



שלשות פיתגוריות, מספרים מרוכבים, חבורות אבליות ומספרים ראשוניים

אמנון יקותיאל
המחלקה למתמטיקה
אוניברסיטת בן גוריון
amyekut@math.bgu.ac.il

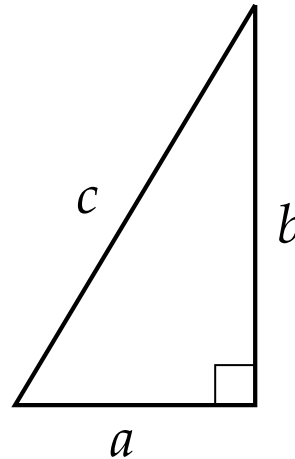
18 בדצמבר 2020

1. שלשות פיתגוריות

שלשה פיתגורית (באנגלית: Pythagorean Triple) היא שלשה (a, b, c) של מספרים שלמים חיוביים, אשר מקיימים את המשוואה

$$a^2 + b^2 = c^2.$$

הסיבה לשם זה היא כי לפי משפט פיתגורס, בהנתן משולש ישר זווית עם בסיס באורך a , אנך באורך b , ויתר באורך c , כולם שלמים, הרי השלשה (a, b, c) הינה פיתגורית.



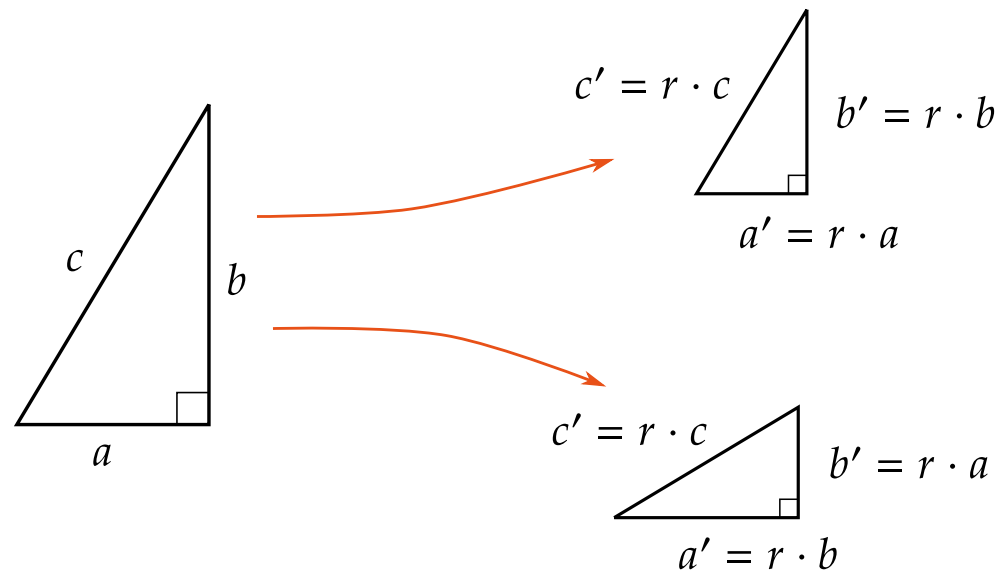
אומרים כי שתי שלשות פיתגוריות (a, b, c) ו- (a', b', c') הן שקולות אם המשולשים המתאימים דומים.

זה אומר שיש מספר ממשי חיובי r כך ש-

$$(a', b', c') = (r \cdot a, r \cdot b, r \cdot c)$$

או

$$(a', b', c') = (r \cdot b, r \cdot a, r \cdot c)$$



קל לראות כי המספר r בעמוד הקודם חייב להיות רציונלי.

הגדרה (1.1). שלשה פיתגורית (a, b, c) נקראת מנורמלת אם מתקיימים התנאים הבאים:

• המחלק המשותף המירבי של שלושת המספרים a, b, c הוא 1.

• $a \leq b$.

תרגיל (1.2). הראה שכל שלשה פיתגורית שקולה לשלשה מנורמלת יחידה.

משום כך אנו נתעניין רק בשלשות פיתגוריות מנורמלות.

תרגיל (1.3). תהי (a, b, c) שלשה פיתגורית מנורמלת. הוכח כי c איזוגי ו- $a < b$.

הנה שאלה מעניינת:

שאלה (1.4). האם יש אינסוף שלשות פיתגוריות מנורמלות?

התשובה היא כן.

דבר זה כבר היה ידוע ליוונים הקדמונים. ישנה נוסחה - מסורבלת מאד ולא יעילה - לחישוב שלשות פיתגוריות מנורמלות. אנו נראה מימוש גיאומטרי של נוסחה זאת בהמשך.

הגדרה (1.5). עבור מספר שלם חיובי c , נסמן ב- $PT(c)$ את קבוצת השלשות הפיתגוריות המנורמלות בעלות יתר c .

ברור שזו קבוצה סופית; אבל יתכן שהיא ריקה!

