

שלשות פיתגוריות, מספרים מרוכבים, חבורות אבליות ומספרים ראשוניים

אמנון יקותיאל
המחלקה למתמטיקה
אוניברסיטת בן גוריון
amyekut@math.bgu.ac.il
11/08/2015

0. הקדמה

במאמר זה נציג שיטה לחישוב כל השלשות הפיתגוריות. כפי שהכותרת רומזת, אנו נשתמש במספרים מרוכבים, בתורת החבורות האבליות, ובתכונות של המספרים הראשוניים. ביתר פרוט, התוצאה העיקרית שלנו (משפט 1) הינה תאור המבנה של החבורה הכפלית שאבריה הן הנקודות על מעגל היחידה עם קואורדינטות רציונליות. מתוך תאור זה נקבל איפיון מדויק של כל השלשות הפיתגוריות המצומצמות המסודרות (משפט 2), ואת הנוסחה למספר השלשות הללו בעלות יתר נתון (מסקנה 1).

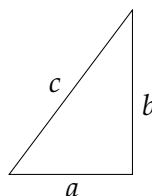
מבחינת הקושי, חלקים 1-2 של המאמר משתמשים רק בתכונות אלמנטריות של המספרים המרוכבים. להבנת חלק 3 יש צורך בהיכרות מסויימת עם חוגים קומוטיביים וחבורות אבליות. להבנת משפט 1 (בחלק 4 של המאמר) צריך לדעת מהי חבורה אבלית חופשית. לא הבאנו הוכחה מלאה של משפט זה, אלא רק תמצית ההוכחה. (כתיבת ההוכחה המלאה של משפט 1 יכולה להיות אתגר מעניין לקוראים!) משפט 2 ומסקנה 1 אמורים להיות מובנים לרוב הקוראים. כמו כן, השתדלנו לתת הסברים מפורטים לבניות השונות המופיעות במאמר.

1. שלשות פיתגוריות

שלשה פיתגורית היא שלשה סדורה (a, b, c) של מספרים שלמים חיוביים, אשר מקיימים את המשוואה

$$a^2 + b^2 = c^2 \quad (1)$$

הסיבה לשם זה היא כי לפי משפט פיתגורס, אלו אורכי הצלעות במשולש ישר זווית. ליתר דיוק, בהנתן משולש ישר זווית עם בסיס באורך a ואנך באורך b , אורך היתר של המשולש הוא c .



אומרים כי שתי שלשות פיתגוריות (a, b, c) ו- (a', b', c') הן **שקולות** אם המשולשים המתאימים דומים. זה אומר שיש מספר חיובי r כך ש-

$$(a', b', c') = (ra, rb, rc) \quad (2)$$

(מתיחת המשולש הראשון פי r), או

$$(a', b', c') = (rb, ra, rc)$$

(מתיחה, והחלפה בין הבסיס והאנך). קל לראות כי המספר r חייב להיות רציונלי.

שלשה פיתגורית (a, b, c) נקראת **מצומצמת** אם המחלק המשותף המירבי של שלושת המספרים הוא 1. השלשה הזאת נקראת **מסודרת** אם $a \leq b$. קל לראות שכל שלשה פיתגורית (a, b, c) שקולה לשלשה מצומצמת ומסודרת יחידה (a', b', c') .

תרגיל 1. תהי (a, b, c) שלשה פיתגורית מצומצמת ומסודרת. אז $a < b$, וכן c הוא איזוגי.

הנה שאלה מעניינת:

שאלה 1. האם יש אינסוף שלשות פיתגוריות מצומצמות ומסודרות?

