

פרק 3: פונקציות ריבועיות ב-2 משתנים

אע"פ: אם $\Delta < 0$ אז $f(x,y) \neq 0$ לכל $(x,y) \in \mathbb{Z}^2$
סימן קבוע, $\text{Sign}(f(x,y)) = \text{Sign}(a) = \text{Sign}(c)$

משפט: נניח כי $f(x,y) = (u'x + v'y)(r'x + s'y)$ כאשר $u', v', r', s' \in \mathbb{Z}$
אז יש פירוק בלתי-אמיתי $f(x,y) = (ux + vy)(rx + sy)$
כאשר $f(x,y)$ פונקציה ריבועית ב-2 משתנים.

משפט: אם $f(x,y)$ פונקציה ריבועית ב-2 משתנים אז $f(x,y)$ יש פירוק לאמיתי
למעשה במקרה של $\Delta \neq 0$ הוא ריבועי שלם.

הערה: נניח פונקציה ריבועית ב-2 משתנים $f(x,y)$ ויהי u מספר טבעי
שאינו כולל גורמים ראשוניים ש-2 חלקה. אז $f(u,v)$ אינו מתפצל
לכמה גורמים ב- $\mathbb{Z}$ ונניח $f(u,v) = u$.

אע"פ: נניח $\Delta \equiv 0, 1 \pmod{4}$ ויהי u מספר שלם.
אז קיימת פונקציה ריבועית ב-2 משתנים $f(x,y)$ המקיימת Δ בריבוע
לכל $x, y \in \mathbb{Z}$ ויש u מספר טבעי שאיננו מתפצל ב- $\mathbb{Z}$ וקיים
כזה $x^2 \equiv \Delta \pmod{4u}$ לכל $x \in \mathbb{Z}$.

הערה: יש פונקציה ריבועית ב-2 משתנים $f(x,y)$ וקיימת פונקציה
אחרת $g(x,y) = f(x,y)u$ כאשר $u \in \text{SL}_2(\mathbb{Z})$ ב- $\mathbb{Z}$ ויש
ואז $g(x,y)$ היא פונקציה ריבועית ב-2 משתנים.

$f(x,y) = (x,y) A \begin{pmatrix} x \\ y \end{pmatrix}, A = A^t$
 $g(x,y) = (x,y) B \begin{pmatrix} x \\ y \end{pmatrix}, B = B^t, B = u A u^t$

אע"פ: (1) ההחלפה $u = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ היא חזקה
ב- $\mathbb{Z} \times \mathbb{Z}$ ל- $\mathbb{Z} \times \mathbb{Z}$.

(2) $x, y \in \mathbb{Z}$ הם זרים $\Leftrightarrow x', y'$ זרים.

נקודות גבול: $f(x,y), g(x,y)$ → ריבועי

$$f(\mathbb{Z} \times \mathbb{Z}) = g(\mathbb{Z} \times \mathbb{Z}) \quad (1) ; \text{כן}$$

לכן: $\begin{cases} g(x,y)=n \\ x,y \in \mathbb{Z} \end{cases} \Rightarrow \begin{cases} f(x,y)=n \\ x,y \in \mathbb{Z} \end{cases}$ (2) $\Rightarrow$ ρ מונוטון

(3) n עצום $\tilde{f}$ ו- n עצום $\tilde{g}$ $\Rightarrow f$ ו- g $\Rightarrow$ ρ מונוטון

$$\begin{cases} f(x,y)=n \\ \gcd(x,y)=1 \end{cases} \Rightarrow \text{יש נקודה ב-} \rho$$

$$\begin{cases} g(x,y)=n \\ \gcd(x,y)=1 \end{cases} \Rightarrow \text{יש נקודה ב-} \rho$$

