{r_i})$ .

**טענה:**  $\sigma$  פונקציה כפלית.

**טענה:** יהי  $p \in \mathbb{P}$  ויהי  $n \in \mathbb{N}$  אזי  $\sigma(p^n) = \frac{p^{n+1}-1}{p-1}$ .

**מסקנה:** יהי  $n \in \mathbb{N}$  עם פירוק לראשוניים  $n = \prod_{m=1}^k p_m^{r_m}$  אזי  $\sigma(n) = \prod_{m=1}^k \frac{p_m^{r_m+1}-1}{p_m-1}$ .

**טענה:** תהא  $f$  פונקציה כפלית אזי  $F(n) = \sum_{d|n} f(d)$  כפלית.

**פונקציית מביוס:** נגדיר  $\mu: \mathbb{N} \rightarrow \{0, \pm 1\}$  כפלית יהי  $p \in \mathbb{P}$  ויהי  $r \in \mathbb{N}_+$  אזי  $\mu(p^r) = \begin{cases} 1 & r=0 \\ -1 & r=1 \\ 0 & r \geq 2 \end{cases}$

**משפט נוסחת ההיפוך של מביוס:** תהא  $f: \mathbb{N} \rightarrow \mathbb{C}$  אזי  $\left( f(n) = \sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) \right) \iff \left( F(n) = \sum_{d|n} f(d) \right)$ .

**משפט אוקלידס:** יהי  $M_p \in \mathbb{P}$  אזי  $\frac{1}{2}M_p(M_p+1)$  מושלם.

**משפט אוילר:** יהי  $n \in \mathbb{N}_{\text{even}}$  מושלם אזי  $(n = \frac{1}{2}M_k(M_k+1)) \wedge (M_k \in \mathbb{P}) \iff \exists k \in \mathbb{N}$ .

**שלשה פיתגורית:**  $x, y, z \in \mathbb{N}_+$  המקיימים  $x^2 + y^2 = z^2$ .

**אלגוריתם מציאת כל הנקודות הרציונליות על חתך חרוט:** יהיו  $r, s \in \mathbb{Q}$  ותהא עקומה  $rx^2 + sy^2 = 1$ .

1. מצא פתרון רציונלי  $(a, b)$ .

2. מצאו את נקודות החיתוך בין הישר העובר דרך  $(0, t)$ ,  $(a, b)$  ובין העקומה.

$$\bullet \text{ פתור את מערכת המשוואות } \begin{cases} (t-b)x + a(y-t) = 0 \\ rx^2 + sy^2 = 1 \end{cases}$$

3. החזר את כל פתרונות החיתוך עבור  $t \in \mathbb{Q}$ .

**טענה:** יהיו  $r, s \in \mathbb{Q}$  אזי (אלגוריתם מציאת כל הנקודות הרציונליות על חתך חרוט)  $\text{sols}_{\mathbb{Q}}(rx^2 + sy^2 = 1) =$

**משפט:** יהי  $t \in \mathbb{R}$  אזי  $t \in \mathbb{Q} \iff \left( \left( \frac{t^2-1}{t^2+1} \in \mathbb{Q} \right) \wedge \left( \frac{2t}{t^2+1} \in \mathbb{Q} \right) \right)$ .

**משפט:**  $f: \mathbb{Q} \rightarrow \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\} \setminus \{(1, 0)\}$  המוגדרת  $f(t) = \left( \frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1} \right)$  הינה חח"ע ועל.

**משפט:**  $\text{sols}_{\mathbb{Q}}(x^2 + y^2 = 1) = \{(1, 0)\} \cup \left\{ \left( \frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1} \right) \mid t \in \mathbb{Q} \right\}$ .

**מסקנה:** תהא  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{N}_+^3$  שלשה פתגורית אזי מתקיים אחד מהבאים

$\bullet$  קיימים  $u, v \in \mathbb{N}_{\text{odd}}$  המקיימים  $\gcd(u, v) = 1$  עבורם  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} u^2-v^2 \\ 2uv \\ u^2+v^2 \end{pmatrix}$ .

$\bullet$  קיימים  $u, v \in \mathbb{N}_+$  המקיימים  $\gcd(u, v) = 1$  וכן  $u+v \in \mathbb{N}_{\text{odd}}$  עבורם  $\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} u^2-v^2 \\ 2uv \\ u^2+v^2 \end{pmatrix}$ .

**מספרים קונגרואנטים:** יהי  $n \in \mathbb{N}_+$  אזי  $a, b \in \mathbb{Z}$  המקיימים  $a \equiv b \pmod{n}$ .

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

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי יחס הקונגרואציה מודולו  $n$  הינו יחס שקילות על  $\mathbb{Z}$ .

**סימון:**  $a + n\mathbb{Z} = \{a + n \cdot m \mid m \in \mathbb{Z}\}$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $[a]_{\text{mod } n} = a + n\mathbb{Z}$ .

**מסקנה:**  $\mathbb{Z}/\text{mod } n = \{a + n\mathbb{Z} \mid a \in \{0 \dots n-1\}\}$ .

**סימון:**  $\mathbb{Z}_n = \mathbb{Z}/\text{mod } n$ .

**טענה:** יהי  $n \in \mathbb{N}_+$  ויהיו  $a, a', b, b' \in \mathbb{Z}$  המקיימים  $a \equiv a' \pmod n$  וכן  $b \equiv b' \pmod n$

$$\bullet a + b \equiv a' + b' \pmod n$$

$$\bullet ab \equiv a'b' \pmod n$$

**מסקנה:** יהי  $f \in \mathbb{Z}[x]$  ויהיו  $b, c \in \mathbb{Z}$  המקיימים  $b \equiv c \pmod n$  אזי  $f(b) \equiv f(c) \pmod n$

**משפט סימן החלוקה:** יהי  $n \in \mathbb{Z}$  מתקיים

$$\bullet \text{ סימן חלוקה ב-2: } (2 \mid n) \iff (\text{ספרת האחדות של } n \text{ היא זוגית})$$

$$\bullet \text{ סימן חלוקה ב-5: } (5 \mid n) \iff (\{0, 5\} \text{ היא } n \text{ של } \{0, 5\})$$

$$\bullet \text{ סימן חלוקה ב-10: } (10 \mid n) \iff (0 \text{ היא } n \text{ של } \{0, 10\})$$

$$\bullet \text{ סימן חלוקה ב-3: } (3 \mid n) \iff (3 \text{ סכום הספרות של } n \text{ מתחלק ב-3})$$

**אריתמטיקה של מחלקות קונגרוואציה:** יהי  $n \in \mathbb{N}_+$  ויהיו  $(a + n\mathbb{Z}), (b + n\mathbb{Z}) \in \mathbb{Z}_n$  אזי

$$\bullet \text{ חיבור: } (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

$$\bullet \text{ כפל: } (a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = ab + n\mathbb{Z}$$

