שלשות פיתגוריות ותורת החבורות

אמנון יקותיאלי

16.10.2010

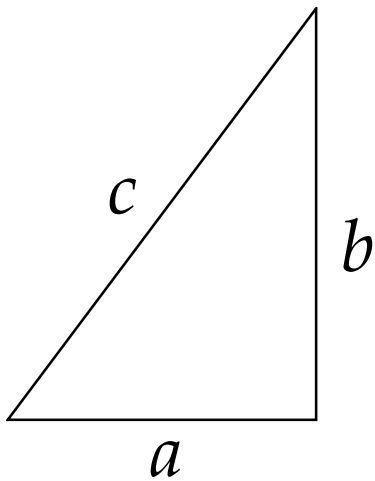
1. שלשות פיתגוריות

שלשה פיתגורית 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, אלו אורכי הצלעות במשולש ישר זוית.

ליתר דיוק, בהנתן משולש ישר זוית עם בסיס באורך a ואנך באורך b, אורך היתר של המשולש הוא c.


c
b
a

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

זה בעצם אומר שיש מספר חיובי r כך ש־

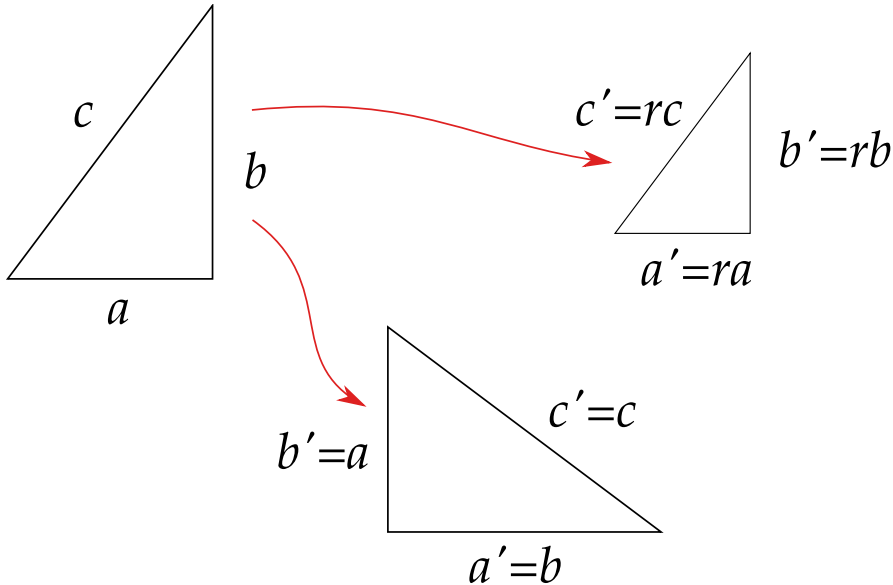
$$(a',b',c') = (ra,rb,rc) \tag{1}$$

(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.


c
b
a
c′=rc
b′=rb
a′=ra
b′=a
c′=c
a′=b

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 שקולה לשלשה מצומצמת ומסודרת יחידה.

כדי לצמצם את השלשה (a,b,c) לוקחים $r := \frac{1}{n}$ במשוואה (1), כאשר n הוא המחלק המשותף המירבי.

תרגיל. תהי (a,b,c) שלשה פיתגורית. אז $a \neq b$.

שאלה מעניינת. האם יש אינסוף שלשות פיתגוריות מצומצמות ומסודרות?

התשובה היא **כן**.

דבר זה כבר היה ידוע ליוונים, ואף ישנה נוסחה (המיוחסת לאויקלידס) למציאת שלשות פיתגוריות.

במאה ה־ 19 נמצאה נוסחה לספירת השלשות הפיתגוריות.

לפני כשנתיים גיליתי דרך לחישוב כל השלשות הפיתגוריות וספירתן. ככל הנראה הגילוי הזה איננו חדש – לפחות חלק מהרעיונות מוכרים בספרות...

יתר ההרצאה יוקדש להסבר של דרך החישוב הזאת.

אפשר לקרוא על תכונות נוספות של שלשות פיתגוריות באינטרנט ב:

Wikipedia: Pythagorean Triple.

2. מספרים מרוכבים

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

נתחיל משלשה פיתגורית מצומצמת (a,b,c).

