

24 תומים

ש. ה. כ. ח.

השערה א' פתרון

$$\pm d^n : p \nmid d \nmid K, \text{ odd } n, \text{ odd } d, 1 \leq d \in \mathbb{Z}$$

$$x^2 - dy^2 = 1$$

Pell

לשונות

$$x^2 - 13y^2 = 1$$

מקרה פחות טוב:

$$x^2 - 12y^2 = 1$$

מתנה פיק

$$x^2 = 1 + 12y^2$$

$y = x^2$

1 13

$2 + 49$

$$y_0 = 2$$

$$X_0 = 7$$

$$x^2 - 61y^2 = 1$$

$$y_0 = 226,153,980$$

$$X_0 = 1766,319,$$

 $\frac{x}{y}$

משפט: $\forall x \in \mathbb{R}$ $\exists$ y רציונלי, $y < x$ קיים אגף מספרים רציונליים

$$|\frac{x}{y} - 3^2| < \frac{1}{y}$$

2) $\gcd(x, y) = 1, x, y \in \mathbb{Z}$

$$[0, 1) = [0, \frac{1}{n}) \cup [\frac{1}{n}, \frac{2}{n}) \cup \dots \cup [\frac{n-1}{n}, 1)$$

תוכן:

חנה שמס

$\alpha \in \mathbb{R}$. מתקיים $\alpha - [\alpha] \in [0, 1)$ כאשר $[\alpha]$ הוא חלקו של α .

(סמל) δ הנחיש קיפ הישקורי פ' ו' $0, \zeta, 2\zeta, \dots, n\zeta$ $\leftarrow$ ו' $n+1$ נכנסת

[illegible]

1. $|x-y| < \frac{1}{n}$ נכנסים x ו- y ל- $X = \{j\}$ ו- $Y = \{k\}$, $y = j-k$ (3 נק')

$\gcd(x, y) = d > 1$ $\Rightarrow$ $\exists$ $p \mid d$, $\gcd(x, y) = 1$ $\Rightarrow$ $\exists$ $p \nmid d$. $0 < y \leq n$, $x, y \in \mathbb{Z}$

$$|x' - y'| \leq \frac{1}{an} < \frac{1}{n} \quad \text{ע"פ תנאי} \quad y' = \frac{y}{a}, \quad x' = \frac{x}{a} \quad \text{נניח}$$

נכיון !- $0 < y = h$ פסקנ $\frac{1}{ny} < \frac{1}{y^2}$ $\left| \frac{x}{y} - 3 \right| < \frac{1}{ny}$ $\leftarrow$ מתקיי n של x

הבה נקבע אינדיקס פתיונות, (שים לב שמתקיים $|x - \frac{1}{3}| \neq 0$),

ל γ $0 < x, y \in \mathbb{Z}$ $\exists$ $\frac{1}{m} < |\frac{x}{y} - \zeta|$ $\forall$ $0 < m \in \mathbb{Z}$ $\wedge$ $n \in \mathbb{N}$

-የሃይማኖት ጥበቃና መልካም - $\left| \frac{x_1}{y_1} - \frac{1}{my_1} \right| < \frac{1}{my_1}$, $\left| \frac{x}{y} - \frac{1}{y} \right| < \frac{1}{y}$

$$\frac{x_1}{y_1} \neq \frac{x}{y}$$

הא"ש חזק עין

משפט גרין - $x^2 dy^2$ מחזוריות בקו סגור

(נמו) נמצא את $x+y$ עם נורמה 1, y ו- x (שקיים).

(d) 15 ימים)

משפט קוויס $M > 0$ קר $|x^2 - dy^2| < M$ יש אין סוף פתרונות.

המשוואה $x^2 - dy^2 = (x + y\sqrt{d})(x - y\sqrt{d})$ נקראת משוואת פנוליס.

$$(z = \sqrt{d}) \quad |x - y\sqrt{d}| \leq \frac{1}{y} \quad \text{es } p \text{ prim } \nmid d \text{ prim } \nmid (x, y)$$

• p d) $|x + \sqrt{2}y| \leq |x - y\sqrt{2}| + |2y\sqrt{2}| < \frac{1}{y} + 2y\sqrt{2} : \text{no}$

$$|x^2 - dy^2| < (\frac{1}{y} + 2\sqrt{d}) \frac{1}{y} = \frac{1}{y^2} + 2\sqrt{d} < 1 + 2\sqrt{d}$$

$$\blacksquare |x^2 - dy^2| < M \quad \text{נישאלנו זוגות } (x, y) \text{ ק"ש-} M = 1 + 2\sqrt{d} \quad \text{ע"פ נה"ח}$$

משפט: אם d שיש חזקי שאינו ריבוע שלם אז למשוואה $x^2 - dy^2 = 1$ יש אינסוף פתרונות.

יתר על כן קיים פתרון (x_1, y_1) כך שכל פתרון נוסף מהצורה

$$(x_n, y_n) = \pm (x_1 + y_1 \sqrt{d})^n \quad \text{כאשר } n \in \mathbb{Z}$$

⚠ דבורה אשתי נהגה $(x_1 - y_1 \sqrt{d})^n = x_n - y_n \sqrt{d}$ (כדי שהיה נוח) (נראה=1).

הוכחה: אם המשוואה $x^2 - dy^2 = m$ יש לה אינסוף פתרונות (x, y) אז $x^2 - dy^2 = 1$

(כי חסם בין M ו- M ומקבל ערכים שלמים בלבד).