**טענה:**  $\mathbb{Z}_n$  חוג עם אריתמטיקה של מחלקות קונגרוואציה.

**איבר הפיך ב- $\mathbb{Z}_n$ :**  $a \in \mathbb{Z}_n$  המקיים  $\exists b \in \mathbb{Z}_n. a \cdot b = 1$

**איבר הפיך מודולו  $n$ :**  $a \in \mathbb{Z}$  המקיים  $\exists b \in \mathbb{Z}. a \cdot b \equiv 1 \pmod n$

**טענה:** יהי  $a \in \mathbb{Z}$  אזי  $(a \text{ הפיך מודולו } n) \iff (a + n\mathbb{Z} \text{ הפיך ב-}\mathbb{Z}_n)$

**טענה:** יהי  $a$  הפיך ב- $\mathbb{Z}_n$  אזי  $\exists! b \in \mathbb{Z}_n. a \cdot b = 1$

**טענה:** יהי  $a \in \mathbb{Z}$  אזי  $(a \text{ הפיך מודולו } n) \iff (\gcd(a, n) = 1)$

$$\bullet \text{ סימון: } \mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid \exists b \in \mathbb{Z}_n. a \cdot b = 1\}$$

$$\bullet \text{ סימון: } \bar{a} = a + n\mathbb{Z}$$

**סימון:** יהי  $\bar{a} \in \mathbb{Z}_n$  הפיך ויהי  $\bar{b} \in \mathbb{Z}_n$  המקיים  $\bar{a}\bar{b} = \bar{1}$  אזי  $\bar{a}^{-1} = \bar{b}$

$$\bullet \text{ טענה: } (\bar{a} \cdot \bar{b})^{-1} = \bar{a}^{-1} \cdot \bar{b}^{-1}$$

$$\bullet \text{ פונקציית אוילר: } \phi(n) = |\mathbb{Z}_n^*|$$

**טענה:** יהי  $p \in \mathbb{P}$  אזי  $\phi(p) = p - 1$

**מסקנה:** יהי  $p \in \mathbb{P}$  אזי  $\mathbb{Z}_p$  שדה.

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

**טענה:** יהיו  $n, k \in \mathbb{N}_+$  זרים אזי  $(ka \equiv kb \pmod n) \iff (a \equiv b \pmod n)$

**טענה:** יהיו  $n, k \in \mathbb{N}_+$  ויהי  $r \in \mathbb{N}$  מחלק משותף אזי  $(ka \equiv kb \pmod n) \iff (\frac{k}{r}a \equiv \frac{k}{r}b \pmod{\frac{n}{r}})$

**מסקנה:** יהיו  $n, k \in \mathbb{N}_+$  אזי  $(ka \equiv kb \pmod n) \iff (a \equiv b \pmod{\frac{n}{\gcd(k, n)}})$

**טענה:** יהי  $p \in \mathbb{P}$  ויהי  $m \in \mathbb{N}_+$  עבורו  $p \mid m$  אזי  $\phi(pm) = p\phi(m)$

**טענה:** יהי  $p \in \mathbb{P}$  ויהי  $m \in \mathbb{N}_+$  עבורו  $p \nmid m$  אזי  $\phi(pm) = (p - 1)\phi(m)$

$$\bullet \text{ מסקנה: יהיו } s, \ell \in \mathbb{N}_+ \text{ ויהי } p \in \mathbb{P} \text{ המקיים } p \nmid s \text{ אזי } \phi(p^\ell \cdot s) = \begin{cases} p^{\ell-1}(p-1) & s=1 \\ p^{\ell-1}(p-1)\phi(s) & \text{else} \end{cases}$$

**מסקנה:** יהי  $n \in \mathbb{N}$  עם פירוק לראשוניים  $n = \prod_{m=1}^k p_m^{r_m}$  אזי  $\phi(n) = \prod_{i=1}^k p_i^{r_i-1}(p_i - 1)$

**מסקנה:** יהי  $n \in \mathbb{N}$  עם פירוק לראשוניים  $n = \prod_{m=1}^k p_m^{r_m}$  אזי  $\phi(n) = n \prod_{p \mid n} (1 - \frac{1}{p})$

**מסקנה:**  $\phi$  פונקציה כפלית.

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $\sum_{d \mid n} \phi(d) = n$

**ראשוני סופי ז'רמן:**  $q \in \mathbb{P}$  עבור  $2q + 1 \in \mathbb{P}$ .

**משפט:** יהי  $n \in \mathbb{N}$  ויהי  $q \in \mathbb{P} \setminus \{2\}$  עבורם  $\phi(n) = 2q$  אזי  $q$  ראשוני סופי ז'רמן.

**טענה:** יהי  $n \in \mathbb{N}_+$  אזי  $n\phi(n) = \sum_{\substack{\gcd(k,n)=1 \\ 1 \leq k \leq n}} k$ .

**משפט:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  ויהי  $b \in \mathbb{Z}$  ויהי  $n \in \mathbb{N}_+$  אזי  $(\gcd(a, n) | b) \iff (\text{sols}_{\mathbb{Z}_n}(ax = b) \neq \emptyset)$ .

**למה:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  יהיו  $b, c \in \mathbb{Z}$  ויהי  $n \in \mathbb{N}_+$  המקיימים  $\gcd(a, n) | b$  וכן  $c \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$  אזי  $(\frac{a}{\gcd(a, n)}) \cdot c \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$ .  
 $\text{sols}_{\mathbb{Z}_n}(ax = b) = \left\{ \frac{cb+rn}{\gcd(a, n)} \mid r \in \mathbb{Z} \right\}$ .

**משפט:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  יהיו  $b, c \in \mathbb{Z}$  ויהי  $n \in \mathbb{N}_+$  המקיימים  $\gcd(a, n) | b$  וכן  $c \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$  אזי  $(\frac{a}{\gcd(a, n)}) \cdot c \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$ .  
 $\text{sols}_{\mathbb{Z}_n}(ax = b) = \left\{ \frac{cb+kn}{\gcd(a, n)} \mid 0 \leq k \leq \gcd(a, n) \right\}$ .

**מסקנה:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  יהיו  $b, c \in \mathbb{Z}$  ויהי  $n \in \mathbb{N}_+$  המקיימים  $\gcd(a, n) | b$  אזי  $|\text{sols}_{\mathbb{Z}_n}(ax = b)| = \gcd(a, n)$ .

**משפט פתרון משוואות דיפנסיות לינאריות:** יהי  $a \in \mathbb{Z} \setminus \{0\}$  יהיו  $b, c, \alpha \in \mathbb{Z}$  ויהי  $n \in \mathbb{N}_+$  המקיימים  $\gcd(a, n) | b$  וגם  $\gcd(a, n) | \alpha$ .

$\text{sols}_{\mathbb{N}^2}(ax + ny = b) = \left\{ \left( \frac{cb+rn}{\gcd(a, n)}, -\frac{\alpha b+ra}{\gcd(a, n)} \right) \mid r \in \mathbb{Z} \right\}$  וכן  $(\frac{a}{\gcd(a, n)}) \cdot c \equiv 1 \pmod{\frac{n}{\gcd(a, n)}}$  אזי  $\frac{ac}{\gcd(a, n)} = 1 + \frac{\alpha n}{\gcd(a, n)}$ .

**משפט השאריות הסיני:** יהיו  $n_1 \dots n_k \in \mathbb{N}_+$  זרים ויהיו  $c_1 \dots c_k \in \mathbb{Z}$  אזי  $\exists! x \in \mathbb{Z}_{\prod_{i=1}^k n_i} \cdot \forall i \in [k] \cdot x \equiv c_i \pmod{n_i}$ .

**משפט אוילר:** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  ויהי  $a \in \mathbb{Z}$  המקיים  $\gcd(a, n) = 1$  אזי  $a^{\phi(n)} \equiv 1 \pmod{n}$ .

**מסקנה:** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  ויהי  $a \in \mathbb{Z}$  המקיים  $\gcd(a, n) = 1$  אזי  $a^{\phi(n)-1} \cdot a \equiv 1 \pmod{n}$ .

**מסקנה:** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  ויהיו  $a, x \in \mathbb{Z}$  המקיימים  $\gcd(a, n) = 1$  אזי  $a^x \equiv a^{x \pmod{\phi(n)}} \pmod{n}$ .

**המשפט הקטן של פרמה:** יהי  $p \in \mathbb{P}$  ויהי  $a \in \mathbb{Z}$  המקיים  $\gcd(a, p) = 1$  אזי  $a^{p-1} \equiv 1 \pmod{p}$ .

**הגדרה:**  $\mathbb{Z}_n[x] = \bigcup_{m=0}^{\infty} \{ \sum_{i=0}^m a_i x^i \mid \forall i \in [m] \cdot a_i \in \mathbb{Z}_n \}$ .

