

שאלה: פתרו את $x^2 + y^2 = n$ → פתרון

$x^2 + y^2 = n$

\uparrow \uparrow \uparrow

P.N.R.U. \uparrow \uparrow \uparrow

P.N.R.U. \uparrow \uparrow \uparrow

P.N.R.U. \uparrow \uparrow \uparrow

התחברים ונר ג'אוס:

$$\mathbb{D}(i) = \{r + s\sqrt{-1} : r, s \in \mathbb{Q}\} \quad . i = \sqrt{-1}$$

$$\mathbb{D}(i) \subseteq \mathbb{C} \quad \text{המרוכבים}$$

$$\mathbb{Z}(i) = \{m + ni : m, n \in \mathbb{Z}\} \quad \text{השלמים של ג'אוס}$$

$$z = r + si \in \mathbb{D}(i) \quad \text{סוגר תחת חיבור}$$

$$w = u + vi$$

↓

$$z + w = (r + u) + (s + v)i$$

$$r + u \in \mathbb{Q}$$

$$s + v \in \mathbb{Q}$$

$$z \pm w \in \mathbb{D}(i) \quad \text{אם}$$

$$i^2 = -1 \quad z \cdot w \in \mathbb{D}(i) \quad \text{סוגר תחת כפל}$$

$$z \cdot w = (r + si)(u + vi) = ru + rvi + sui - sv = (ru - sv) + (rv + su)i$$

$\frac{1}{z} \in \mathbb{D}(i)$ מנסה, $\mathbb{D}(i)$ הוא $\mathbb{Z}(i)$, נומר: כל $z \in \mathbb{D}(i)$ ו-0 השני

$$\frac{1}{z} = \frac{\bar{z}}{z \cdot \bar{z}} = \frac{r - si}{(r + si)(r - si)} = \frac{r - si}{r^2 + s^2}$$

$$z = r + si \quad \text{כברוק}$$

$$\text{Re}\left(\frac{1}{z}\right) = \frac{r}{r^2 + s^2}$$

כומר

$$\text{Im}\left(\frac{1}{z}\right) = \frac{-s}{r^2 + s^2} \in \mathbb{Q}$$

השלמים של ג'אוס מרוכבים $\mathbb{Z}(i)$, נומר סגור תחת חיבור/חיבור (כל)

אבל לא כל שלם של ג'אוס הוא הסך ה- $\mathbb{Z}(i)$. (כל $\frac{1}{2} \notin \mathbb{Z}(i)$, $\frac{1}{2} \in \mathbb{D}(i)$)

$$N(z) = z \cdot \bar{z} = |z|^2 \quad \text{ונומר: } N: \mathbb{C} \rightarrow \mathbb{R} \quad \text{מוכרם ע'היות}$$

$$N(z) = x^2 + y^2 \quad z = x + iy$$

$$z = 0 \Leftrightarrow N(z) = 0 \quad \text{כמו כן: } N: \mathbb{Z}(i) \rightarrow \mathbb{Z}_+, \quad N: \mathbb{D}(i) \rightarrow \mathbb{Q}_+$$

$$N(zw) = N(z) \cdot N(w) \quad \text{כומר: ה- N היא כפ'ית}$$

$$\overline{z \cdot w} = \bar{z} \cdot \bar{w} \quad \text{(תבוק 1) : כ'יקרתי יותר פשוט לבדוק שזוהי שומרת על}$$

$$\Rightarrow N(zw) = zw \cdot \overline{zw} = zw \cdot \bar{z} \cdot \bar{w} = z\bar{z} \cdot w\bar{w} = N(z) \cdot N(w)$$

! $N(z) \geq 1$ לכל $z \in \mathbb{Z}(i)$ ו-0 $z \neq 0$ של ג'אוס $\neq 0$: (שום צ' שגור שלם של ג'אוס $\neq 0$)

$$\mathbb{Z}[i]^{\times} = \{z \in \mathbb{Z}[i] \text{ s.t. } \exists w \in \mathbb{Z}[i]. zw = 1\} \quad : \text{ההפיכים של } \mathbb{Z}[i]$$

$$\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\} \quad : \text{ההפיכים של } \mathbb{Z}[i] \leftarrow \mathbb{Z}^{\times} = \{\pm 1\} \quad : \text{ההפיכים של } \mathbb{Z}$$

(הוכחה)

אם $z \in \mathbb{Z}[i]^{\times}$ אז $z \cdot \bar{z} = 1$ כי $N(z) = 1$

$$N(z) \cdot N(\bar{z}) = N(z\bar{z}) = N(1) = 1$$

עבור $N(z) = 1$ אז $N(\bar{z}) = 1$ ולכן $N(z) \in \mathbb{Z}^{\times} = \{\pm 1\}$

$$N(z) = x^2 + y^2 = 1 \quad (z = x + iy) \quad : N(z) = 1 \quad \text{עם } z \in \mathbb{Z}[i]$$