ניסוח אחר של שאלה (1.4) הוא: האם ישנם אינסוף מספרים שלמים חיוביים c כך שהקבוצה $PT(c)$ איננה ריקה?

תרגיל (1.3) מראה לנו שהקבוצה $PT(c)$ היא ריקה אם c הוא זוגי.

שאלה יותר מעניינת היא זו:

שאלה (1.6). בהנתן מספר שלם חיובי c , מהו גודל הקבוצה $PT(c)$?

שאלה עוד יותר מעניינת היא:

שאלה (1.7). בהנתן מספר שלם חיובי c , האם יש דרך אפקטיבית לחשב את אברי הקבוצה $PT(c)$, כלומר למצוא את כל השלשות הפיתגוריות המנורמלות (a, b, c) עם יתר c ?

במהלך ההרצאה אנו ניתן תשובות חיוביות לשאלות אלו.

אם הזמן יספיק, גם אסביר את ההוכחות.

המומחיות שלי במתמטיקה איננה בתורת המספרים. איך הגעתי לחשוב על שלשות פיתגוריות?

הסיפור הוא זה: בשיחה עם אחיין צעיר שלי עלתה השאלה (1.4), כלומר האם יש אינסוף שלשות פיתגוריות לא דומות.

אני אמרתי לו שנדמה לי שכן, אבל לא ידעתי הוכחה.

במקום לחפש תשובה במקורות, ניסית למצוא הוכחה בעצמי. בתור אתגר.

הערה צדדית: הניסיון המחקרי שלי מראה כי לעתים עדיף לחפש תשובות לבד, בלי חיפוש במקורות. לא תמיד מצליחים למצוא תשובה טובה, אבל מדי פעם כן, ולפעמים מגלים דברים חדשים ומעניינים!

אז חשבתי על הבעיה. די מהר הבנתי את הקשר למספרים מרוכבים על מעגל היחידה (שיוסבר עוד מעט).

יום אחד עלה בדעתי הרעיון של החבורה הכפלית של המעגל. מרעיון זה נובע מייד שיש אינסוף שלשות פיתגוריות לא דומות. אני אדגים את זה בטבלה (3.4).

אחרי זה המשכתי לחקור את הבעייה, והגעתי למשפט (4.5), שהוא פתרון מלא לכל השאלות הקודמות.

בדיעבד התברר לי שחלק מן הדברים שגיליתי היו כבר ידועים, בצורה זאת או אחרת.

בפרט, חיפוש יסודי בספרות היה מספק תשובות לשאלות (1.4) ו-(1.6).

אולם ככל הנראה התשובה שלי לשאלה (1.7), כלומר החישוב האפקטיבי של השלשות הפיתגוריות המנורמלות עם יתר נתון c , הינה חדשה !!!

ההרצאה הנוכחית אמורה לחשוף אתכם לכמה נושאים במתמטיקה שטרם למדתם, ולקשרים ביניהם לבין נושאים שכבר למדתם.

סיבה נוספת למתן ההרצאה הנוכחית היא שאין אפשרות להרצות במסגרת זאת על המחקר שלי.

זה משום הצורך בהרבה ידע מוקדם להבנת נושאי המחקר הללו.

מי שרוצה יכול לעיין ברשימות המאמרים וההרצאות שלי

<http://www.math.bgu.ac.il/~amyekut/publications>

<http://www.math.bgu.ac.il/~amyekut/lectures>



2. מספרים מרוכבים

האבחנה הראשונה היא כי אפשר להצפין שלשות פיתגוריות כמספרים מרוכבים בעלי ערך מוחלט 1.

נתחיל משלשה פיתגורית מצומצמת מסודרת (a, b, c) .

נעבור למספר המרוכב $z := a + b \cdot i$.

הערך המוחלט שלו הוא $|z| = \sqrt{a^2 + b^2} = c$.

