

אלגברה מופשטת 2 – הרצאה בנושא השלמים של גאוס

מרצה : אדם צ'פמן (במקום עוזי וישנה).

טענה

הוכח כי $\mathbb{Z}[i]$ הוא תחום פריקות יחידה.

הוכחה

לפי משפט מהרצאה קודמת, עבור $D \in \{-1, \pm 2, \pm 3, 5, -7, -11, 13\}$ הוא O_D הוא אוקלידי. ידוע כי כל תחום אוקלידי הוא תחום ראשי, וכי כל תחום ראשי הוא תחום פריקות יחידה.

משפט (וילסון)

לכל ראשוני p , $(p-1)! \equiv -1 \pmod{p}$.

הוכחה

\mathbb{Z}_p הוא שדה, ולכן למשוואה $x^2 - 1 = 0$ ישנם שני פיתרונות, והם $x = \pm 1$. מאידך, לכל מספר אחר שונה מאפס ב \mathbb{Z}_p יש הופכי השונה ממנו, ולכן במכפלה $(p-1)!$ נקבל זוגות של הופכיים (שמבטלים זה את זה) ואת 1 ו -1 , אז המכפלה יוצאת -1 .

טענה

אם $p \equiv 1 \pmod{4}$ אז קיים $x \in \mathbb{Z}$ כך ש $x^2 \equiv -1 \pmod{p}$.

הוכחה

ניקח $x = \left(\frac{p-1}{2}\right)!$. נשים לב כי $p - k \equiv -k \pmod{p}$ לכל $1 \leq k \leq \frac{p-1}{2}$,

ולכן $(p-1)! \equiv (-1)^{\frac{p-1}{2}} x^2 = x^2$.

טענה

לכל ראשוני $\pi \in \mathbb{Z}[i]$, $N(\pi)$ הוא ראשוני טבעי או ריבוע של ראשוני כזה.

הוכחה

המספר $N(\pi)$ מתפרק למכפלה של ראשוניים טבעיים $p_1 \cdot \dots \cdot p_t$ [עם אפשרות

לחזרות]. כלומר $\pi \bar{\pi} = p_1 \cdot \dots \cdot p_t$. כעת, π ראשוני, ולכן קיים $p = p_i$

ראשוני טבעי כך ש $p \mid \pi$. לכן $p^2 \mid N(\pi)$. אולם $N(\pi)$ הוא מספר טבעי ולכן

$N(\pi) \in \{1, p, p^2\}$. לא בא בחשבון משום שאז π היה הפיך.

טענה

ראשוני טבעי p שונה מ-2 הוא ראשוני ב $\mathbb{Z}[i]$ אם ורק אם $p \equiv -1 \pmod{4}$.

הוכחה

אם לא מתקיים $p \equiv -1 \pmod{4}$ זה אומר בהכרח ש $p \equiv 1 \pmod{4}$, ואז קיים

$1 \leq x \leq p-1$ כך ש $x^2 \equiv -1 \pmod{p}$, ואז $x^2 + 1 = (x+i)(x-i)$. אולם

בגלל ש x לא מתחלק ב p , לא יכול לחלק את אף אחד מהאיברים במכפלה,

ולכן p לא ראשוני.

מאידך, אם p לא ראשוני אזי הוא מתפרק למכפלת ראשוניים $\pi_1 \cdot \dots \cdot \pi_t$. אולם,

הנורמה של כל אחד מהם צריכה להיות ראשוני טבעי או ריבוע של ראשוני טבעי,

ולכן האופצייה היחידה היא ש p הוא מכפלה של שני ראשוניים שהנורמה של

שניהם היא p , ולבפרט זה אומר שהם צומדים אחד של השני, כלומר קיים π

ראשוני כך ש $\pi\bar{\pi} = p$. כעת, $\pi = a + bi$, לאיזשהם $a, b \in \mathbb{Z}$, ולכן $p = a^2 + b^2$. בהכרח אחד מהם זוגי ואחד אי-זוגי (כי אחרת הסכום הוא זוגי). בה"כ נאמר כי b זוגי, ולכן $4 \mid b^2$, משמע $p \equiv a^2 \pmod{4}$ ולכן $p \equiv 1 \pmod{4}$.