כאשר $x^2 \geq 1, y^2 \geq 1 \Rightarrow x^2 + y^2 \geq 2$

$$\begin{aligned} z = \pm 1 &\Leftrightarrow x^2 = 1, y^2 = 0 \\ z = \pm i &\Leftrightarrow x^2 = 0, y^2 = 1 \end{aligned}$$

חלוקה עם שאריות - $\mathbb{Z}[i]$

משפט: אם $A, B \in \mathbb{Z}[i]$ אז קיימת חלוקה $A = QB + R$

כאשר $N(R) < N(B)$

$$N(R) < N(B) = 2 \quad \Leftrightarrow \text{קיימת } A = QB + R \quad \text{פ.ד.ח.} \quad \begin{matrix} A = 5+i \\ B = 1+i \end{matrix}$$

$$A = QB + R \Leftrightarrow \frac{A}{B} - Q = \frac{R}{B}$$

$$\frac{A}{B} = \frac{5+i}{1+i} = \frac{(5+i)(1-i)}{(1+i)(1-i)} = \frac{6-4i}{2} = 3-2i \in \mathbb{Z}[i]$$

לכן $B|A$ כי $R=0$

$$\frac{A}{B} = \frac{5+i}{2+i} = \frac{(5+i)(2-i)}{(2+i)(2-i)} = \frac{11-3i}{5}$$

$$N(R) < N(B) = 5 \quad \begin{matrix} A = 5+i \\ B = 2+i \end{matrix}$$

$$Q = \left(\frac{11}{5}\right) + \frac{1-3i}{5}$$

$$R := A - QB, \quad Q = 2$$

$$\sqrt{N(R) = 2 < 5}, \quad R = (5+i) - 2(2+i) = 1-i$$

כי $N(R) < N(B)$

$$A = 2 \cdot C + (1-i)$$

הוכחה

הוכחה: $A = QB + R, Q, R \in \mathbb{Z}[i], A, B \in \mathbb{Z}[i]$

$$m, n \in \mathbb{Z} \text{ פ.ד.ח. } r, s \in \mathbb{R}, \frac{A}{B} = r + si \quad : \text{כתיוב}$$

$$\begin{cases} Q := m + ni \in \mathbb{Z}[i] \\ R := A - BQ \in \mathbb{Z}[i] \end{cases} \quad \begin{cases} |r-m| \leq 1/2 \\ |s-n| \leq 1/2 \end{cases}$$

$$R = A - QB = B \left(\frac{A}{B} - Q \right)$$

כי $N(R) < N(B)$

$$N(R) = N(B) \cdot N\left(\frac{A}{B} - Q\right) \rightarrow N\left(\frac{A}{B} - Q\right) = N((r-m) + (s-n)i) = (r-m)^2 + (s-n)^2 \leq \frac{1}{2} + \frac{1}{2} = 1 < 1$$

תמונת תחום 19

⚠️ הפונקציה $N: R \rightarrow \mathbb{Z}_+$ "נוכחה" על R היא "תחום שטוח" מורכב

התקיים (1) $N(z) \neq 0$ $\forall z \in R, z \neq 0$ $N(0) = 0$

(2) $A, B \in R$ מתקיים: $A = QB + R$ $\exists Q, R \in R, R \neq 0$ $N(R) < N(B)$ $\vee R=0$

① $N(a) = |a|$ \mathbb{Z}
 ② $N(z) = z \cdot \bar{z}$ \mathbb{C}
 ③ $N(f) = \deg f$ $F[x]$ F שדה

הכפלה: $\mathbb{Z}[i]$ - D $A, B \in \mathbb{Z}[i]$ $B|A$ $\forall A, B \in \mathbb{Z}[i]$ $A = B \cdot C$ $C \in \mathbb{Z}[i]$

חיתוך חשופה: $A, B \in \mathbb{Z}[i]$ $D \in \mathbb{Z}[i]$ D מחלק משותף של A, B $\forall A, B \in \mathbb{Z}[i]$

חיתוך חשופה מקסימלי של A, B הוא D המקסימלי $\leftarrow \text{GCD}(A, B)$

(1) $D|A, D|B$ D מחלק משותף

(2) "מקסימלי": $d \nmid D$ $d|A, d|B$

משפט: $\mathbb{Z}[i]$ - D $\text{GCD}(A, B)$ של $A, B \in \mathbb{Z}[i]$ $\neq 0$ (כלל בוקר יחיד)

③ $\text{GCD}(A, B)$ $\neq 0$ \exists $\pm i, \pm 1$ $\text{GCD}(A, B) \cdot \epsilon = \text{GCD}(A, B)$ $\epsilon \in \{1, -1, i, -i\}$

④ יש $u, v \in \mathbb{Z}[i]$ $u, v \neq 0$ $\text{GCD}(A, B) = uA + vB$ "תורת Bezout"

הוכחה:

כמו "אויזטו" $I = \langle A, B \rangle = \{uA + vB \mid u, v \in \mathbb{Z}[i]\}$ $I + I \subseteq I$ (1) אזי