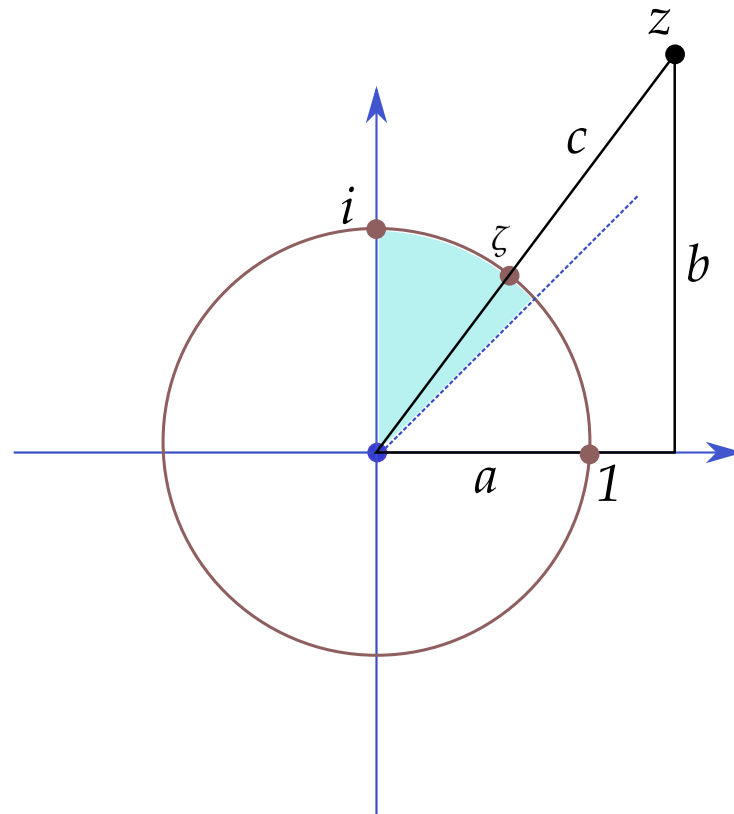
נתבונן במספר המרוכב $\zeta := z/|z|$, אשר מקיים $|\zeta| = 1$.

נגדיר את המספרים הרציונליים $r := \frac{a}{c}$ ו- $s := \frac{b}{c}$.

מקבלים $\zeta = \frac{a}{c} + \frac{b}{c} \cdot i = r + s \cdot i$.

כלומר ζ הוא מספר מרוכב על מעגל היחידה עם רכיבים רציונליים.

מאחר שהשלושה (a, b, c) מנורמלת, הרי המספר ζ נמצא בשמינית השנייה של המעגל.



ציור (2.1)

אפשר לשחזר את המספר המרוכב z , ולכן גם את השלשה הפיתגורית המנורמלת (a, b, c) , בקלות מתוך המספר המרוכב ζ .

עושים זאת ע"י סילוק המכנים מזוג המספרים הרציונליים (r, s) .

אנו רואים שהתהליך הזה נותן התאמה מלאה (פונקציה ביג'קטיבית) בין שתי הקבוצות הבאות:

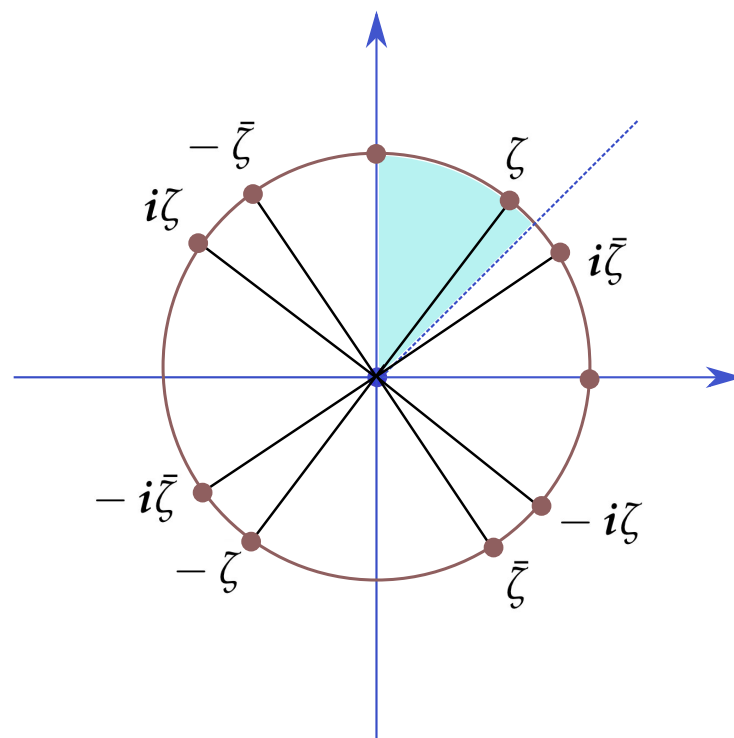
• שלשות פיתגוריות מנורמלות (a, b, c) .

• מספרים מרוכבים ζ עם רכיבים רציונליים בשמינית השניה של מעגל היחידה.



למטרת ספירה יהיה נוח לשנות במקצת את כללי המשחק.

כפי שניתן לראות בציור הבא, כל שלשה פיתגורית מנורמלת מתוארת בדיוק על ידי 8 נקודות שונות עם קואורדינטות רציונליות במעגל היחידה (אחת בכל שמינית).



ציור (2.2)

כל הנקודות הללו מתקבלות מהנקודה ζ על ידי הפעולות הבאות: כפל בחזקה של i והצמדה.

נקרא לשמונה הפעולות האלו הסימטריות הפיתגוריות של המעגל.

מצד שני, כל מספר מרוכב ζ עם קואורדינטות רציונליות במעגל היחידה, מלבד ארבע הנקודות המיוחדות ± 1 ו- $\pm i$, מתאר שלשה פיתגורית מנורמלת, כמו בציור (2.1).