נעבור למספר המרוכב

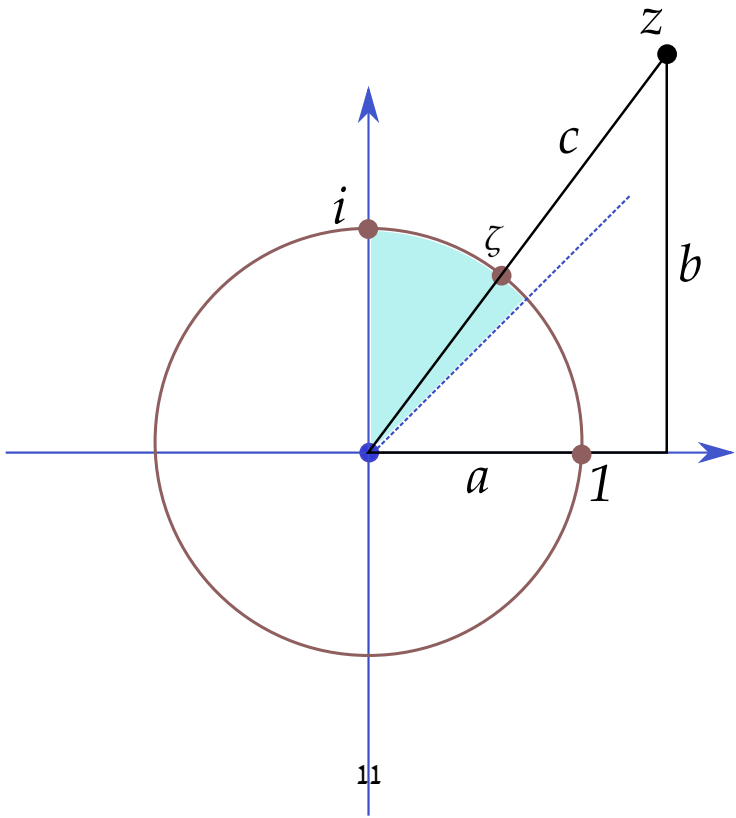
$$z := a + b\boldsymbol{i}$$

אשר הערך המוחלט שלו הוא $|z| = c$.

נתבונן במספר המרוכב

$$\zeta = r + s\boldsymbol{i} := \frac{z}{|z|} = \frac{a}{c} + \frac{b}{c}\boldsymbol{i} \ .$$

זהו מספר מרוכב על מעגל היחידה, עם רכיבים רציונליים.


z
c
i
ζ
b
a
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).

אנו רואים שהתהליך הזה נותן התאמה מלאה בין שתי הקבוצות הבאות:

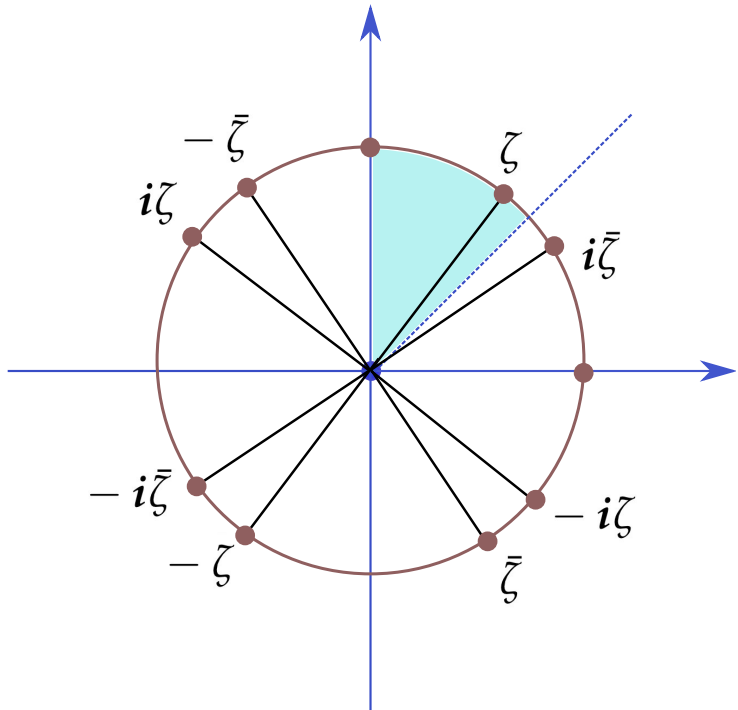
- שלשות פיתגוריות מצומצמות ומסודרות (a,b,c).
- מספרים מרוכבים ζ עם רכיבים רציונליים, בשמינית השניה של מעגל היחידה.

נשים לב כי עבור מספר מרוכב ζ על מעגל היחידה, בדיוק אחד מבין שמונה המספרים

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

נופל בשמינית השניה של מעגל היחידה.

(פרט למקרים המיוחדים $\zeta = \pm 1, \pm\boldsymbol{i}$.)