יתר על כן, לאפשר למצוא (x_1, y_1) , (x_2, y_2) כך ש- $x_1 = x_2(m)$, $y_1 = y_2(m)$

$$(x_1^2 - dy_1^2 = m, x_2^2 - dy_2^2 = m) \Rightarrow x^2 - dy^2 = m^2 \quad \text{יש לה אינסוף פתרונות "חזריים".}$$

$$\alpha = x_1 - y_1 \sqrt{d}, \beta = x_2 - y_2 \sqrt{d} \quad \text{נסתב ע"ש } \frac{\alpha}{\beta}$$

~~הוכחה שהמשוואה היא חזרית~~

$$\Delta \text{ ההפך: אם } \delta = x + y\sqrt{d}, \delta' = x - y\sqrt{d}, \delta \delta' = x^2 - dy^2 = m \quad N(\delta \delta') = N(\delta) \cdot N(\delta') \leq N(\delta)$$

(הוכחנו רק עבור $d=2$ אבל נכון לכל d).

$$\alpha \beta' = (x_1 - y_1 \sqrt{d})(x_2 + y_2 \sqrt{d}) = x_1 x_2 - dy_1 y_2 + (x_1 y_2 - y_1 x_2) \sqrt{d}$$

$$m | (x_1 x_2 - dy_1 y_2) \leftarrow x_1 x_2 - dy_1 y_2 = x_1^2 - dy_1^2 = m(m) \quad \text{כזוטה}$$

$$m | (x_1 y_2 - y_1 x_2) \leftarrow x_1 y_2 - y_1 x_2 = x_1 y_1 - x_1 y_1 = 0 \quad \text{כזוטה}$$

$$\frac{m}{N(\alpha)} \cdot \frac{m}{N(\beta)} = m^2 (u^2 - dv^2) \quad \text{אם } \alpha \beta' = m(u + v\sqrt{d}), u, v \in \mathbb{Z} \quad \leftarrow$$

$$u^2 - dv^2 = 1 \quad \text{יש פתרון.} \quad \leftarrow$$

$$N(\frac{\alpha}{\beta}) = \frac{N(\alpha)}{N(\beta)} = 1 \quad \text{גם מתקיים: } u + v\sqrt{d} = \frac{\alpha}{\beta} = \frac{\alpha \beta'}{N(\beta)} = \frac{\alpha \beta'}{m}$$

$$u^2 - dv^2 = 1 \quad \text{אם קיבלנו } V \neq 0 \quad \text{נבדוק ש- } V \neq 0$$

$$\alpha \beta' = \pm m \quad \leftarrow \quad u = \pm 1 \quad \text{אם } V = 0$$

$$\text{כפ"ס } \beta \text{ נקבל: } \alpha m = \pm \beta, \quad x_1 = \pm x_2, \quad y_1 = \pm y_2 \quad \text{כחירה!}$$

ע"פ $V \neq 0$, קיבלנו פתרון לא טריוויאלי.

אנחנו שפתחנו את (x, y) עבור $N(u, v) = 1$ אל (u, v) .

(כעת רק ע"פ פתרונות ע"פ (u, v) אז $(x, y) > (u, v)$)

$$x = \sqrt{1 + dy^2} > \sqrt{1 + dv^2} = x' \quad \text{אם } y = y' \quad \text{פתרונות}$$

$y \in \mathbb{Z}$ ע"פ קיים פתרון שהוא הפך קוויטר וטריאלי- (x_1, y_1)

הוכחת תוצאה

כנסת ההוכחה:

אנחנו יודעים: כי פתרון המשוואה $(x_n + y_n \sqrt{d}) = \pm (x_1 + y_1 \sqrt{d})^n$, $n \in \mathbb{Z}$

נסמן $d = x_1^2 + y_1^2$ (פתרון המשוואה), $0 < x_1, y_1 \in \mathbb{Z}$

$\beta = r + s\sqrt{d}$ ו- $r, s > 0$

נראה שיש סדרה כזו ו- $\beta = \alpha^n$ אחרת, קיים $n > 0$ ו- $\alpha^n < \beta < \alpha^{n+1}$

נניח $1 < \alpha^{-n} \beta < \alpha$

זהו פתרון וזה יהיה סתירה אם α מינימלי, לכן רק במקרה של היתכנות

יש $(\alpha')^n \beta = A + B\sqrt{d}$, $A, B \in \mathbb{Z}$, $r, s > 0$

$A^2 - dB^2 = 1$ (נניח שהיה) לכן $A + B\sqrt{d}$ פתרון. ואם $A, B > 0$

$1 < A + B\sqrt{d} < \alpha$. $A - B\sqrt{d} = (A + B\sqrt{d})^{-1} > 0$

לכן: $A = \frac{1}{2}[(A + B\sqrt{d}) + (A - B\sqrt{d})] > 0$ ו- $A - B\sqrt{d} = (A + B\sqrt{d})^{-1} < 1$

כי $A + B\sqrt{d} > 1 \Leftrightarrow B = \frac{1}{2\sqrt{d}}[(A + B\sqrt{d}) - (A - B\sqrt{d})] > 0$ ו- $B > 0$ ו- $A > 0$

לכן קיבלנו סתירה ו- $\beta = \alpha^n$, $0 < n$

אם פתרון β , $\beta = r + s\sqrt{d}$, $0 < r, s$

אם $\beta = \alpha^n \Leftrightarrow u > 0 \Leftrightarrow \beta = \alpha^{-n} \Leftrightarrow n > 0$, $\beta' = \alpha^n$ כל, $v < 0$, $\beta = u + v\sqrt{d}$ כל

אם $u < 0$ כל, $n \in \mathbb{Z}$, $-\beta = \alpha^n$ כל, $n \in \mathbb{Z}$, $\beta = -\alpha^n$

לכן אם פתרון $\beta = u + v\sqrt{d}$, $u, v \in \mathbb{Z}$, $\beta = \pm \alpha^n$, $n \in \mathbb{Z}$