התשובה היא כן. דבר זה כבר היה ידוע ליוונים הקדמונים. ישנה נוסחה (המיוחסת לאויקלידס) להצגת כל השלשות הפיתגוריות, והיא מראה שיש אינסוף שלשות פיתגוריות מצומצמות ומסודרות. אולם הנוסחה הזאת מסורבלת למדי, ולכן לא נרשום אותה כאן. מי שמעוניין יכול למצוא את הנוסחה הזאת בקלות בחיפוש באינטרנט. לדוגמה:

http://en.wikipedia.org/wiki/Pythagorean_triple
<http://mathworld.wolfram.com/PythagoreanTriple.html>

בהמשך נראה טיעון גיאומטרי יפה, אשר בעצם מתבסס על אותו רעיון כמו הנוסחה הישנה הזאת.

עבור מספר שלם חיובי c , נסמן ב- $PT(c)$ את קבוצת השלשות הפיתגוריות המצומצמות המסודרות בעלות יתר c . ניסוח אחר של שאלה 1 הוא: האם ישנם אינסוף מספרים שלמים חיוביים c כך שהקבוצה $PT(c)$ איננה ריקה? למשל, תרגיל 1 מראה לנו שהקבוצה $PT(c)$ היא ריקה אם c הוא זוגי.

שאלה יותר מעניינת היא:

שאלה 2. בהנתן מספר שלם חיובי c , מהו גודל הקבוצה $PT(c)$?

במאה ה-19 נמצאה נוסחה פשוטה למדי לחישוב הגודל של $PT(c)$. אבל ההוכחה המקובלת עקיפה ומסובכת למדי. אנו נחזור אל הנוסחה הזאת בהמשך - ראו מסקנה 1 בסוף המאמר (אבל ההוכחה שלנו אחרת לחלוטין מזו שבספרות).

שאלה עוד יותר מעניינת היא:

שאלה 3. בהנתן מספר שלם חיובי c , האם יש דרך אפקטיבית לחשב את אברי הקבוצה $PT(c)$, כלומר למצוא את כל השלשות המצומצמות המסודרות (a, b, c) עם יתר c ?

לפני שנים אחדות מצאתי דרך (אולי חדשה - קשה לעקוב אחרי הספרות בנושא הוותיק הזה) אשר עונה בחיוב על כל שלוש השאלות. מטרת המאמר הזה היא להסביר (ללא הוכחות מלאות) את הדרך הזאת.

2. מספרים מרוכבים

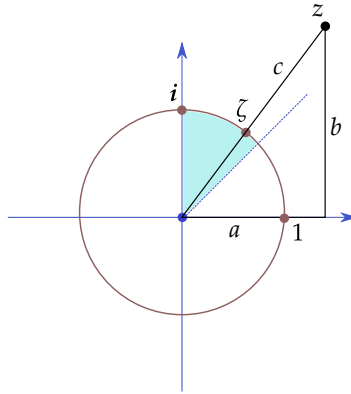
עובדה שהיתה ידועה מזמן, היא כי ניתן להצפין שלשות פיתגוריות כמספרים מרוכבים בעלי ערך מוחלט 1. נתחיל משלשה פיתגורית מצומצמת (a, b, c) . נעבור למספר המרוכב

$$z := a + b \cdot i$$

אשר הערך המוחלט שלו הוא $|z| = c$. נתבונן במספר המרוכב

$$\zeta = r + s \cdot i := \frac{z}{|z|} = \frac{a}{c} + \frac{b}{c} \cdot i \quad (3)$$

זהו מספר מרוכב על מעגל היחידה ברביע הראשון, שונה מ-1 ומ- i , עם קואורדינטות רציונליות $r = \frac{a}{c}$ ו- $s = \frac{b}{c}$. יתר על כן, אנו רואים כי השלשה (a, b, c) הינה סדורה אס"ם המספר המרוכב ζ נמצא בשמינית השניה של מעגל היחידה. ראה ציור 1.



ציור 1

אפשר לשחזר את המספר המרוכב z , ולכן גם את השלשה הפיתגורית (a, b, c) , בקלות מתוך המספר המרוכב ζ . עושים זאת ע"י סילוק המכנים מזוג המספרים הרציונליים $(r, s) = (\frac{a}{c}, \frac{b}{c})$.