**הגדרה:** יהיו  $\sum_{i=0}^m a_i x^i, \sum_{i=0}^m b_i x^i \in \mathbb{Z}_n[x]$  אזי  $(a_i = b_i)$   $\iff (\sum_{i=0}^m a_i x^i = \sum_{i=0}^m b_i x^i)$ .

**סימון:** יהיו  $f, g \in \mathbb{Z}_n[x]$  אזי  $(f \equiv g \pmod{n}) \iff (f = g)$ .

**אריטמטיקה ב-**  $\mathbb{Z}_n[x]$ : יהיו  $\sum_{i=0}^m a_i x^i, \sum_{i=0}^k b_i x^i \in \mathbb{Z}_n[x]$  אזי

$$(\sum_{i=0}^m a_i x^i) + (\sum_{i=0}^k b_i x^i) = \sum_{i=0}^{\max\{m, k\}} (a_i + b_i) x^i.$$

$$(\sum_{i=0}^m a_i x^i) \cdot (\sum_{i=0}^k b_i x^i) = \sum_{i=0}^{m+k} \left( \sum_{\ell=0}^i a_\ell b_{i-\ell} \right) x^i.$$

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

**טענה:** יהי  $f \in \mathbb{Z}[x]$  ויהי  $m \in \mathbb{N}$  עם פירוק  $m = \prod_{i=1}^k p_i^{r_i}$  אזי  $|\text{sols}_{\mathbb{Z}_m}(f(x) = 0)| = \prod_{i=1}^k |\text{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x) = 0)|$ .

**מסקנה:** יהי  $f \in \mathbb{Z}[x]$  ויהי  $m \in \mathbb{N}$  עם פירוק  $m = \prod_{i=1}^k p_i^{r_i}$  אזי  $(\text{sols}_{\mathbb{Z}_m}(f(x)=0) \neq \emptyset) \iff (\forall i \in [k] \cdot \text{sols}_{\mathbb{Z}_{p_i^{r_i}}}(f(x)=0) \neq \emptyset)$ .

**משפט:** יהי  $f \in \mathbb{Z}[x]$  יהי  $p \in \mathbb{P}$  ויהי  $a_1 \in \mathbb{Z}$  פתרון של  $f(x) \equiv 0 \pmod{p}$  וכן  $f'(a_1) \not\equiv 0 \pmod{p}$  יהי  $f' \in \mathbb{N} \setminus \{0, 1\}$ .

אזי קיים ויחיד  $a_j \in \mathbb{Z}_{p^j}$  המקיים  $f(a_j) \equiv 0 \pmod{p^j}$  וכן  $a_j \equiv a_{j-1} \pmod{p^{j-1}}$ .

**הרמת פתרון:** יהי  $f \in \mathbb{Z}[x]$  יהי  $p \in \mathbb{P}$  יהי  $j \in \mathbb{N}_+$  ויהיו  $a_j, c \in \mathbb{Z}$  עבורם  $f(a_j) \equiv 0 \pmod{p^j}$  אזי  $a_j + cp^j \in \mathbb{Z}_{p^{j+1}}$ .

המקיים  $f(a_j + cp^j) \equiv 0 \pmod{p^{j+1}}$ .

**סדר:** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  ויהי  $a \in \mathbb{Z}_n^*$  אזי  $\text{ord}_n(a) = \min \{ d \in \mathbb{N}_+ \mid a^d \equiv 1 \pmod{n} \}$ .

**טענה:** יהי  $a \in \mathbb{Z}_n^*$  אזי  $(\text{ord}_n(a) | k) \iff (a^k \equiv 1 \pmod{n})$ .

**מסקנה:** יהי  $a \in \mathbb{Z}_n^*$  אזי  $\text{ord}_n(a) | \phi(n)$ .

**טענה:** יהי  $a \in \mathbb{Z}_n^*$  אזי  $\{1, a, a^2, \dots, a^{\text{ord}_n(a)-1}\}$  תת חבורה של  $\mathbb{Z}_n^*$ .

**טענה:** יהי  $a \in \mathbb{Z}_n^*$  ויהי  $m \in \mathbb{Z}$  אזי  $\text{ord}_n(a^m) = \frac{\text{ord}_n(a)}{\gcd(m, \text{ord}_n(a))}$ .

**שורש פרימיטיבי (ש"פ):** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  אזי  $a \in \mathbb{Z}_n^*$  המקיים  $\text{ord}_n(a) = \phi(n)$ .

**טענה:** יהי  $n \in \mathbb{N} \setminus \{0, 1\}$  ויהי  $a \in \mathbb{Z}_n^*$  אזי  $(a \text{ ש"פ}) \iff (a \text{ יוצר את } \mathbb{Z}_n^*)$ .

**טענה:** יהי  $a \in \mathbb{Z}_n^*$  שורש פרימיטיבי אזי קיימים  $\phi(\phi(n))$  שורשים פרימיטיביים מודולו  $n$ .

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

**משפט:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $j \in \mathbb{N}_+$  אזי קיים שורש פרימיטיבי מודולו  $p^j$ .

**מסקנה:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $j \in \mathbb{N}_+$  אזי קיים שורש פרימיטיבי מודולו  $2p^j$ .

**למה:** יהי  $j \in \mathbb{N} \setminus \{0, 1, 2\}$  ויהי  $b \in \mathbb{N}_{\text{odd}}$  אזי  $b^{2^{j-2}} \equiv 1 \pmod{2^j}$ .

**מסקנה:** יהי  $j \in \mathbb{N} \setminus \{0, 1, 2\}$  ויהי  $b \in \mathbb{N}_{\text{odd}}$  אזי  $2^{j-2} \mid \text{ord}_{2^j}(b)$ .

**טענה:** יהי  $j \in \mathbb{N} \setminus \{0, 1, 2\}$  אזי לא קיים שורש פרימיטיבי מודולו  $2^j$ .

**למה:** יהיו  $n_1, n_2 \in \mathbb{N} \setminus \{0, 1, 2\}$  זרים ויהי  $a \in \mathbb{Z}_{n_1 n_2}^*$  אזי  $a^{\frac{1}{2}\phi(n_1 n_2)} \equiv 1 \pmod{n_1 n_2}$ .

**משפט:** יהי  $n \in \mathbb{N}_+$  אזי  $(\text{קיים שורש פרימיטיבי מודולו } n) \iff (n \in \{1, 2, 4\} \cup \{p^j \mid \frac{p \in \mathbb{P}}{j \in \mathbb{N}_+}\} \cup \{2p^j \mid \frac{p \in \mathbb{P}}{j \in \mathbb{N}_+}\})$ .

**משפט:** יהי  $n \in \mathbb{N}$  בעל שורש פרימיטיבי יהי  $a \in \mathbb{Z}_n^*$  ויהי  $m \in \mathbb{N}_+$  אזי  $(\text{sols}_{\mathbb{Z}_n}(x^m = a) \neq \emptyset) \iff (a^{\frac{\phi(n)}{\gcd(m, \phi(n))}} \equiv 1 \pmod{n})$ .

**מסקנה:** יהי  $n \in \mathbb{N}$  בעל שורש פרימיטיבי ויהי  $m \in \mathbb{N}_+$  נגדיר  $f: \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$   $f(x) \equiv x^m \pmod{n}$  אזי  $\text{Im}(f) = \left\{ a \in \mathbb{Z}_n^* \mid a^{\frac{\phi(n)}{\gcd(m, \phi(n))}} \equiv 1 \pmod{n} \right\}$ .

**טענה:** יהיו  $n, m \in \mathbb{N}_+$  באשר  $\gcd(m, \phi(n)) = 1$  אזי  $f: \mathbb{Z}_n^* \rightarrow \mathbb{Z}_n^*$   $f(x) \equiv x^m \pmod{n}$  חח"ע ועל.