(2) $\mathbb{Z}[i] \cdot I \subseteq I$ $(r(uA + vB) = ruA + rvB)$

נתה $D \in I, D \neq 0$ עם נורמה מינימלית (נשים לב $A = 1A + 0B$ $B \in I$)

טבעי: $I = \mathbb{Z}[i] \cdot D = (D)$ D "זכר" את האיזוטו I

תוצא $(D) \subseteq I$ D זכר $C \in I$ $C = QD$ $Q \in \mathbb{Z}[i]$ $I \subseteq (D)$ D כושר

כאשר $Q \in \mathbb{Z}[i]$ $I \subseteq (D)$ D כושר

נתק את C - D עם שארית $C = QD + R$ $R=0$ Q ומו $C|D$ D שולבו

או $0 < N(R) < N(D)$ $R \in I$ $R = C - QD \in I$ $R=0$ $C = QD$

וכן $N(R) < N(D)$ $R=0$ D כושר

\checkmark $C|D$ $R=0$ \iff

$D = \text{GCD}(A, B)$ \iff $A, B \in I = (D)$ \iff $A = Q_1 D, B = Q_2 D$ D כושר

מחלק משותף (ראה שיקבעו): $D = uA + vB$ $A = S_1 d, B = S_2 d$ $D = uA + vB$

\checkmark $d|D \iff D = uA + vB = uS_1 d + vS_2 d = (uS_1 + vS_2)d$ D כושר

נותר להוכיח את ② - נהפכות שהיא יחיד עם כזו בהפך.

נניח D_1, D_2 הם $\text{GCD}(A, B)$. אז $D_1 \mid D_2$ ויש $D_2 = xD_1$ וכן $D_2 \mid D_1$ יש $D_1 = yD_2$.

□ $xy \in \mathbb{Z}[i]^{\times} \iff 1 = xy \iff D_1 = yx \cdot D_1 \iff D_1 = y \cdot D_2, D_2 = xD_1 \iff$

ליק מובילים $\text{GCD}(A, B)$? מסמך המוצגות של אוקלידס.

$$\left(\begin{array}{l} R_{n+1} = \text{GCD}(A, B) \iff \\ A = Q_1 B + R_1 \\ B = Q_2 R_1 + R_2 \\ \vdots \\ R_{n-1} = Q_n R_n + R_{n+1} \\ R_n = Q_{n+1} R_{n+1} \end{array} \right)$$

$\frac{A}{B} = \frac{5-i}{5+i} = \frac{2A-10i}{20} = \frac{2}{1} + \frac{-2-10i}{20}$: $\frac{A}{B}$: $\frac{A}{B}$
 $A = 5-i, B = 5+i$

$R_1 = A - Q_1 B = 5-i - 5-i = -2i \Rightarrow A = B - 2i$

$\frac{B}{R_1} = \frac{5+i}{-2i} = \frac{-2+10i}{4} = -\frac{1}{2} + 2\frac{1}{2}i = \frac{2}{2i} + (-\frac{1}{2} + \frac{1}{2}i)$

$R_2 = B - Q_2 R_1 = 5+i + 4 = 1+i \Rightarrow B = 2i R_1 + (1+i)$

$\frac{R_1}{R_2} = \frac{-2i}{1+i} = \frac{-2-2i}{2} = -1-i \Rightarrow R_1 = (-1-i)R_2$

$R_2 = 1+i = \text{GCD}(5-i, 5+i)$ (המספרים)

$A = 5-i = (2-3i)(1+i)$
 $B = 5+i = (3-2i)(1+i)$

$\pi = AB$ פה $\pi \neq 0, \pi \neq 1$ פה $\pi \in \mathbb{Z}[i]$ (הזכרתי)

$(A, B \in \mathbb{Z}[i])$ אם A הפך או B הפך

יש $1+i$ אי פריק. נניח $1+i = A \cdot B$. נחשב (ונראה).

$2 = N(1+i) = N(A \cdot B) = N(A) \cdot N(B)$

$1 = N(A) \iff N(B) = 1$ או $N(A) = 1 \iff N(B) = 1$

משפט סטריי: מספרים רגולריים p (שכזה)

אי פריק $p \equiv 3 \pmod{4} \iff \mathbb{Z}[i]$ אי פריק. π אי פריק. $N(\pi) = p$ (היחיד)

פריק $\iff p = 2$ או $p \equiv 1 \pmod{4} \iff (p = x^2 + y^2) \iff p = 1 \pmod{4}$ או $p = 2$ (צוטעו: $(N=13) 3 \pm 2i, (N=5) 2 \pm i$)

שאלה: האם יש אי פריק עם נורמה 3? $\text{כ} \iff 3 \nmid p$

טענה: 3 אי פריק. סיבה: $9 = N(A) \cdot N(B)$ $\iff 3 \mid N(A)$ או $3 \mid N(B)$ $\iff 3 = N(A)$ או $3 = N(B)$ \iff אי פריק.