בהנתן מספר מרוכב ζ עם קואורדינטות רציונליות במעגל היחידה, השונה מארבע הנקודות המיוחדות $\pm 1, \pm i$, נסמן ב- $pt(\zeta)$ את השלשה הפיתגורית המצומצמת מסודרת היחידה (a, b, c) אשר מתאימה למספר ζ , כלומר שעבורה מתקיימת נוסחה (3).

קיבלנו פונקציה pt מקבוצת המספרים המרוכבים עם רכיבים רציונליים על מעגל היחידה (ללא ארבע הנקודות המיוחדות) אל קבוצת השלשות הפיתגוריות המצומצמות מסודרות. הפונקציה הזאת היא סוראקטיבית (כלומר התמונה היא כל הקבוצה). כל שלשה פיתגורית מצומצמת מסודרת מתקבלת בדיוק 8 פעמים כ- $pt(\zeta)$, מאחר שבדיוק אחד מבין שמונה המספרים

$$\pm \zeta, \pm i \cdot \zeta, \pm \bar{\zeta}, \pm i \cdot \bar{\zeta}$$

נופל בשמינית השניה של מעגל היחידה. כמובן פרט למקרים המיוחדים $\zeta = \pm 1, \pm i$. ראה ציור 2.

מסקנה: כדי להראות שיש אינסוף שלשות פיתגוריות מצומצמות מסודרות, מספיק להראות שיש אינסוף מספרים מרוכבים עם קואורדינטות רציונליות על מעגל היחידה.

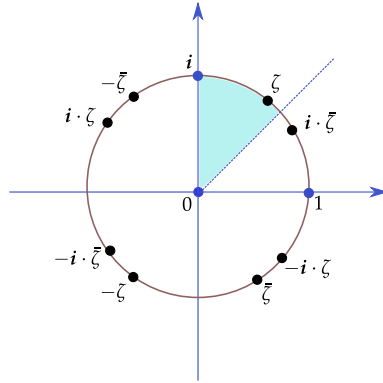
כעת אפשר להציג את ההוכחה הגיאומטרית לעובדה הישנה (הידועה עוד מימי היוונים העתיקים) לכך שיש אינסוף שלשות פיתגוריות מצומצמות מסודרות. כלומר, תשובה חיובית לשאלה 1. נסמן ב- S^1 את מעגל היחידה (הספרה החד-מימדית). נתבונן בהטלה הסטריאוגרפית מהמעגל לישר הממשי, עם מוקד בנקודה i (הקוטב הצפוני), כפי שמתואר בציור 3. זו הפונקציה הביז'קטיבית (חד-חד ערכית ועל)

$$f : S^1 - \{i\} \rightarrow \mathbb{R}$$

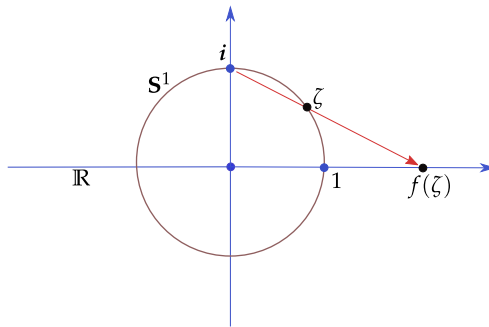
השולחת את המספר המרוכב ζ למספר הממשי $f(\zeta)$, הנמצא על הקו הישר המחבר את i ו- ζ . ראו ציור 3.

תרגיל 2. להראות כי למספר המרוכב ζ על מעגל היחידה יש קואורדינטות רציונליות אס"ם המספר הממשי $f(\zeta)$ הוא רציונלי. (רמז: משולשים דומים.)