**אלגוריתם RSA:**

• נבחר  $p, q \in \mathbb{P}$  גדולים, ונסמן  $n = pq$ .

• נבחר  $m \in \mathbb{Z}_{\phi(n)}^*$ , ונחשב  $s \equiv m^{-1} \pmod{\phi(n)}$ .

• נפרסם את  $(n, m)$  ונשמור בסוד על  $s$ .

• כאשר מישהו שולח לנו את ההודעה  $A$  הוא יחשב  $B \equiv A^m \pmod{n}$  וישלח את  $B$ , רק מי שידע את  $s$  יוכל לפצח את

$B$  כך  $A \equiv B^s \pmod{n}$ .

**טענה:** יהיו  $p, q \in \mathbb{P}$  נסמן  $N = pq$  נניח כי אנו יודעים את  $N, \phi(N)$  אזי אנו יודעים את  $p, q$  ב- $\mathcal{O}(1)$ .

**טענה:** מציאת פתרון למשוואה  $x^m \equiv B \pmod{n}$  באלגוריתם RSA שקול למציאת  $p, q$ .

**טענה:** מציאת  $p, q$  באלגוריתם RSA זוהי בעיה לא פתירה בזמן סביר. לא ניכנס כאן פורמלית לסיבוכיות פירוק לראשוניים

**טענה:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $a \in \mathbb{Z}_p^*$  אזי  $(a^{\frac{p-1}{2}} \equiv 1 \pmod{p}) \vee (a^{\frac{p-1}{2}} \equiv -1 \pmod{p})$ .

**מסקנה:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $a \in \mathbb{Z}_p^*$  אזי  $(\text{sols}_{\mathbb{Z}_p}(x^2 = a) \neq \emptyset) \iff (a^{\frac{p-1}{2}} \equiv 1 \pmod{p})$ .

**שארית ריבועית:** יהי  $p \in \mathbb{P} \setminus \{2\}$  אזי  $a \in \mathbb{Z}_p^*$  המקיים  $\text{sols}_{\mathbb{Z}_p}(x^2 = a) \neq \emptyset$ .

**מסקנה:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $a \in \mathbb{Z}_p^*$

•  $(a \text{ שארית ריבועית מודולו } p) \iff (a^{\frac{p-1}{2}} \equiv 1 \pmod{p})$ .

•  $(a \text{ לא שארית ריבועית מודולו } p) \iff (a^{\frac{p-1}{2}} \equiv -1 \pmod{p})$ .

**סימן לז'נדר:** יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $a \in \mathbb{Z}_p^*$  אזי  $\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ שארית ריבועית } p \\ -1 & \text{else} \end{cases}$ .

**מסקנה:**  $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ .

**טענה:**  $\left| \left\{ a \in \mathbb{Z}_p^* \mid \left(\frac{a}{p}\right) = 1 \right\} \right| = \frac{p-1}{2} = \left| \left\{ a \in \mathbb{Z}_p^* \mid \left(\frac{a}{p}\right) = -1 \right\} \right|$ .

**טענה:** יהי  $\alpha \in \mathbb{Z}_p^*$  שארית לא ריבועית ויהי  $\beta \in \alpha(\mathbb{Z}_p^*)^2$  אזי  $\beta$  לא שארית ריבועית.

**משפט:** יהי  $\alpha \in \mathbb{Z}_p^*$  שארית לא ריבועית אזי  $\{a^2 \mid a \in \mathbb{Z}_p^*\} \dot{\cup} \{\alpha \cdot a^2 \mid a \in \mathbb{Z}_p^*\} = \mathbb{Z}_p^*$ .

**טענה:** יהיו  $a, b \in \mathbb{Z}_p^*$  אזי  $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$ .



**משפט אוילר**: יהי  $p \in \mathbb{P} \setminus \{2, 3\}$  המקיים  $p \equiv 3 \pmod{4}$  וכן  $2p+1 \in \mathbb{P}$  אזי  $2^p - 1$  פריק.

**טענה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$  אזי  $\text{sols}_{\mathbb{Z}_2}(x^2 = a) = \{1\}$ .

**טענה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$

• אם  $a \equiv 1 \pmod{4}$  אזי  $\text{sols}_{\mathbb{Z}_4}(x^2 = a) = \{1, 3\}$

• אם  $a \not\equiv 1 \pmod{4}$  אזי  $\text{sols}_{\mathbb{Z}_4}(x^2 = a) = \emptyset$

**טענה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$

• אם  $a \equiv 1 \pmod{8}$  אזי  $\text{sols}_{\mathbb{Z}_8}(x^2 = a) = \{1, 3, 5, 7\}$

• אם  $a \not\equiv 1 \pmod{8}$  אזי  $\text{sols}_{\mathbb{Z}_8}(x^2 = a) = \emptyset$

**טענה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$  ויהי  $k \in \mathbb{N} \setminus \{0, 1, 2\}$  אזי  $(a \equiv 1 \pmod{8}) \iff (\text{sols}_{\mathbb{Z}_{2^k}}(x^2 = a) \neq \emptyset)$

**מסקנה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$  ויהי  $k \in \mathbb{N}_+$  אזי  $(a \equiv 1 \pmod{\gcd(8, 2^k)}) \iff (\text{sols}_{\mathbb{Z}_{2^k}}(x^2 = a) \neq \emptyset)$

**טענה**: יהי  $a \in \mathbb{Z}_{\text{odd}}$  ויהי  $k \in \mathbb{N}_+$  עבורם  $a \equiv 1 \pmod{\gcd(8, 2^k)}$  אזי  $|\text{sols}_{\mathbb{Z}_{2^k}}(x^2 = a)| = \begin{cases} 1 & k=1 \\ 2 & k=2 \\ 3 & k \geq 3 \end{cases}$

**טענה**: יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $j \in \mathbb{N}_+$  ויהי  $a \in \mathbb{Z}_p^*$  אזי  $(a^{\frac{1}{2}\phi(p^j)} \equiv 1 \pmod{p^j}) \iff (\text{sols}_{\mathbb{Z}_{p^j}}(x^2 = a) \neq \emptyset)$

**טענה**: יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $j \in \mathbb{N}_+$  ויהי  $a \in \mathbb{Z}_p^*$  המקיים  $a^{\frac{1}{2}\phi(p^j)} \equiv 1 \pmod{p^j}$  אזי  $|\text{sols}_{\mathbb{Z}_{p^j}}(x^2 = a)| = 2$

**טענה**: יהי  $n \in \mathbb{N}_+$  עם פירוק  $n = 2^{r_0} \prod_{i=1}^k p_i^{r_i}$  ויהי  $a \in \mathbb{Z}_n^*$

$(\text{sols}_{\mathbb{Z}_n}(x^2 = a) \neq \emptyset) \iff ((a \equiv 1 \pmod{\gcd(8, 2^{r_0})}) \wedge (\forall i \in [k]. a^{\frac{1}{2}\phi(p_i^{r_i})} \equiv 1 \pmod{p_i^{r_i}}))$

**מסקנה**: יהי  $n \in \mathbb{N}_+$  עם פירוק  $n = 2^{r_0} \prod_{i=1}^k p_i^{r_i}$  ויהי  $a \in \mathbb{Z}_n^*$  המקיים  $\text{sols}_{\mathbb{Z}_n}(x^2 = a) \neq \emptyset$  נסמן  $m = \begin{cases} 0, & r_0 \in \{0, 1\} \\ 1, & r_0 = 2 \\ 2, & \text{else} \end{cases}$

אזי  $|\text{sols}_{\mathbb{Z}_n}(x^2 = a)| = 2^k \cdot 2^m$

**הלמה של גאוס**: יהי  $p \in \mathbb{P} \setminus \{2\}$  ויהי  $a \in \mathbb{Z}_p^*$  אזי  $\left(\frac{a}{p}\right) = (-1)^{\left|\left\{j \in \{1, \dots, \frac{p-1}{2}\} \mid \begin{matrix} aj \in [-\frac{p-1}{2}, \frac{p-1}{2}] \\ aj < 0 \end{matrix} \right\}\right|}$