טענה

לכל p ראשוני טבעי כך ש $p \equiv 1 \pmod{4}$, קיים פיתרון יחיד למשוואה $p = a^2 + b^2$ כאשר $a, b \in \mathbb{Z}$.

הוכחה

לכל $a, b \in \mathbb{Z}$ המקיימים $p = a^2 + b^2$, מתקיים $p = x\bar{x}$ כאשר $x = a + bi$. אולם, קיים (לפי מה שראינו) ראשוני π כך ש $\pi\bar{\pi} = p$, ומדובר בתחום פריקות יחידה, ולכן בה"כ $x = \pi$.

הקריטריון של אוילר

מספר טבעי הוא סכום של שני ראשוניים אם ורק אם בפירוק שלו לגורמים ראשוניים (טבעיים) כל גורם ראשוני ששארית החלוקה שלו ב-4 היא 3 מופיע מספר זוגי של פעמים.

הוכחה

אם $n = a^2 + b^2$ אזי $n = (a + bi)(a - bi)$. כל גורם טבעי ראשוני ששארית החלוקה שלו ב-4 היא 3 הוא ראשוני גם ב- $\mathbb{Z}[i]$, ולכן אם הוא את $a + bi$ או את $a - bi$, אך אם הוא מחלק אחד מהם אז הוא מחלק בהכרח את a ו- b ולכן הוא מחלק גם את השני. משמע, הוא יופיע מספר זוגי של פעמים בפירוק של n לגורמים ראשוניים.

מאיזך, נניח כי $n = p_1 \dots p_t m^2$ כאשר p_1, \dots, p_t הם ראשוניים ששארת החלוקה שלהם ב-4 היא 1. אזי קיימים ראשוניים ב- $\mathbb{Z}[i]$, π_1, \dots, π_t כך ש $p_i = \pi_i \bar{\pi}_i$ לכל $1 \leq i \leq t$. לכן $n = (m\pi_1 \dots \pi_t) \overline{(m\pi_1 \dots \pi_t)}$, ולכן הוא שווה לסכום של שני ריבועים.

טענה

התכונות הבאות שקולות עבור p ראשוני טבעי שונה מ-2:

1. $p \equiv 1 \pmod{4}$.
2. p לא ראשוני ב- $\mathbb{Z}[i]$.
3. יש איבר $x \in \mathbb{Z}[i]$ עם נורמה $N(x) = p$.

הוכחה

ראינו כבר כי 1 שקול ל-2. ראינו גם כי אם p לא ראשוני אז קיים π ראשוני כך ש $\pi \bar{\pi} = p$, וזה אומר ש $N(\pi) = p$. מאיזך, אם קיים $x \in \mathbb{Z}[i]$ כך ש $N(x) = p$, אזי $x\bar{x} = p$ ולכן p לא יכול להיות ראשוני.

משפט

הראשוניים של $\mathbb{Z}[i]$ הם [עד כדי חברות]:

1. $1+i$.
2. הראשוניים הטבעיים ששארת החלוקה שלהם ב-4 היא 3.
3. המספרים $a+bi$ ו $a-bi$ כאשר $a^2 + b^2$ הוא ראשוני טבעי ששארת החלוקה שלו ב-4 היא 1.

הוכחה

זה שאלו ראשוניים ב $\mathbb{Z}[i]$ כבר ראינו. נסביר מדוע אין עוד מלבד אלו. לכל ראשוני π של $\mathbb{Z}[i]$ הנורמה שלו היא ראשוני טבעי או ריבוע שלו. אם היא מספר ראשוני p טבעי שונה מ-2 אז p איננו ראשוני ב $\mathbb{Z}[i]$, כלומר שארית החלוקה של p ב-4 היא 1 ולכן π הוא מקטגוריה 3.

אם π הוא מנורמה p^2 לאיזשהו ראשוני טבעי שונה מ-2 אזי $\pi = p$ בגלל ש $\mathbb{Z}[i]$ תחום פריקות יחידה, ולכן p ראשוני גם ב $\mathbb{Z}[i]$, משמע שארית החלוקה שלו ב-4 היא 3, ולכן π הוא מקטגוריה 2.

לא קיים π ראשוני מנורמה 4 (בגלל פריקות יחידה), אלא מנורמה 2, והוא $1+i$.

[הערה: $1-i = (-i)(1+i)$ ולכן $1-i$ הוא חבר של $1+i$.]