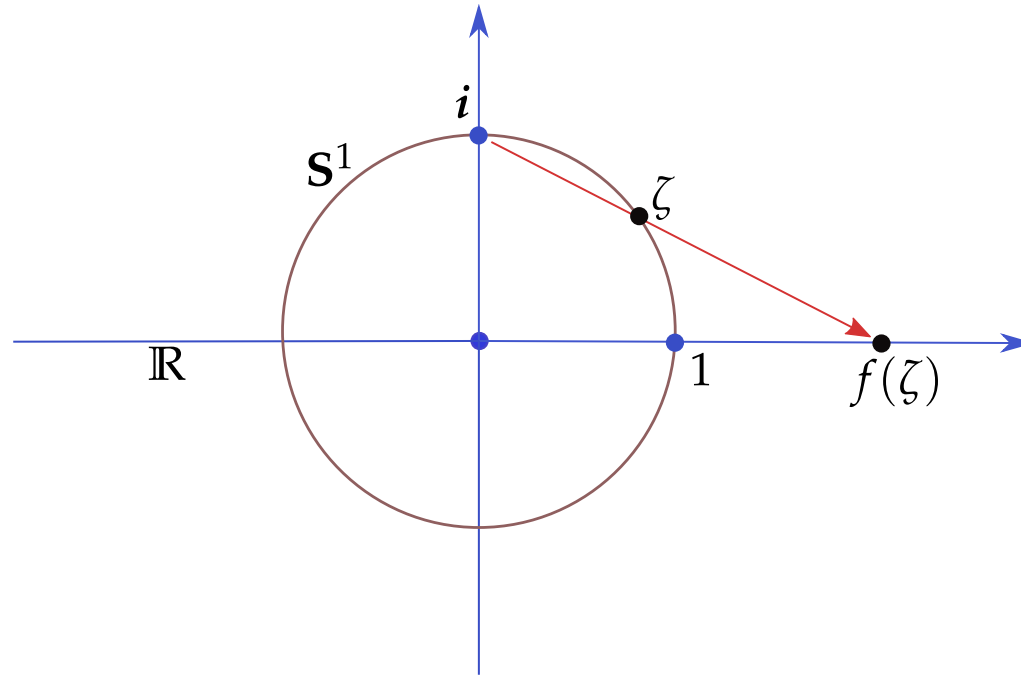
נסמן את השלשה הזאת ב- $pt(\zeta)$.

אם כן, כדי לדעת שיש אינסוף שלשות פיתגוריות מנורמלות, מספיק להראות שיש אינסוף מספרים מרוכבים עם קואורדינטות רציונליות על מעגל היחידה.

כעת אפשר להציג את ההוכחה הגיאומטרית לעובדה הישנה (הידועה עוד מימי היוונים העתיקים) לכך שיש אינסוף שלשות פיתגוריות מנורמלות. כלומר, תשובה חיובית לשאלה (1.4).

נסמן ב- S^1 את מעגל היחידה. נתבונן בהטלה הסטריאוגראפית מהמעגל לישר הממשי, עם מוקד בנקודה i (הקוטב הצפוני).

זו הפונקציה הביג'קטיבית $f : S^1 - \{i\} \rightarrow \mathbb{R}$ השולחת את המספר המרוכב ζ למספר הממשי $f(\zeta)$, הנמצא על הקו הישר המחבר את i ו- ζ . ראו בציור הבא.



ציור (2.3)

תרגיל (2.4). להראות כי למספר המרוכב ζ על מעגל היחידה יש קואורדינטות רציונליות אם"ם המספר הממשי $f(\zeta)$ הוא רציונלי.

מאחר שיש אינסוף מספרים רציונליים, אנו רואים שישנן אינסוף נקודות עם קואורדינטות רציונליות על מעגל היחידה.

הסיפור הזה - אודות מעגל היחידה וההטלה הסטריאוגרפית - כבר היה ידוע מזמן, במאה ה-19 ואולי אף קודם לכן.

אני למדתי על הגישה הזאת מאת איתן בכמט (פרופ' במחלקה למדעי מחשב באב"ג) אחרי שנתתי הרצאה דומה לזאת לפני כמה שנים. (הוא גם הסביר לי את המשמעות של ההטלה הסטריאוגרפית מבחינת גיאומטריה אלגברית, אבל זה לא דבר שמתאים להרצאה שלנו.)

חיפוש באינטרנט היה יכול לגלות לי כבר קודם את הסיפור של ההטלה הסטריאוגרפית. אבל, כאמור, לא חיפשתי...

עד כאן דיברתי על דברים ישנים, אשר אני הייתי אמור לדעת אלמלא הייתי כל כך עצל או בור.

בשקף הבא נעבור לדברים חדשים.