**טענה**: יהי  $p \in \mathbb{P} \setminus \{2\}$  אזי  $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

**מסקנה**: יהי  $p \in \mathbb{P} \setminus \{2\}$  אזי  $\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod{8} \\ -1 & p \equiv \pm 3 \pmod{8} \end{cases}$

**משפט ההדדיות הריבועית של גאוס**: יהיו  $p, q \in \mathbb{P} \setminus \{2\}$  באשר  $p \neq q$  אזי  $\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{1}{4}(p-1)(q-1)}$

**מסקנה**: בסדרה  $\{5n-1\}_{n=1}^{\infty}$  ישנם אינסוף ראשוניים.

**סמל יעקובי**: יהי  $n \in \mathbb{N}_{\text{odd}}$  עם פירוק  $n = \prod_{i=1}^k p_i^{r_i}$  ויהי  $a \in \mathbb{Z}_n^*$  אזי  $\left(\frac{a}{n}\right) = \prod_{i=1}^k \left(\frac{a}{p_i}\right)^{r_i}$

**טענה**: יהי  $n \in \mathbb{N}_{\text{odd}}$  ויהיו  $a, b \in \mathbb{Z}_n^*$

•  $(a \equiv b \pmod{n}) \implies \left(\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)\right)$

•  $(a \not\equiv b \pmod{n}) \iff \left(\left(\frac{a}{n}\right) = -1\right)$

**למה**: יהיו  $n_1 \dots n_k \in \mathbb{N}_{\text{odd}}$  אזי

•  $\frac{1}{2} \left( \left( \prod_{i=1}^k n_i \right) - 1 \right) \equiv \frac{1}{2} \sum_{i=1}^k (n_i - 1) \pmod{2}$

•  $\frac{1}{2} \left( \left( \prod_{i=1}^k n_i \right)^2 - 1 \right) \equiv \frac{1}{2} \sum_{i=1}^k (n_i^2 - 1) \pmod{2}$

**משפט**: יהיו  $n, m \in \mathbb{N}_{\text{odd}}$  ויהיו  $a, b \in \mathbb{N}_+$

• נניח כי  $a, b \in \mathbb{Z}_n^*$  אזי  $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{b}{n}\right)$

- נניח כי  $a \in \mathbb{Z}_n^* \cap \mathbb{Z}_m^*$  אזי  $\left(\frac{a}{n \cdot m}\right) = \left(\frac{a}{n}\right) \cdot \left(\frac{a}{m}\right)$
- נניח כי  $n \neq 1$  אזי  $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
- $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$

**חוק ההדיות של גאוס:** יהיו  $n, m \in \mathbb{N}_{\text{odd}} \setminus \{1\}$  אזי  $\left(\frac{m}{n}\right) \cdot \left(\frac{n}{m}\right) = (-1)^{\frac{1}{4}(n-1)(m-1)}$   
**אלגוריתם חישוב סמל יעקובי:** יהי  $n \in \mathbb{N}_{\text{odd}}$  עם פירוק  $n = \prod_{i=1}^k p_i^{r_i}$  ויהי  $a \in \mathbb{Z}_n^*$

**function** JacobiSymbolCalculator ( $a, n$ )

```

|  $k \leftarrow 0$ 
|  $s \leftarrow a$ 
| while  $s \in \mathbb{Z}_{\text{even}}$ 
|   |  $r \leftarrow \max \{ \ell \in \mathbb{N} \mid (2^\ell \mid s) \}$ 
|   |  $k \leftarrow k + r$ 
|   |  $s' \leftarrow (0 \leq s' \leq n-1) \wedge \left( s' \equiv \frac{s}{r} \pmod{n} \right)$ 
|   |  $s \leftarrow s'$ 
| return  $(-1)^{\frac{1}{8}k(n^2-1) + \frac{1}{4}(n-1)(s-1)} \cdot \text{JacobiSymbolCalculator}(n, s)$ 

```

**עד פרמה:** יהי  $n \in \mathbb{N}_+$  אזי  $a \in \mathbb{Z}_n^*$  המקיים  $a^{n-1} \not\equiv 1 \pmod{n}$

**מספרי קרמייקל:**  $n \in \mathbb{N}_+ \setminus \mathbb{P}$  עבורו  $\forall a \in \mathbb{Z}_n^*. a^{n-1} \equiv 1 \pmod{n}$

**טענה:** יהי  $k \in \mathbb{N} \setminus \{0, 1\}$  ויהי  $n \in \mathbb{N}_+$  עם פירוק לראשוניים זרים  $n = \prod_{i=1}^k p_i$  המקיימים  $(p_i - 1) \mid (n - 1)$ . אזי  $n$  מספר קרמייקל.

**כפולה משותפת מינימלית:** יהיו  $a_1 \dots a_n \in \mathbb{Z}$  באשר  $a_1 \dots a_n \neq 0$  אזי  $\min \{ d \in \mathbb{Z} \mid \forall i \in [n]. (a_i \mid d) \}$

**הגדרה:** נגדיר  $\lambda : \mathbb{N}_+ \rightarrow \mathbb{N}_+$  כך

$$\lambda(1) = 1$$

$$\lambda(2) = \phi(2) = 1$$

$$\lambda(4) = \phi(4) = 2$$

$$\lambda(2^j) = 2^{j-2} \text{ אזי } j \in \mathbb{N} \setminus \{0, 1, 2\}$$

$$\lambda(p^j) = \phi(p^j) = p^{j-1}(p-1) \text{ אזי } j \in \mathbb{N}_+ \text{ ויהי } p \in \mathbb{P} \setminus \{2\}$$

$$\lambda(n) = \text{lcm}(\lambda(2^{j_0}), \lambda(p_1^{j_1}), \dots, \lambda(p_k^{j_k})) \text{ אזי } n = 2^{j_0} \prod_{i=1}^k p_i^{j_i}$$

$$\text{ord}_{2^j}(5) = 2^{j-2} \text{ אזי } j \in \mathbb{N} \setminus \{0, 1, 2\}$$

**משפט:** יהי  $n \in \mathbb{N}_+$

$$\forall a \in \mathbb{Z}_n^*. a^{\lambda(n)} \equiv 1 \pmod{n}$$

$$\exists c \in \mathbb{Z}_n^*. \text{ord}_n(c) = \lambda(n)$$

**למה:** יהי  $n \in \mathbb{N} \setminus \{0, 1, 2\}$  אזי  $n \in \mathbb{N}_{\text{even}}$

**משפט:** יהי  $n \in \mathbb{N}$  מספר קרמייקל אזי קיים  $k \in \mathbb{N} \setminus \{0, 1\}$  וקיימים  $p_1 \dots p_k \in \mathbb{P}$  שונים עבורם  $n = \prod_{i=1}^k p_i$  וכן

$$\forall i \in [k]. (p_i - 1) \mid (n - 1)$$

**עד אוילריינקובי**: יהי  $n \in \mathbb{N}_{\text{odd}}$  אזי  $a \in \mathbb{Z}_n^*$  המקיים  $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ .  
**משפט**: יהי  $n \in \mathbb{N}_{\text{odd}}$  פריק אזי קיים עד אוילריינקובי.  
**אלגוריתם מבחן רביןמילר לבדיקת ראשוניות**: יהי  $n \in \mathbb{N}_{\text{odd}} \setminus \{1\}$  ויהי  $b \in \mathbb{Z}_n^*$  אזי

