

תוספת 22

כנסו ליחידות דיפרנציאליות ועקרון חוקי היסודיים

שאלה: $\sqrt{2}$ אינו רציונלי

הוכחה: נניח בשלילה ש $\sqrt{2}$ רציונלי, $\Leftrightarrow \exists x, y \in \mathbb{Z} : \sqrt{2} = \frac{x}{y}$
 $x, y \in \mathbb{Z} : x^2 = 2y^2 = 0 \pmod{2}$

$\otimes$ אומרים שהעריון של $\otimes$ הוא פרימיטיביות $\gcd(x, y) = 1$.

אם יש פתרון שליוו (ס,ס) אז יש פתרון פרימיטיבי. נניח של (x, y) פתרון פרימיטיבי.

$x^2 - 2y^2$ אז x^2 זוגי, זמן x זוגי. $x = 2z$, $4z^2 = 2y^2 \Leftrightarrow (2z)^2 = 2y^2$
 $2z^2 = y^2$
 וזין y^2 זוגי, זמן y זוגי $\Leftrightarrow 2|x, 2|y$ וזה סתירה! פתרון פרימיטיבי.

צורתה של משוואה דיפרנציאלית: $y^2 = 4x + 3$

טענה: אין פתרון שלמשוואה זו. מתקיים: $y^2 = 3(4)$

אין פתרון! $\Rightarrow \left(\frac{3}{4}\right) = \left(\frac{4}{3}\right) = \left(\frac{2}{3}\right) = -1$

צורתה: $y^2 = x^3 + 7$, $x, y \in \mathbb{Z}$.

שאלה: אין פתרון. הוכחה:

אם יש פתרון x אי-זוגי, x אי-זוגי $\Rightarrow x^3 + 7$ אי-זוגי $\Rightarrow y^2$ אי-זוגי. $y^2 = 3(4)$ וזה אי-אפשר.
 $y^2 + 1 = (x+2)(x-1)^2 + 3$
 $\Leftrightarrow y^2 + 1 = x^3 + 8 = (x+2)(x^2 - 2x + 4)$ (כח תוספת)

$(x-1)^2 + 3 = 3(4)$ כי $x-1$ זוגי. (כאן): $(x-1)^2 + 3 = p_1 p_2 \dots p_r$ מכפלת חזקות שלמים.

אז p_i אי-זוגי, $p_i \equiv 1 \pmod{3}$ אבל לא ייתכן שהחזקת $p_i \equiv 1 \pmod{3}$ כי אז $3 \mid (x-1)^2 + 3$.

(תהי) $(x-1)^2 + 3 = 1(4)$ הסתירה. לכן יש i כך של $p_i \equiv 3(4)$.

$\Rightarrow p_i \mid (x-1)^2 + 3 \Leftrightarrow p_i \mid y^2 + 1 \Leftrightarrow p_i \mid y^2 - 1 \pmod{p_i} \Leftrightarrow p_i \equiv 1(4)$ סתירה! $\square$

הערות מקומיות חשובות:

$x \in \mathbb{Z}^n$ וקטור. $F(x) = \sum_{j=1}^n a_{ij} x_i x_j$. a_{ij} מטריצה סימטרית $n \times n$.

זו תכנית יסודית.

צורתה: $F(x) = x_1^2 + x_2^2 + 2x_3 + 2x_1 x_2$, $A = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ $n=3$

$F(x) = b(p)$, $0 \neq b \in \mathbb{Z}$, $x \neq 0$. האם יש פתרון שלם לא טריוויאלי?

אם יש פתרון $\mathbb{Z}^n$ אז יש פתרון $\mathbb{R}$, ויש פתרון למעלה $\mathbb{Q}$.

אז יש פתרון מודולו m אם $1 < m$.

נתון מקומי זוגי n א.א. יש פתרון מודולו m אם $p \mid m$ יש פתרון $\pmod{m}$.
אז יש פתרון מודולו 2 .

אם יש פתרון x וקונז' $F(x) = b \pmod{p}$ $\forall p \mid m$ אז יש פתרון $\pmod{m}$.
אם המשתנה x אינו פתרון מודולו 2 .

$$F(x_1, x_2, x_3) = -9x_1^2 + 2x_1x_2 + 7x_2^2 + 2x_3^2 = 1, \quad A = \begin{pmatrix} -9 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix} \quad \text{Borovoi, Rudnik 5:1.2.13}$$

יש מודולו p^e $\forall p \mid m$ אם x פתרון מודולו p $\forall p \mid m$.
יש פתרון מודולו 2 $F(-\frac{1}{2}, \frac{1}{2}, 1) = 1$.