$-\bar{\zeta}$
ζ
$i\zeta$
$i\bar{\zeta}$
$-i\bar{\zeta}$
$-i\zeta$
$-\zeta$
$\bar{\zeta}$

מסקנה. כדי להוכיח שיש אינסוף שלשות פיתגוריות (מצומצמות ומסודרות), מספיק להראות שיש אינסוף מספרים מרוכבים עם רכיבים רציונליים על מעגל היחידה.

3. החבורה הכפלית של מעגל היחידה

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

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

זוהי חבורה תחת פעולת הכפל, משום ש־

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

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

$$G(\mathbb{Q}) := \{\zeta = s + r\boldsymbol{i} \mid s, r \in \mathbb{Q}\} \subset G(\mathbb{R}) \ .$$

זוהי תת־חבורה, כי

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

ו־

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

ברצוננו להראות כי $G(\mathbb{Q})$ היא חבורה 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 כי יש בדיוק ארבעה כאלה:

$$1, \boldsymbol{i}, -1, -\boldsymbol{i} .$$

לכן, אם ניקח איזשהו איבר ζ השונה מהם, הרי תת־החבורה

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

תהיה אינסופית.

הבה נראה שיש איברים כאלה.

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

$$\zeta := \tfrac{3}{5} + \tfrac{4}{5}\boldsymbol{i} \ .$$

זהו איבר מסדר אינסופי!

להלן טבלת החזקות החיוביות הראשונות, והשלשות הפיתגוריות המתאימות:

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

4. מספרים ראשוניים

יהי

$$\zeta := \tfrac{3}{5} + \tfrac{4}{5}\boldsymbol{i} \ .$$

הטבלה בשקף הקודם מרמזת כי המספר המרוכב ζ^n מייצג שלשה פיתגורית מצומצמת ומסודרת עם יתר 5^n.

מסתבר שההבחנה הזאת נכונה. יתר על כן: יש **בדיוק** שלשה פיתגורית (מצומצמת ומסודרת) אחת עם יתר 5^n.

בעזרת ידע נוסף באלגברה (נדבר על כך קצת בהמשך) אפשר לתאר באופן מלא את המבנה של החבורה $G(\mathbb{Q})$.

משם הדרך קצרה להוכחת המשפט הבא:

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

$$c = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k} .$$

כאן $p_1, \ldots, p_k$ ראשוניים שונים, ו־ $n_1, \ldots, n_k$ שלמים חיוביים.

1. ניתן לחשב בצורה מפורשת את כל השלשות הפיתגוריות המצומצמות הסדורות שיש להן יתר c, מתוך הפירוק הראשוני של c.

2. המספר c מופיע כיתר בשלשה פיתגורית מצומצמת אם ורק אם

$$p_j \equiv 1 \pmod 4$$

לכל j.

3. נניח כי המספר c מקיים את התנאי בסעיף 2. אז מספר השלשות הפיתגוריות המצומצמות הסדורות שיש להן יתר c הינו 2^{k-1}.

ההוכחה עושה שימוש במבנה האלגברי הבא.

נתבונן בקבוצת המספרים

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

זהו תת־חוג של $\mathbb{C}$ הנקרא **חוג השלמים של גאוס**.

בחוג $\mathbb{Z}[\boldsymbol{i}]$ יש פריקות יחידה לגורמים ראשוניים, אשר נקראים **ראשוניים גאוסיים**.

נדגים את סעיף 1 במשפט עבור המספר $c = 13$.

הפרוק הראשוני הוא $c = p_1^{n_1}$, עם $p_1 = 13$, $n_1 = 1$ ו־ $k = 1$.

מאחר של־ 13 יש שארית 1 מודולו 4, הרי הוא סכום של שני ריבועים:

$$13 = 9 + 4 = 3^2 + 2^2 .$$

מכך אפשר לחשב את הפרוק של 13 לגורמים ראשוניים גאוסיים:

$$13 = (3 + 2\boldsymbol{i}) \cdot (3 - 2\boldsymbol{i}) .$$

ניקח את המנה של הגורמים הללו:

$$\zeta := \frac{3+2\boldsymbol{i}}{3-2\boldsymbol{i}} = \frac{5}{13} + \frac{12}{13}\boldsymbol{i} \ .$$

זהו איבר ב־ $G(\mathbb{Q})$ אשר מייצג את השלשה הפיתגורית המצומצמת הסדורה

$$(5, 12, 13) \ .$$

לסיום:

תרגיל. 1. מצא את שתי השלשות הפיתגוריות (המצומצמות הסדורות) שיש להן יתר 65.

2. מצא את השלשה הפיתגורית (המצומצמת הסדורה) היחידה שיש לה יתר 17.

**** סוף ****