3. החבורה הכפלית של מעגל היחידה

נסמן ב- $G(\mathbb{R})$ את קבוצת המספרים המרוכבים על מעגל היחידה, כלומר

$$G(\mathbb{R}) := \{ \zeta \in \mathbb{C} \mid |\zeta| = 1 \}$$

זו אותה קבוצה אשר קודם סימנו ב- S^1 , אולם כעת רצוי לעבור לסימון החדש. (הערה: הסימון החדש הוא בעל משמעות בגיאומטריה אלגברית.)

הקבוצה $G(\mathbb{R})$ הינה חבורה תחת פעולת הכפל, משום ש-

$$|\zeta_1 \cdot \zeta_2| = |\zeta_1| \cdot |\zeta_2| = 1 \cdot 1 = 1$$

-ו

$$|\zeta^{-1}| = |\zeta|^{-1} = 1^{-1} = 1$$

תהי $G(\mathbb{Q})$ קבוצת האיברים ב- $G(\mathbb{R})$ עם קואורדינטות רציונליות, כלומר

$$G(\mathbb{Q}) := G(\mathbb{R}) \cap \{ s + r \cdot i \mid s, r \in \mathbb{Q} \} \quad (3.1)$$

תרגיל (3.2). הקבוצה $G(\mathbb{Q})$ היא תת-חבורה של $G(\mathbb{R})$. (רמז: לחשב במפורש את הקואורדינטות של $\zeta_1 \cdot \zeta_2$ ו- ζ^{-1} .)

כבר שמנו לב שכדי להראות שיש אינסוף שלשות פיתגוריות מנורמלות, מספיק להראות כי הקבוצה $G(\mathbb{Q})$ היא אינסופית.

אולם כעת ידוע לנו כי לקבוצה $G(\mathbb{Q})$ יש מבנה: היא חבורה אבלית. מבנה זה יתן לנו דרך אחרת לחלוטין למצוא אינסוף איברים ב- $G(\mathbb{Q})$.

תחילה נמצא את האיברים מסדר סופי בחבורה $G(\mathbb{Q})$.

אלו הם שורשי היחידה: האיברים $\zeta \in G(\mathbb{Q})$ המקיימים $\zeta^n = 1$ לאיזה n שלם חיובי.

ידוע כי יש בדיוק ארבעה כאלה: $\pm 1, \pm i$.

זו עובדה מתורת המספרים האלגברית, הקשורה למבנה חוג השלמים של גאוס.

עובדה זאת, וכל מה שנחוץ כדי להבין את פרטי ההרצאה הזו, כולל את ההוכחות, אפשר למצוא בספרי לימוד רבים באלגברה, ובפרט

M. Artin, "Algebra", Prentice-Hall, 1991.

R. Takloo-Bighash, "A Pythagorean Introduction to Number Theory", Springer, 2018.

לכן, אם ניקח איזשהו איבר ζ ב- $G(\mathbb{Q})$ השונה מארבעת שורשי היחידה, הרי תת-החבורה הציקלית שנוצרת על ידי ζ , כלומר הקבוצה $\{\zeta^n \mid n \in \mathbb{Z}\} \subseteq G(\mathbb{Q})$, תהיה אינסופית!

הרי חישוב מפורש.

ניקח את השלשה הפיתגורית המוכרת $(3, 4, 5)$.

היא מיוצגת על ידי המספר המרוכב

$$\zeta_5 := \frac{3}{5} + \frac{4}{5} \cdot i \in G(\mathbb{Q}) \quad (3.3)$$

מאחר ש ζ_5 איננו אחד מארבעת המספרים $\pm 1, \pm i$, הרי הוא איבר מסדר אינסופי.

ננסה לחשב את השלשה הפיתגורית המנורמלת $\text{pt}(\zeta_5^2)$.

תחילה נכפול את המספרים המרוכבים:

$$\zeta_5^2 = \left(\frac{3}{5} + \frac{4}{5} \cdot i\right) \cdot \left(\frac{3}{5} + \frac{4}{5} \cdot i\right) = \frac{-7}{25} + \frac{24}{25} \cdot i$$

באמצעות סילוק המכנה 25 והפעלת אחת מן הסימטריות הפיתגוריות שבציור (2.2) מקבלים את השלשה $(7, 24, 25)$.

בדיקה שזו שלשה פיתגורית:

$$.7^2 + 24^2 = 49 + 576 = 625 = 25^2$$

אכן מצאנו שלשה פיתגורית מנורמלת חדשה!

להלן טבלת החזקות החיוביות הראשונות של ζ_5 , והשלשות הפיתגוריות המנורמלות המתאימות:

$\text{pt}(\zeta_5^n) = (a_n, b_n, c_n)$	ζ_5^n	n
$(3, 4, 5)$	$\frac{3}{5} + \frac{4}{5} \cdot i$	1
$(7, 24, 25)$	$-\frac{7}{25} + \frac{24}{25} \cdot i$	2
$(44, 117, 125)$	$-\frac{117}{125} + \frac{44}{125} \cdot i$	3
$(336, 527, 625)$	$-\frac{527}{625} - \frac{336}{625} \cdot i$	4

טבלה (3.4)

תרגיל (3.5). מצא שלשה פיתגורית מצומצמת מסודרת עם יתר 3,125.