פתרון מודולו p^e אם p אינו 2 $\frac{1}{2} \in \mathbb{Z}/p\mathbb{Z}$ $2y \equiv 1 \pmod{p}$ יש פתרון.

$$F(-y, y, 1) \equiv 1 \pmod{p^e} \quad 1-2^e \quad F(4, 1, 1) = -127 \equiv 1 \pmod{2^8} \quad p=2 \text{ דבר}$$

$$\frac{f(1)}{f'(1)} = \frac{-2^8}{2 \cdot 11} \quad \Leftarrow \quad \begin{aligned} f(x) &= F(4, x, 1) - 1 \\ f'(x) &= 22x \end{aligned}$$

על $F(x_1, x_2, x_3) = F$ אין פתרון מודולו 2 .

$$2x_3^2 - 1 = (x_1 - x_2)^2 + 8(x_1 - x_2)(x_1 + x_2)$$

$$-9x_1^2 + 2x_1x_2 + 7x_2^2 + 2x_3^2 = 1$$

החזק של משוואה אי-זוגית $x_1 - x_2$ אי-זוגי (מחזק את 3 ימין)

$$8(x_1 - x_2)(x_1 + x_2) \equiv 8 \pmod{16} \quad \text{כאשר } x_1 + x_2 \text{ אי-זוגי}$$

$$(x_1 - x_2)^2 \equiv 1 \pmod{8} \quad \text{כאשר } x_1 - x_2 \text{ אי-זוגי}$$

$$\text{RHS} \equiv 1 \pmod{16} \quad \text{כאשר } (x_1 - x_2)^2 \equiv 1 \pmod{16} \quad \text{כאשר } 9 \pmod{16}$$

$$2x_3^2 - 1 \equiv -1 \pmod{8} \quad \text{כאשר } x_3 \text{ אי-זוגי}$$

$$2x_3^2 \equiv 2 \pmod{16} \quad \text{כאשר } x_3^2 \equiv 1 \pmod{8}$$

$$\text{RHS} \equiv 1 \pmod{16} \quad \text{כאשר } 2x_3^2 - 1 \equiv 1 \pmod{16} \quad \Leftarrow$$

$$x_1 - x_2 \equiv \pm 3 \pmod{8} \quad \text{כאשר } (x_1 - x_2)^2 \equiv 9 \pmod{16} \quad \Leftarrow \quad 8(x_1 - x_2)(x_1 + x_2) \equiv 8 \pmod{16}$$

$$p_i \equiv \pm 3 \pmod{8} \quad \text{כאשר } x_1 - x_2 = p_1 p_2 \dots p_r$$

$$(2x_3)^2 \equiv 2 \pmod{p} \quad 2x_3^2 \equiv 1 \pmod{p} \quad \Leftarrow \quad p \mid 2x_3^2 - 1 \quad \text{כאשר } p \mid \text{RHS}$$

$$\text{אם } p \equiv \pm 1 \pmod{8} \quad \text{כאשר } \frac{2}{p} \equiv 1 \pmod{p}$$

החומר תחילת:

חספרים טרנסנדנטיים וצייבוי

$$\alpha \in \mathbb{R} \text{ אלטרנטיבי} \quad \exists, f(\alpha) = 0 \quad f = a_n x^n + \dots + a_0 \quad a_i \in \mathbb{Z}$$

$$\sqrt{2} \leftarrow x^2 - 2 = 0, \quad 2 \leftarrow x - 2 = 0$$

מספר טרנסנדנטי = לא אלטרנטיבי פולינום.

$$\mathbb{Z} \subset \mathbb{M} \subset \mathbb{Q} \leftarrow \mathbb{R} \subset \mathbb{C} \leftarrow \mathbb{R} \subset \mathbb{M} \subset \mathbb{Q} \leftarrow \mathbb{R} \subset \mathbb{M} \subset \mathbb{Q}$$

$$\mathbb{Q} \neq \mathbb{R}$$

צודאיות למספרים טרנסנדנטיים: $e, \pi, \sqrt{2}$.

$$1 \pm \frac{1}{2^1} \pm \frac{1}{2^2} \pm \frac{1}{2^3} \pm \dots$$

המספרים:

מספרים שאינם טרנסנדנטיים.

לא רציונליים - ונראה כי הם לא אלטרנטיביים.