**function** RabinMillerPrimalityTest ( $n, b$ )

```

| if  $b^{n-1} \not\equiv 1 \pmod{n}$ 
|   return false
| if  $b^{\frac{n-1}{2}} \equiv \pm 1 \pmod{n}$ 
|   | if  $\frac{n-1}{2} \in \mathbb{N}_{\text{even}}$ 
|   |   | if  $b^{\frac{n-1}{2}} \equiv 1 \pmod{n}$ 
|   |   |   return RabinMillerPrimalityTest  $\left(n, b^{\frac{1}{2}}\right)$ 
|   |   | if  $b^{\frac{n-1}{2}} \equiv -1 \pmod{n}$ 
|   |   |   return maybe
|   |   return maybe
|   | if  $\frac{n-1}{2} \in \mathbb{N}_{\text{odd}}$ 
|   |   return maybe
| if  $b^{\frac{n-1}{2}} \not\equiv \pm 1 \pmod{n}$ 
|   return false

```

**משפט**: יהי  $n \in \mathbb{N}_{\text{odd}} \setminus \{1\}$  ויהי  $b \in \mathbb{Z}_n^*$  אזי  $(n \notin \mathbb{P}) \iff (\text{RabinMillerPrimalityTest}(n, b) = \text{false})$ .  
**תבנית ריבועית**: יהיו  $a, b, c \in \mathbb{Z}$  אזי  $f \in \mathbb{Z}[x, y]$  המוגדר  $f(x, y) = ax^2 + bxy + cy^2$ .  
**מטריצה מייצגת של תבנית ריבועית**: תהא  $f(x, y) = ax^2 + bxy + cy^2$  תבנית ריבועית אזי  $A_f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$ .  
**קבוצת התבניות הריבועיות**:  $\text{sym}_2(\mathbb{Z}) = \{A \in M_2(\mathbb{Z}) \mid A = A^t\}$ .  
**טענה**: תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי  $f(v) = vA_f v^t$ .  
**דיסקרימיננטה של תבנית ריבועית**: תהא  $f = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$  תבנית ריבועית אזי  $\Delta_f = b^2 - 4ac$ .  
**טענה**: תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי  $(\Delta_f \equiv 0 \pmod{4}) \vee (\Delta_f \equiv 1 \pmod{4})$ .  
**טענה**: יהי  $\delta \in \mathbb{Z}$  המקיים  $(\delta \equiv 0 \pmod{4}) \vee (\delta \equiv 1 \pmod{4})$  אזי  $\exists f \in \text{sym}_2(\mathbb{Z}). \Delta_f = \delta$ .  
**פירוק תבנית ריבועית לגורמים לינאריים**:  $f \in \text{sym}_2(\mathbb{Z})$  עבורה  $(f(x, y) = (mx + \ell y)(rx + sy))$   $\iff \exists m, \ell, r, s \in \mathbb{Q}$ .  
**משפט גאוס**: תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי  $(f \text{ פריקה לגורמים לינאריים מעל } \mathbb{Q}) \iff (f \text{ פריקה לגורמים לינאריים מעל } \mathbb{Z})$ .  
**טענה**: תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי  $(f \text{ פריקה לגורמים לינאריים מעל } \mathbb{Z}) \iff (\exists k \in \mathbb{Z}. \Delta_f = k^2)$ .  
**ייצוג על ידי תבנית**: תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי  $n \in \mathbb{N}$  המקיים  $f(v, u) = n$   $\iff \exists u \in \mathbb{Z}. \exists v \in \mathbb{Z}_u^*. f(v, u) = n$ .  
**משפט**: יהי  $\delta \in \mathbb{Z} \setminus \{k^2 \mid k \in \mathbb{Z}\}$  המקיים  $(\delta \equiv 0 \pmod{4}) \vee (\delta \equiv 1 \pmod{4})$  ויהי  $n \in \mathbb{Z}$  אזי (קיימת)  $f \in \text{sym}_2(\mathbb{Z})$  המקיימת  $\Delta_f = \delta$  וכן  $n$  מיוצג על ידי  $f$   $\iff (\text{sols}_{\mathbb{Z}_{4n}}(x^2 = \delta) \neq \emptyset)$ .  
**סימון**:  $\text{SL}_2(\mathbb{Z}) = \{U \in M_2(\mathbb{Z}) \mid \det(U) = 1\}$ .  
**טענה**:  $\text{SL}_2(\mathbb{Z})$  חבורה ביחס לכפל מטריצות.

**תבניות ריבועיות שקולות:**  $f, g \in \text{sym}_2(\mathbb{Z})$  המקיימות  $f((x, y)) = g((x, y)U)$   $\exists U \in \text{SL}_2(\mathbb{Z})$ .

**טענה:** שקילות תבניות ריבועיות הינו יחס שקילות.

**סימון:** יהיו  $f, g \in \text{sym}_2(\mathbb{Z})$  שקולות אזי  $f \sim g$ .

**טענה:** יהיו  $f, g \in \text{sym}_2(\mathbb{Z})$  אזי  $A_g = U A_f U^t$   $\iff (\exists U \in \text{SL}_2(\mathbb{Z}))$ .

**טענה:** תהא  $U \in \text{SL}_2(\mathbb{Z})$  ונגדיר  $T_U: \mathbb{Z}^2 \rightarrow \mathbb{Z}^2$   $T_U(m, n) = (m, n) \cdot U$  אזי

•  $T_u$  חח"ע ועל.

• יהיו  $m, n \in \mathbb{Z}$  אזי  $(\gcd(T_U(m, n)) = 1) \iff (\gcd(m, n) = 1)$ .

**טענה:** תהיינה  $f, g \in \text{sym}_2(\mathbb{Z})$  שקולות אזי

•  $\Delta_f = \Delta_g$ .

•  $f(\mathbb{Z} \times \mathbb{Z}) = g(\mathbb{Z} \times \mathbb{Z})$ .

• יהי  $n \in \mathbb{Z}$  אזי  $(n \text{ מיוצג על ידי } f) \iff (n \text{ מיוצג על ידי } g)$ .

**משפט:** תהא  $f \in \text{sym}_2(\mathbb{Z})$  אזי קיימת  $f \sim \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$  המקיימת  $|b| \leq |a| \leq |c|$ .

**אלגוריתם חפיפת תבנית לצורה קנונית:** תהא  $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$  אזי

**function** CanonicalFormMatrixCongruence  $\left( \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \right)$

|  $M \leftarrow \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$

| **while**  $\neg (|b| \leq |a| \leq |c|)$

|     | **if**  $|c| < |a|$

|     |      $M \leftarrow \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} M \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^t$

|     | **if**  $|a| < |b|$

|     |      $k \leftarrow \{k \in \mathbb{Z} \mid |-b + 2ck| \leq |c|\}$

|     |      $M \leftarrow \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix} M \begin{pmatrix} 1 & 0 \\ k & 1 \end{pmatrix}^t$

| **return**  $M$

**משפט:** נסמן  $\text{CanonicalFormMatrixCongruence} \left( \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \right) = \begin{pmatrix} d & \frac{e}{2} \\ \frac{e}{2} & f \end{pmatrix}$  אזי  $\begin{pmatrix} d & \frac{e}{2} \\ \frac{e}{2} & f \end{pmatrix} \sim \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$  וכן  $|e| \leq |d| \leq |f|$ .

**סימון:** תהא  $A \in \text{sym}_2(\mathbb{Z})/\sim$  ותהא  $f \in A$  אזי  $\Delta_A = \Delta_f$ .

**מסקנה:** יהי  $\delta \in \mathbb{Z} \setminus \{k^2 \mid k \in \mathbb{Z}\}$  המקיים  $(\delta \equiv 0 \pmod{4}) \vee (\delta \equiv 1 \pmod{4})$  אזי  $|\{A \in \text{sym}_2(\mathbb{Z})/\sim \mid \Delta_A = \delta\}| \in \mathbb{N}$ .

**תבנית חיובית לחלוטין:**  $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$  המקיימת  $(\Delta < 0) \wedge (a > 0)$ .