תרגיל (3.6). מה יקרה אם ניקח חזקות שליליות של ζ_5 ?

הערה (3.7). משה נוימן, אשר האזין לגירסה קודמת של הרצאה זו, הפנה את תשומת לבי לכך שהקשר בין שלשות פיתגוריות לבין החבורה הכפלית של המעגל התגלה כבר בשנת 1970 על ידי אולגה טאוסקי.

O. Taussky, Sums of squares, Amer. Math. Monthly 77 (1970), 805-830.

עיון במאמר הזה מראה שאכן המחברת הבחינה בקשר בין הדברים, אולם ההבנה לא היתה מלאה והנוסחאות שם די מעורפלות.

בפרט, לא מופיעה במאמר הזה הדרך האפקטיבית לחישוב השלשות הפיתגוריות, כפי שהיא מוצגת בטבלה (3.4) למעלה ובמשפט (4.5) שבהמשך.



4. מספרים ראשוניים

המפתח למיון המלא של השלשות הפיתגוריות הוא הבנה של תכונות מסויימות של מספרים ראשוניים.

התכונה החשובה של מספר ראשוני p בהקשר שלנו היא שארית של p בחלוקה ב-4.

מסתבר שאם $p \equiv 1 \pmod{4}$, הרי p הוא סכום של שני ריבועים שלמים:

$$p = m^2 + n^2.$$

מאחר ש- p איזוגי, הרי $|m| \neq |n|$. לכן אפשר להניח, בלי הגבלת הכלליות, כי $0 < m < n$.

נגדיר את המספר המרוכב הבא: $q := m + n \cdot i$.

אז המספר הצמוד הוא $\bar{q} = m - n \cdot i$.

חשבון קל מראה שהמספר p מתפרק כמכפלה

$$p = m^2 + n^2 = (m + n \cdot i) \cdot (m - n \cdot i) = q \cdot \bar{q} \quad (4.1)$$

הגדרה (4.2). בהנתן ראשוני p המקיים $p \equiv 1 \pmod{4}$, עם פרוק $p = q \cdot \bar{q}$ כמו בנוסחה (4.1), נגדיר את המספר המרוכב $\zeta_p := q/\bar{q}$.

קל לראות שלמספר המרוכב ζ_p יש קואורדינטות רציונליות וערך מוחלט 1; כלומר זה איבר ב- $G(\mathbb{Q})$.

דוגמה (4.3). ניקח $p = 5$. רואים מייד ש- $5 = 1^2 + 2^2$.

אז $m = 1$, $n = 2$, $q = 1 + 2 \cdot i$, $\bar{q} = 1 - 2 \cdot i$ ו-

$$\zeta_5 = q/\bar{q} = -\frac{3}{5} + \frac{4}{5} \cdot i$$

זה איננו בדיוק המספר ζ_5 שהיה לנו בנוסחה (3.3), אבל אפשר להגיע מאחד לשני באמצעות אחת הסימטריות הפיתגוריות של המעגל, ולכן שניהם מתארים את אותה שלשה הפיתגורית מנורמלת, שהיא $\text{pt}(\zeta_5) = (3, 4, 5)$.



יהי c מספר שלם גדול מ-1.

נזכיר כי הפרוק הראשוני של c הוא

$$c = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} \quad (4.4)$$

כאשר k הוא מספר שלם חיובי, $p_1 < \cdots < p_k$ הם מספרים ראשוניים, ו- n_1, \dots, n_k הם מספרים שלמים חיוביים.

בהגדרה (4.2) התאמנו לכל מספר ראשוני p המקיים $p \equiv 1 \pmod{4}$ את המספר המרוכב ζ_p .

בשקף הבא יופיע המשפט העיקרי שלנו.

משפט (4.5). יהי c מספר שלם גדול מ-1, עם פרוק ראשוני (4.4).

(1). אם מתקיים $p_j \equiv 1 \pmod{4}$ לכל אינדקס j , אז

$$, PT(c) = \left\{ \text{pt}(\zeta_{p_1}^{n_1} \cdot \zeta_{p_2}^{\epsilon_2 \cdot n_2} \cdots \zeta_{p_k}^{\epsilon_k \cdot n_k}) \mid \epsilon_2, \dots, \epsilon_k \in \{\pm 1\} \right\}$$

קבוצה ובה 2^{k-1} איברים שונים.

(2). אחרת, הקבוצה $PT(c)$ היא ריקה.



החישוב ש- $|PT(c)| = 2^{k-1}$ מיוחס לגאוס; ההוכחה שלו לא מוכרת לי.

משפט (4.5) הוא אפקטיבי - כלומר הוא מאפשר בנייה מפורשת של השלשות הפיתגוריות.

דוגמה (4.6). ניקח את המספר $c = 289$.