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



ציור 2



ציור 3

3. החבורה הכפלית של מעגל היחידה

קודם השתמשנו בסימון S^1 עבור מעגל היחידה. כעת נעבור לסימון אחר לאותה קבוצה, המקובל בגיאומטריה אלגברית, והוא יהיה מועיל יותר עבורנו. מעתה נרשום

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

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

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

-1

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

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

$$G(\mathbb{Q}) := \{ \zeta = s + r \cdot i \mid s, r \in \mathbb{Q}, s^2 + r^2 = 1 \} \subset G(\mathbb{R}) \subset \mathbb{C} \quad (4)$$

זוהי תת-חבורה, כי

$$\begin{aligned} \zeta_1 \cdot \zeta_2 &= (r_1 + s_1 \cdot i) \cdot (r_2 + s_2 \cdot i) \\ &= (r_1 \cdot r_2 - s_1 \cdot s_2) + (r_1 \cdot s_2 + s_1 \cdot r_2) \cdot i \end{aligned}$$

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

טבלה 1

-1

$$\zeta^{-1} = s - r \cdot i$$

כדי לענות בחיוב על שאלה 1 (בדרך אחרת מזו שתוארה קודם לכן), אנחנו נראה כי החבורה האבלית $G(\mathbb{Q})$ היא אינסופית.

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 (מתורת המספרים האלגברית) כי יש בדיוק ארבעה כאלה:

$$1, i, -1, -i \quad (5)$$

לכן, אם ניקח איזשהו איבר ζ בחבורה $G(\mathbb{Q})$ השונה מארבעת המספרים האלו, הרי תת-החבורה הציקלית

$$\{\zeta^n \mid n \in \mathbb{Z}\} \subset G(\mathbb{Q})$$

תהיה אינסופית. הבה נראה שיש איברים כאלה.

ניקח את השלשה הפיתגורית המוכרת (3, 4, 5). האיבר המתאים ב- $G(\mathbb{Q})$ הינו

$$\zeta := \frac{3}{5} + \frac{4}{5} \cdot i \quad (6)$$

מאחר ש- ζ איננו אחד המספרים ב- (5), הרי זהו איבר מסדר אינסופי!

הערה: את החומר הדרוש מתורת המספרים האלגברית, ולמעשה את כל החומר הדרוש להבנת המאמר הזה ולהשלמת ההוכחות, אפשר למצוא בספר

Algebra, by M. Artin, Prentice-Hall.

בטבלה 1 רשמנו את החזקות החיוביות הראשונות של המספר ζ מנוסחה (6), ואת השלשות הפיתגוריות המצומצמות המסודרות המתאימות.

תרגיל 3. מצא שלשה פיתגורית מצומצמת מסודרת עם יתר $c = 3125$. (אחר כך נראה שישנה רק אחת כזאת.)

4. פרוק ראשוני בחוג השלמים הגאוסיים

מטרתנו עתה היא לתאר באופן מלא את המבנה של החבורה האבלית $G(\mathbb{Q})$.

יהי

$$K := \mathbb{Q}[i] = \{s + r \cdot i \mid s, r \in \mathbb{Q}\}$$

זהו תת-שדה של שדה המספרים המרוכבים \mathbb{C} . נוסחה (4) מראה לנו כי

$$G(\mathbb{Q}) = \{\zeta \in K \mid |\zeta| = 1\} \quad (7)$$

יהי

$$A := \mathbb{Z}[i] = \{m + n \cdot i \mid m, n \in \mathbb{Z}\}$$

זהו חוג השלמים הגאוסיים (ring of Gauss integers). השדה K הינו שדה השברים של החוג A . ידוע כי החוג A הינו תחום פריקות יחידה (unique factorization domain). לכן מבנה החבורה הכפלית של השדה הוא

$$K^\times = T \times F \quad (8)$$

כאשר $T := A^\times$ היא החבורה הכפלית של החוג A , ו- F היא חבורה אבלית חופשית, עם בסיס הממוספר על ידי האיברים הראשוניים בחוג A .