**מחלקה חיובית לחלוטין:**  $A \in \text{sym}_2(\mathbb{Z})/\sim$  עבורה כל  $f \in A$  הינה חיובית לחלוטין.

**תבנית שלילית לחלוטין:**  $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$  המקיימת  $(\Delta < 0) \wedge (a < 0)$ .

**מחלקה שלילית לחלוטין:**  $A \in \text{sym}_2(\mathbb{Z})/\sim$  עבורה כל  $f \in A$  הינה שלילית לחלוטין.

**תבנית בצורה מצומצמת:**  $\begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \in \text{sym}_2(\mathbb{Z})$  המקיימת  $(0 \leq b \leq a = c) \vee (-a < b \leq a < c)$ .

**טענה:** תהא  $A \in \text{sym}_2(\mathbb{Z})/\sim$  חיובית לחלוטין אזי קיימת  $f \in A$  מצומצמת.

**טענה:** תהא  $f \in \text{sym}_2(\mathbb{Z})$  מצומצמת אזי  $f(x, y) = a - |b| + c$   $\min_{x, y \in \mathbb{Z} \setminus \{0\}}$ .

**מסקנה:** תהא  $f \in \text{sym}_2(\mathbb{Z})$  מצומצמת אזי  $f(x, y) = a$   $\min_{(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}}$

**מסקנה:** תהא  $f \in \text{sym}_2(\mathbb{Z})$  מצומצמת אזי  $f(x, y) = a$   $\min_{\gcd(x,y)=1}$

**משפט:** יהיו  $f, g \in \text{sym}_2(\mathbb{Z})$  מצומצמות אזי  $(f \sim g) \iff (f = g)$

**סימון:** יהי  $\delta \in \mathbb{Z} \setminus \mathbb{N}$  אזי  $h(\delta) = |\{A \in \text{sym}_2(\mathbb{Z}) / \sim \mid (\Delta_A = \delta) \wedge (A \text{ חיובית לחלוטין})\}|$

**משפט:** יהי  $n \in \mathbb{N}_+$  אזי  $(\exists k, m \in \mathbb{N}. k^2 + m^2 = n) \iff (\forall p \in \mathbb{P}. (p \mid n) \wedge (p \equiv 3 \pmod{4}) \implies \max\{r \in \mathbb{N} \mid (p^r \mid n)\} \in \mathbb{N}_{\text{even}})$

**מסקנה משפט פרמה:** יהי  $p \in \mathbb{P} \setminus \{2\}$  אזי  $(p \equiv 1 \pmod{4}) \iff (\exists k, m \in \mathbb{N}. k^2 + m^2 = p)$

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי (קיים  $\theta$  לצוג עשרוני סופי)  $\iff (\exists z \in \mathbb{Z}. \exists n, k \in \mathbb{N}. \theta = \frac{z}{2^n 5^k})$

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי (קיים  $\theta$  לצוג עשרוני סופי)  $\iff$  (קיימים  $\theta$  לצוגים עשרוניים שונים).

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי (קיים  $\theta$  לצוג מחזורי החל ממקום מסויים)  $\iff (\theta \in \mathbb{Q})$

**סימון:** יהיו  $x_0 \dots x_n \in \mathbb{R}$  אזי  $[x_0, \dots, x_n] = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\ddots + \frac{1}{x_n}}}}}$

**שבר משולב:** יהיו  $a_0 \dots a_n \in \mathbb{Z}$  אזי  $[a_0, \dots, a_n]$

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי  $(\theta \in \mathbb{Q}) \iff (\exists a_0 \dots a_n \in \mathbb{Z}. \theta = [a_0, \dots, a_n])$

**סימון:** תהא  $x \in \mathbb{R}^{\mathbb{N}}$  אזי  $[x_0, x_1, \dots] = x_0 + \frac{1}{x_1 + \frac{1}{x_2 + \frac{1}{x_3 + \frac{1}{\ddots}}}}$

**שבר משולב:** תהא  $a \in \mathbb{Z}^{\mathbb{N}}$  אזי  $[a_0, a_1, \dots]$

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי  $(\theta \notin \mathbb{Q}) \iff (\exists a \in \mathbb{Z}^{\mathbb{N}}. \theta = [a_0, a_1, \dots])$

**אלגוריתם פיתוח מספר ממשי לשבר משולב:** יהי  $\theta \in \mathbb{R}$  אזי

**function** ContinuedFractionConverter ( $\theta$ )

```

| if  $\theta \in \mathbb{Z}$ 
|   return  $\theta$ 
|  $a \leftarrow \lfloor \theta \rfloor$ 
|  $\theta' \leftarrow \frac{1}{\theta - a}$ 
| return  $a + \frac{1}{\text{ContinuedFractionConverter}(\theta')}$ 

```

**משפט:** יהי  $\theta \in \mathbb{R}$  אזי ContinuedFractionConverter ( $\theta$ ) הינו שבר משולב של  $\theta$ . אם רץ לנצח השבר אינסופי

**מנות חלקיות:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  אזי  $a \in \mathbb{Z}^{\mathbb{N}}$  עבורה  $\theta = [a_0, a_1, \dots]$

**הגורמים המתכנסים:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  ותהא  $\theta = [a_0, a_1, \dots]$  אזי  $\{[a_0, \dots, a_k]\}_{k=0}^{\infty}$

**הגדרה:** תהא  $a \in \mathbb{Z}^{\mathbb{N}}$  אזי נגדיר  $p, q \in \mathbb{Z}^{\mathbb{N} \uplus \{-1, -2\}}$  כך

$$(\forall k \in \mathbb{N}. p_k = a_k p_{k-1} + p_{k-2}) \wedge \begin{pmatrix} p_{-2}=0 \\ p_{-1}=1 \end{pmatrix} \bullet$$

$$(\forall k \in \mathbb{N}. q_k = a_k q_{k-1} + q_{k-2}) \wedge \begin{pmatrix} q_{-2}=1 \\ q_{-1}=0 \end{pmatrix} \bullet$$

**טענה:** תהא  $a \in \mathbb{R}^{\mathbb{N}}$  אזי  $\frac{p_n}{q_n} = [a_0 \dots a_n]$   $\forall n \in \mathbb{N}$ .

**טענה:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  ותהא  $\theta = [a_0, a_1, \dots]$  אזי  $\{q_n\}_{n=1}^{\infty}$  עולה ממש.

**טענה:**  $\forall n \in \mathbb{N} \uplus \{-1\}. p_n q_{n-1} - p_{n-1} q_n = (-1)^{n-1}$

**מסקנה:**  $\forall n \in \mathbb{N} \cup \{-1\}. \gcd(p_n, q_n) = 1$ .

**טענה:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  אזי  $\lim_{n \rightarrow \infty} \frac{p_n}{q_n} = \theta$ .

**מסקנה:** תהא  $a \in \mathbb{Z}^{\mathbb{N}}$  אזי  $\lim_{n \rightarrow \infty} [a_0 \dots a_n] = [a_0, a_1 \dots]$ .

**למה:** יהי  $a \in \mathbb{Z}$  יהי  $b \in \mathbb{N}$  ויהי  $x \in \mathbb{R}$  אזי  $\lfloor \frac{a+x}{b} \rfloor = \left\lfloor \frac{a+\lfloor x \rfloor}{b} \right\rfloor$ .

**סימון:** יהיו  $a_0 \dots a_n, b_0 \dots b_m \in \mathbb{Z}$  אזי  $[a_1 \dots a_n, \overline{b_1 \dots b_m}] = [a_1 \dots a_n, b_1 \dots b_m, b_1 \dots b_m \dots]$ .