נשים לב כי $289 = 17^2$ וכי 17 הוא מספר ראשוני המקיים $17 \equiv 1 \pmod{4}$.

לפי המשפט יש בדיוק שלשה פיתגורית מנורמלת אחת עם יתר $c = 289$. ננסה לחשב אותה.

בקלות רואים כי $17 = 1 + 16 = 1^2 + 4^2$,

ולכן $m = 1$, $n = 4$, $q = 1 + 4 \cdot i$, $\bar{q} = 1 - 4 \cdot i$ ו-

$$\zeta_{17} = q/\bar{q} = (q^2)/(q \cdot \bar{q}) = (1 + 4 \cdot i) \cdot (1 + 4 \cdot i) \cdot \frac{1}{17} = -\frac{15}{17} + \frac{8}{17} \cdot i$$

כעת נחשב את ζ_{17}^2 :

$$\zeta_{17}^2 = \left(-\frac{15}{17} + \frac{8}{17} \cdot i\right) \cdot \left(-\frac{15}{17} + \frac{8}{17} \cdot i\right) = \frac{161}{289} + \frac{-240}{289} \cdot i$$

(המשך) השלשה שמקבלים היא

$$\cdot \text{pt}(\zeta_{17}^2) = (161, 240, 289)$$

בדיקה שזו באמת שלשה פיתגורית:

$$\cdot 161^2 + 240^2 = 25,921 + 57,600 = 83,521 = 289^2$$



תרגיל (4.7). מצא את שתי השלשות הפיתגוריות המצומצמות המסודרות עם יתר $c = 65$.

אם ישאר זמן אסקור את ההוכחה של משפט (4.5). אחרת -

$$= \text{סוף} =$$

5. הוכחת המשפט הראשי

המפתח להוכחת משפט (4.5) הינו המשפט הבא על מבנה החבורה האבלית $G(Q)$.

כולכם למדתם (יש לקוות) על המבנה של חבורות אבליות נוצרות סופית.

החבורה $G(Q)$ איננה נוצרת סופית, אולם המבנה שלה דומה: היא מכפלה של חבורה אבלית סופית T ושל חבורה אבלית חופשית F .

אולם החבורה האבלית החופשית F איננה נוצרת סופית - יש לה בסיס בן מניה.

משפט (5.1). החבורה האבלית $G(\mathbb{Q})$ מתפרקת באופן הבא:

$$G(\mathbb{Q}) = T \times F$$

כאן $T = \{\pm 1, \pm i\}$.

החבורה F היא חבורה אבלית חופשית עם בסיס $\{\zeta_{p_j}\}_{j \geq 1}$, כאשר

$$p_1, p_2, p_3, \dots = 5, 13, 17, \dots$$

הם המספרים הראשוניים המקיימים $p_j \equiv 1 \pmod{4}$, ו- ζ_{p_j} הינו המספר המרוכב מהגדרה (4.2) שמתאם לראשוני p_j .



לפני ההוכחה נעיר כי יש אינסוף ראשוניים p המקיימים $p \equiv 1 \pmod{4}$, אולם עובדה זו איננה משפיעה על ההוכחה של המשפט.

הוכחה. החוג $\mathbb{Z}[i]$, שהינו תת-חוג של השדה \mathbb{C} , נקרא חוג השלמים של גאוס.

ידוע כי זה חוג ראשי, האיברים ההפיכים בו הינם אברי החבורה T , והאיברים האי-פריקים בו הם משלושה סוגים:

(א) לכל ראשוני $p \in \mathbb{Z}$ המקיים $p \equiv 1 \pmod{4}$, האיברים q ו- \bar{q} מהגדרה (4.2) הם אי-פריקים, וזרים זה לזה, בחוג $\mathbb{Z}[i]$.

(ב) כל ראשוני $p \in \mathbb{Z}$ המקיים $p \equiv 3 \pmod{4}$ הינו אי-פריק בחוג $\mathbb{Z}[i]$.

(ג) האיבר $1 + i$ הוא אי-פריק בחוג $\mathbb{Z}[i]$.

נשים לב כי לאיבר אי-פריק q בחוג $\mathbb{Z}[i]$ יש ערך מוחלט \sqrt{p} אם הוא מסוג (א); ערך מוחלט p אם הוא מסוג (ב); וערך מוחלט $\sqrt{2}$ אם הוא מסוג (ג).

שדה השברים של החוג $\mathbb{Z}[i]$ הוא $\mathbb{Q}[i]$.

כמו במקרה של השדה \mathbb{Q} , גם כאן כל איבר z שונה מאפס בשדה $\mathbb{Q}[i]$ ניתן לבטא באופן יחיד כמכפלה של איברים אי-פריקים בחוג $\mathbb{Z}[i]$, עם ריבויים חיוביים או שליליים, כפול איבר הפיך בחוג.