את החבורה T כבר מצאנו - זו חבורת שורשי היחידה בנוסחה (5). כלומר

$$T = \{\pm 1, \pm i\} \quad (9)$$

באשר לחבורה החופשית F : חבורת המנה K^\times/T היא חופשית עם בסיס קאנוני, שהוא קבוצת מחלקות השקילות של האיברים הראשוניים ב- A . יש מספר בן מנייה של מחלקות כאלו. עלינו לבחור נציג $q_i \in A \cap K^\times$ מכל מחלקת שקילות. אז מקבלים בסיס

$$\{q_i\}_{i=1,2,\dots}$$

לחבורה חופשית F בתוך K^\times המקיימת את משוואה (8).

המשמעות של האמור למעלה היא שכל מספר שונה מאפס a בשדה K ניתן לביטוי יחיד כמכפלה

$$a = u \cdot \prod_{i=1}^{\infty} q_i^{n_i} \quad (10)$$

כאשר $u \in T$, n_i מספרים שלמים שנקראים הריבויים, ו- $n_i = 0$ מלבד מספר סופי של אינדקסים. (כלומר המכפלה היא סופית.)

אנו רוצים לתת תיאור דומה של תת-החבורה $G(\mathbb{Q})$. תחילה עלינו לדעת יותר על האיברים הראשוניים בחוג השלמים הגאוסים A . מסתבר שהם מתחלקים לשלושה סוגים.

המספר

$$q := 1 + i$$

הינו ראשוני, והוא המחלק היחיד (עד כדי כפל ב- T) של הראשוני הרציונלי 2. הרי החישוב:

$$q^2 = (1 + i)^2 = 1 + i^2 + 2 \cdot i = 2 \cdot i \in 2 \cdot T$$

כעת ניקח ראשוני רציונלי p , כלומר איבר ראשוני בחוג \mathbb{Z} , המקיים

$$p \equiv 3 \pmod{4}.$$

לדוגמה $p = 3$ או $p = 7$. מסתבר שהמספר p נותר ראשוני גם בחוג A . זהו הסוג השני של איברים ראשוניים בחוג A .

לבסוף ניקח ראשוני רציונלי p המקיים

$$p \equiv 1 \pmod{4}. \quad (11)$$

לדוגמה $p = 5$ או $p = 13$. כאן ידוע שיש שני איברים ראשוניים בחוג A , צמודים אחד לשני, אבל לא שקולים אחד לשני על ידי כפל ב- T , נאמר q ו- \bar{q} , כך ש-

$$p = u \cdot q \cdot \bar{q} \quad (12)$$

עבור איזה $u \in T$. האיברים q ו- \bar{q} אשר מתקבלים כך הם הסוג השלישי של איברים ראשוניים בחוג A .

יש דרך קלה למדי למצוא את הפרוק הראשוני (12). ידוע כי ראשוני רציונלי חיובי p אשר מקיים את משוואה (11), הוא סכום של שני ריבועים שלמים:

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

אז לוקחים

$$q := m + n \cdot i, \quad \bar{q} := m - n \cdot i$$

בהנתן ראשוני רציונלי p המקיים את משוואה (11), עם פירוק ראשוני בחוג A כמופיע בנוסחה (12), נגדיר

$$\zeta := q/\bar{q} \in K \quad (13)$$

מנוסחה (7) רואים כי $\zeta \in G(\mathbb{Q})$. אם נחליט שנבחר את ζ בתוך השמינית השנייה של מעגל היחידה, הוא יהיה מוגדר בצורה יחידה.

ידוע כי ישנם אינסוף מספרים ראשוניים רציונליים p מטיפוס (11). נמספר אותם לפי סדר עולה:

$$p'_1 := 5, \quad p'_2 := 13, \quad p'_3 := 17, \dots$$

לכל ראשוני כזה p'_j ניקח את הפרוק הראשוני שלו

$$p'_j = u'_j \cdot q'_j \cdot \bar{q}'_j$$

בחוג A , ונגדיר את המספר

$$\zeta'_j := q'_j/\bar{q}'_j \in G(\mathbb{Q}) \quad (14)$$

הרי התוצאה העיקרית של המאמר.