$\Delta = 0, 1 \pmod{n}$ ונקודות Δ הן ריבועי

($a, c \neq 0$). Δ הוא S של ρ ב- ρ

ריבועי בלבד. Δ הוא S של ρ

ריבועי $f(x,y) = ax^2 + bxy + cy^2$ ב- ρ $\Rightarrow |b| \leq |a| \leq |c|$

נקודות $\Delta = 0, 1 \pmod{n}$, Δ הן ריבועי

אם יש מספר סופי של נקודות ב- ρ הן ריבועי
בלבד. Δ הוא S של ρ

$\Delta < 0$: Δ הוא ρ ; $\Delta < 0$: Δ הוא ρ

$a < 0$: Δ הוא ρ

$\Delta = 0, 1 \pmod{n}$ ו- $\Delta < 0$: Δ הוא ρ

הוא S של ρ ב- ρ הן ריבועי בלבד

$f(x,y) = ax^2 + bxy + cy^2$: Δ הוא S של ρ ב- ρ

ב- ρ : $-a < b \leq a < c$ ו- $0 \leq b \leq a < c$

הוא S של ρ ב- ρ הן ריבועי בלבד

$\Delta < 0$: Δ הוא ρ (חלקי) Δ הן ריבועי

$(x,y) \neq (0,0), x,y \in \mathbb{Z}, \min f(x,y) = a$

$x \neq 0, y \neq 0 \in \mathbb{Z}, \min f(x,y) = a - |b|c$

המסלול המינימלי - בעיה

$$f(x,y) = 6x^2 + 7xy + 5y^2 \quad \text{קוטב:}$$

$$A = \begin{pmatrix} 6 & 3.5 \\ 3.5 & 5 \end{pmatrix} \Rightarrow \begin{pmatrix} 5 & -3.5 \\ -3.5 & 6 \end{pmatrix} \Rightarrow \begin{pmatrix} 5 & 1.5 \\ 1.5 & 4 \end{pmatrix} \quad u = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$$

הוספת שורה ראשונה
לשורה שנייה

$$\Rightarrow \begin{pmatrix} 4 & -1.5 \\ -1.5 & 5 \end{pmatrix} \quad u = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix} \Rightarrow \begin{pmatrix} -1 & -0.5 \\ 0 & 5 \end{pmatrix} \quad u = \begin{pmatrix} -1 & 1 \\ 1 & 2 \end{pmatrix}$$

הערכים המינימליים - קטל

$$g(x,y) = 4x^2 - 3xy + 5y^2$$

חשב $\min_{x,y \in \mathbb{Z}} f(x,y)$, $(x,y) \neq (0,0)$

$$\tilde{f}(x,y) = \alpha x^2 + \beta xy + \gamma y^2 \quad \text{כאשר} \quad \alpha = \min f(x,y)$$

היא תצטרף - המינימום של $f(x,y)$

$$\alpha x^2 + \beta xy + \gamma y^2 = n \quad \text{הערך}$$

הערך המינימלי של $\tilde{f}(x,y)$

$$n < \min \tilde{f}(x,y) \quad \text{הערך המינימלי של} \quad \min \tilde{f}(x,y) = \alpha - |\alpha| + \delta$$

יש לבדוק היעדרות של הצירים.

$$\text{ציר ה-} x: \alpha x^2 = n, \quad \text{ציר ה-} y: \gamma y^2 = n$$

אזרח שגורל היעדרות, נבדל אולם

$$f(x,y) \quad \text{הערך המינימלי של} \quad \tilde{f}(x,y)$$

האם יש מוצא של המסלול המינימלי? m

$$x^2 \equiv m \pmod{4n} \quad \text{ל-} \quad p \quad \text{הערך המינימלי של} \quad p$$

$$\# \quad h(d) = 1 \quad \text{הערך המינימלי של} \quad d$$

$$\beta \text{ יש המסלול המינימלי של} \quad \Delta = d$$

$$\text{הערך המינימלי של} \quad d = \Delta - b^2 - 4ac \leq -3ac$$

$$ac \text{ מספרים: } a, b, c$$

$$\text{צריך לבדוק כי המקרים} \quad -a < b < a < c \quad \text{ול-} \quad 0 \leq b \leq a = c$$