**טרינום:** יהיו  $a, b, c \in \mathbb{R}$  אזי  $f \in \mathbb{R}[x]$  המוגדר  $f(x) = ax^2 + bx + c$ .

**דסקרימיננטה:** יהי  $\Delta = b^2 - 4ac$  טרינום  $ax^2 + bx + c \in \mathbb{R}[x]$ .

**משפט לגראנז':** יהי  $\alpha \in \mathbb{R}$  אזי  $(\exists a_0 \dots a_k, b_1 \dots b_m \in \mathbb{Z}. \alpha = [a_0 \dots a_k, \overline{b_1 \dots b_m}]) \iff$  (קיים טרינום  $f \in \mathbb{Z}[x]$

המקיים  $(f(\alpha) = 0 \text{ עבורו } \Delta \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\})$ .

**מספר ניתן לקירוב דיופנטי מסדר  $r$ :**  $\alpha \in \mathbb{R}$  המקיים  $\exists c \in \mathbb{R}_+. |\{\frac{n}{m} \mid (\frac{n}{m} \in \mathbb{Z}) \wedge (|\alpha - \frac{n}{m}| < \frac{1}{cm^r})\}| \geq \aleph_0$

**טענה:** יהי  $\theta \in \mathbb{R}$  אזי  $\exists p, q \in \mathbb{Z}. \left| \theta - \frac{p}{q} \right| \leq \frac{1}{2q}$ .

**מסקנה:** יהי  $\theta \in \mathbb{R}$  ניתן לקירוב דיופנטי מסדר ראשון.

**טענה:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  אזי  $\forall n \in \mathbb{N}. \left| \theta - \frac{p_n}{q_n} \right| < \frac{1}{q_n^2}$ .

**מסקנה:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  ניתן לקירוב דיופנטי מסדר שני.

**משפט:** יהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  אזי  $\frac{p_n}{q_n}$  הינו הקירוב הדיופנטי הטוב ביותר כלומר

• במובן החלש: יהיו  $a, b \in \mathbb{Z}$  באשר  $1 \leq b < q_n$  אזי  $\left| \theta - \frac{p_n}{q_n} \right| < \left| \theta - \frac{a}{b} \right|$ .

• במובן החזק: יהיו  $a, b \in \mathbb{Z}$  באשר  $1 \leq b < q_{n+1}$  אזי  $|q_n \theta - p_n| < |b \theta - a|$ .

**מספר אלגברי:**  $\alpha \in \mathbb{R}$  המקיים  $f(\alpha) = 0$   $f \in \mathbb{Z}[x]$ .

**מספר טרנסצנדנטי:**  $\alpha \in \mathbb{R}$  שאינו אלגברי.

**מעלה של מספר אלגברי:** יהי  $\alpha \in \mathbb{R}$  אלגברי אזי  $\min \{ \deg(f) \mid (f \in \mathbb{Z}[x]) \wedge (f(\alpha) = 0) \}$ .

**משפט ליוביל:** יהי  $\alpha \in \mathbb{R}$  אלגברי ממעלה  $d$  אזי  $\exists c \in \mathbb{R}_+. \forall \frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}. \left| \alpha - \frac{p}{q} \right| \geq \frac{c}{q^d}$ .

**מספר ליוביל:**  $\alpha \in \mathbb{R}$  המקיים  $\forall d \in \mathbb{N}. \exists \frac{p}{q} \in \mathbb{Q} \setminus \{\alpha\}. \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^d}$ .

**מסקנה:** יהי  $\alpha \in \mathbb{R}$  מספר ליוביל אזי  $\alpha$  הינו טרנסצנדנטי.

**קבוע ליוביל:**  $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ .

**טענה:** קבוע ליוביל הינו מספר ליוביל.

**שדה ריבועי:** יהי  $d \in \mathbb{Z} \setminus \{k^2 \mid k \in \mathbb{N}\}$  אזי  $\mathbb{Q}[\sqrt{d}] = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$ .

**טענה:** יהי  $d \in \mathbb{Z} \setminus \{k^2 \mid k \in \mathbb{N}\}$  אזי

•  $\{1, \sqrt{d}\}$  מ"ו מעל  $\mathbb{Q}$  ממימד 2 עם בסיס  $\{1, \sqrt{d}\}$ .

•  $\mathbb{Q}[\sqrt{d}]$  שדה.

**מספר אירציונלי ממעלה שנייה:**  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  עבורו קיים  $f \in \mathbb{Z}[x]$  טרינום המקיים  $(f(\theta) = 0) \wedge (\Delta = 0)$ .

**משפט:** יהי  $f \in \mathbb{Z}[x]$  טרינום באשר  $\Delta \notin \{k^2 \mid k \in \mathbb{N}\}$  ויהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  פתרון אזי  $\sigma(\theta)$  פתרון מעל  $\mathbb{Q}[\sqrt{\Delta}]$ .

**טענה:** יהיו  $f, g \in \mathbb{Q}[x]$  טרינומים מתוקנים ויהי  $\theta \in \mathbb{R} \setminus \mathbb{Q}$  פתרון של שניהם אזי  $f = g$ .

**מספר אירציונלי ממעלה שנייה בעל מחזוריות טהורה:**  $\theta \in \mathbb{R}$  אירציונלי ממעלה שנייה המקיים  $\exists a_0 \dots a_n \in \mathbb{Z}. \theta = [\overline{a_0 \dots a_n}]$ .

**משפט:** יהי  $\theta \in \mathbb{R}$  אירציונלי ממעלה שנייה אזי  $(\theta \text{ בעל מחזוריות טהורה}) \iff ((\mathbb{Q}[\sqrt{\Delta}] \text{ מעל } -1 < \sigma(\theta) < 0) \wedge (\theta > 1))$ .

**מסקנה:** יהי  $d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}$  אזי  $\sqrt{d} + \left\lfloor \sqrt{d} \right\rfloor, \frac{1}{\sqrt{d} - \left\lfloor \sqrt{d} \right\rfloor}$  בעלי מחזוריות טהורה.

**משוואת פל:** יהי  $d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}$  אזי  $x^2 - dy^2 = 1$ .

**פתרון משוואת פל :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\} \mid \sqrt{d} = [a_0, a_1 \dots a_m]\}$  אזי  $\{ \pm (p_n, q_n) \mid \exists k \in \mathbb{Z}. n = mk - 1 \}$   $\overset{n \in \mathbb{N}_{\text{odd}}}{\text{אזי}}$   $\text{sols}_{\mathbb{Z}^2} (x^2 - dy^2 = 1) =$

**סימון :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}\}$  אזי  $\mathcal{O}_d^* = \left\{ x + y\sqrt{d} \mid \begin{smallmatrix} x, y \in \mathbb{Z} \\ x^2 - dy^2 = 1 \end{smallmatrix} \right\}$

**טענה :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}\}$  אזי  $\mathcal{O}_d^* = \left\{ x + y\sqrt{d} \mid \begin{smallmatrix} x, y \in \mathbb{Z} \\ N(x + y\sqrt{d}) = 1 \end{smallmatrix} \right\}$

**מסקנה :**  $\mathcal{O}_d^*$  תת חבורה של  $\mathbb{Q}[\sqrt{d}]$  ביחס לכפל.

**מסקנה :** יהי  $z \in \mathbb{Q}[\sqrt{d}]$  אזי  $z \in \mathcal{O}_d^* \iff (-z \in \mathcal{O}_d^*) \iff (\frac{1}{z} \in \mathcal{O}_d^*) \iff (z \in \mathcal{O}_d^*)$ .

**טענה :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}\}$  אזי  $|\mathcal{O}_d^*| \geq \aleph_0$ .

**טענה :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}\}$  אזי  $\varepsilon = \min \{x \in \mathcal{O}_d^* \mid x > 1\}$  קיים.

**משפט :** יהי  $\{d \in \mathbb{N} \setminus \{k^2 \mid k \in \mathbb{N}\}\}$  אזי  $\mathcal{O}_d^* = \{\pm \varepsilon^n \mid n \in \mathbb{Z}\}$