כלומר, בהנתן $z \in \mathbb{Q}[i]$, $z \neq 0$, ישנו מספר טבעי יחיד k , איברים אי-פריקים שונים q_1, q_2, \dots, q_k מהסוגים (א), (ב) או (ג), מספרים שלמים e_1, e_2, \dots, e_k השונים מ-0, ואיבר יחיד u מהחבורה T , כך ש-

$$z = u \cdot q_1^{e_1} \cdot q_2^{e_2} \cdots q_k^{e_k} \quad (5.3)$$

יהיה נוח לרשום את הפרוק (5.3) קצת אחרת, לפי מיון האי-פריקים של החוג $\mathbb{Z}[i]$, עם סידור מחדש של המספרים האי-פריקים, ועם הוספת כמה אי-פריקים שאינם מופיעים בפרוק הקודם, עם ריבוי 0.

כך זה נראה:

$$z = u \cdot (1 + i)^c \cdot r_1^{d_1} \cdot \dots \cdot r_l^{d_l} \cdot (q_1^{e_1} \cdot \bar{q}_1^{\bar{e}_1}) \cdot \dots \cdot (q_k^{e_k} \cdot \bar{q}_k^{\bar{e}_k}) \quad (5.4)$$

כאן $1 + i$ הוא האי-פריק מסוג (ג);

r_1, \dots, r_l הם אי-פריקים מסוג (ב);

q_1, \dots, q_k הם אי-פריקים מסוג (א), ו- $\bar{q}_1, \dots, \bar{q}_k$ הם הצמודים שלהם.

אין ב- (5.4) חזרות של אי-פריקים, אבל הריבויים $c, d_1, \dots, d_l, e_1, \bar{e}_1, \dots, e_k, \bar{e}_k$ יכולים להיות 0.

לפי נוסחה (3.1) ברור כי

$$G(\mathbb{Q}) = G(\mathbb{R}) \cap \mathbb{Q}[i] = \{z \in \mathbb{Q}[i] \mid |z| = 1\}$$

ננסה לחקור מה אומר התנאי $|z| = 1$ יחד עם משוואה (5.4).

נזכיר כי $|u| = 1$, $|1+i| = \sqrt{2}$, $|r_i| = r_i$, $|q_i| = |\bar{q}_i| = \sqrt{p_i}$ ו- $p_i = q_i \cdot \bar{q}_i$ כאשר הוא שלם ראשוני.

יהיה מועיל יותר לחשב את הערך המוחלט של z^2 . הרי החישוב לפי נוסחה (5.4):

$$1 = |z| = |z^2| = 1 \cdot 2^c \cdot r_1^{2 \cdot d_1} \cdots r_l^{2 \cdot d_l} \cdot (p_1^{e_1} \cdot p_1^{\bar{e}_1}) \cdots (p_k^{e_k} \cdot p_k^{\bar{e}_k}) \quad (5.5)$$

המכפלה הזאת היא בשדה \mathbb{Q} .

מאחר שהמספרים הראשוניים $2, r_1, \dots, r_l, p_1, \dots, p_k$ כולם שונים, ניתן להסיק כי $d_i = 0$ ו- $\bar{e}_i = -e_i$, $c = 0$.

אם כן, אפשר למחוק את כל האי-פריקים מהסוגים (ב) ו- (ג) בפרוק (5.4). כמו כן אפשר למחוק את כל האי פריקים מסוג (א) עם ריבוי 0.

כל צמד $q_i^{e_i} \cdot \bar{q}_i^{-e_i}$ בפרוק (5.4) עם ריבוי $e_i \neq 0$ אפשר להחליף במספר $\zeta_{p_i}^{e_i}$.

אחרי מיספור מחדש של האי-פריקים שנותרו, כולם מסוג (א), יש לנו פרוק יחיד

$$z = u \cdot \zeta_{p_1}^{e_1} \cdots \zeta_{p_k}^{e_k} \quad (5.6)$$

מש"ל.

עם $k \geq 0$ ו- $e_i \neq 0$.

הוכחת משפט (4.5). ניקח מספר מרוכב $\zeta \in G(\mathbb{Q})$ אשר מייצג שלשה פיתגורית מנורמלת, כלומר $\zeta \notin \{\pm 1, \pm i\}$.

לפי נוסחה (5.6) עם $k \geq 1$, ולפי ההגדרה של הפונקציה pt , בשלשה הפיתגורית המנורמלת $(a, b, c) := pt(\zeta)$ היתר הוא

$$c = p_1^{e_1} \cdots p_k^{e_k}. \quad (5.7)$$

זה מוכיח את סעיף (2) של המשפט.

עבור סעיף (1) של המשפט, נשים לב כי כל עוד איננו משנים את המעריך e_1 , החלפת e_i ב- $-e_i$ עבור כל $i = 2, 3, \dots, k$ תיתן לנו שלשה פיתגורית מצומצת ומסודרת חדשה.

זה בשל הסימטריות הפיתגוריות של המעגל אשר בציר (2.2). ראה גם תרגיל (3.6).

מש"ל.

= סוף =