משפט 1. החבורה $G(\mathbb{Q})$ הינה מכפלה

$$G(\mathbb{Q}) = T \times F'$$

כאשר $T = \{\pm 1, \pm i\}$ היא חבורת שורשי היחידה, ו- F' היא חבורה אבליית חופשית עם בסיס הסדרה

$$\{\zeta'_j\}_{j=1,2,\dots}$$

מנוסחה (14). במלים אחרות, כל איבר ζ בחבורה $G(\mathbb{Q})$ ניתן לביטוי יחיד כמכפלה

$$\zeta = u \cdot \prod_{j=1}^{\infty} \zeta_j^{n_j}$$

כאשר $u \in T$, n_j מספרים שלמים, ו- $n_j = 0$ מלבד מספר סופי של אינדקסים.

תמצית ההוכחה. ניקח מספר ζ שונה מאפס בשדה K המקיים $|\zeta| = 1$. נפתח אותו לפי הפרוק הראשוני בנוסחה (10). לכל ראשוני q_i בחוג A נחשב את $|q_i| \in \mathbb{R}$. מתוך המשוואה $1 = \prod_{i=1}^{\infty} |q_i|^{n_i}$ נובע כי הראשוניים q_i בחוג A אשר אינם באים בזוגות חייבים להופיע עם ריבוי $n_i = 0$. הראשוניים שבאים בזוגות, כלומר אלו שמקיימים את נוסחה (12), חייבים להופיע עם ריבויים מנוגדים, כלומר כחזקה של המספר ζ המתאים.

נזכיר כי עבור מספר מרוכב $\zeta \in G(\mathbb{Q}) - T$ או מסמנים ב- $\text{pt}(\zeta)$ את השלשה הפיתגורית המצומצמת הסדורה המתאימה, כפי שהוסבר בחלק 2 של המאמר.

משפט 2. יהי c מספר שלם גדול מ-1, עם פרוק ראשוני

$$c = p_1^{n_1} \cdots p_k^{n_k}$$

בחוג \mathbb{Z} , כאשר $p_1 < \cdots < p_k$ מספרים ראשוניים חיוביים; n_1, \dots, n_k מספרים שלמים חיוביים; ו- k הוא מספר שלם חיובי.

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

$$\{\pm 1\}^{k-1} \rightarrow \text{PT}(c),$$

$$(\epsilon_2, \dots, \epsilon_k) \mapsto \text{pt}(\zeta_1^{n_1} \cdot \zeta_2^{\epsilon_2 \cdot n_2} \cdots \zeta_k^{\epsilon_k \cdot n_k})$$

היא ביז'קטיבית. כאן ζ_j הינו המספר שמוגדר בנוסחה (13) עבור הראשוני p_j .

2. אחרת, הקבוצה $\text{PT}(c)$ היא ריקה.

תרגיל 4. להוכיח את משפט 2. (רמז: להתבסס על משפט 1, ולחשב את הסימטריות שבציור 2.)

מסקנה ישירה ממשפט 2 היא התוצאה הבאה, אשר מוכרת מן הספרות; ראה לדוגמה הערך

<http://mathworld.wolfram.com/PythagoreanTriple.html>

מסקנה 1. יהי c מספר שלם גדול מ-1, עם פרוק ראשוני כמו במשפט 2.

1. אם מתקיים $p_j \equiv 1 \pmod{4}$ לכל אינדקס j , אז מספר השלשות הפיתגוריות המצומצמות המסודרות עם יתר c הוא 2^{k-1} .

2. אחרת, אין שלשות פיתגוריות מצומצמות מסודרות עם יתר c .

משפט 2 הוא קונסטרוקטיבי - כלומר הוא מאפשר בנייה של השלשות הפיתגוריות. לדוגמה:

תרגיל 5. מצא את שתי השלשות הפיתגוריות המצומצמות המסודרות עם יתר $c = 65$.