משפט פרמה האחרון - דוח התקדמות

מאת: בנימין ווייס - המכון למתמטיקה

דומה כי אין משפט בתורת המספרים שהשפיע על התפתחות תחום זה במאות השנים האחרונות כאותו משפט שניסח פייר פרמה (Pierre Fermat 1601-1665) על הגיליון של ספרו של דיופאנטוס:

בשביל n גדול משלוש אין למשוואה

$$x^n + y^n = z^n$$

פיתרון במספרים שלמים השונים כולם מאפס.

בשביל n = 2, משוואה זאת היא המשוואה המקשרת בין צלעות משולש ישר-זווית (משפט פיתגורס), ואנו מוצאים כבר בכתביהם של הבבלים מהאלף השני לפני הספירה רשימות ארוכות של משולשים כאלה שכל צלעותיהם מספרים שלמים כגון: (3,4;5), (5,12;13),(8,15;17) וכו'. המתמטיקאים היוונים ידעו כיצד למצוא את כל המשולשים "הפיתגוראיים" השלמים, כלומר את כל הפיתרונות במספרים שלמים של המשוואה $x^2 + y^2 = z^2$ (ראה נספח I).

הפיתרון הכללי הנ"ל נמצא (אמנם בצורה אחרת, כי הדגש אצל דיופאנטוס (Diophantus, מאה שלישית) הוא על מספרים רציונליים, ולא על מספרים שלמים) בספרו של דיופאנטוס ח ש ב ו ן, ספר II, בעיה 8. פרמה רשם בעותק שלו של הספר הנ"ל ליד אותו מקום:
"לחלק קוביה לשתי קוביות אחרות, חזקה רביעית או באופן כללי כל חזקה שהיא לשתי חזקות מאותה מעלה הגדולה משתים הוא בלתי אפשרי; אכן מצאתי הוכחה נפלאה לכך, אך השוליים צרים מלהכיל אותה".

עברו מאז למעלה משלוש מאות שנה ולמרות מאמציהם של גדולי המתמטיקאים משך כל התקופה הזאת ה"משפט" הזה של פרמה נשאר בגדר ה ש ע ר ה ב ל ב ד. אמנם, המשפט הוכח בשביל ערכים מסוימים של n. ל n = 4 הגיעה לידינו הוכחה של פרמה עצמו. במאה השמונה עשרה הוכיח אוילר (Euler) את המשפט למקרה n = 3, ובמחצית הראשונה של המאה התשע-עשרה מתמטיקאים כגון לז'נדרה (Legendre), דיריכלה, (Dirichlet),קומר (Kummer) פיתחו טכניקות חדשות שאיפשרו את הוכחת המשפט בשביל ערכים קטנים של n. עד היום, שיטות אלו ואחרות, יחד עם חישובים

נומריים שנעשו בעזרת מחשבים, הביאו לידי הוכחת המשפט לכל n הקטן מ- 100,000 (מספר זה נמצא בספרות מספר שנים, וסביר להניח שהוא כבר שופר). אך אין בכל ההוכחות הללו רמז של הוכחה אפשרית של המשפט בכללותו. במסגרת מאמר זה לא נוכל לסקור את מה שנעשה עד כה, וברצוננו רק לספר על פריצת דרך חדשה בתורת המספרים שנעשתה על-ידי חוקר צעיר G. Faltings, וההשלכות של עבודתו בשביל משפט פרמה. לצורך זה נקדים כמה מלים על משוואות במספרים שלמים.

נתחיל במשוואה ממעלה ראשונה

$$ax + by = c$$

כאשר a,b,c שלמים, ואנו מחפשים פיתרון בשלמים. נניח תחילה שקיים פיתרון (x_0,y_0). אז כל מספר המחלק את a וגם את b, מחלק גם את c, ולכן c חייב להתחלק על-ידי המחלק במשותף המקסימלי של a ו b. אם תנאי זה מתקיים, אזי מסתבר (ראה נספח II) שאכן קיים פיתרון. קל אז לראות שקיים מספר אין-סופי של פיתרונות: כי, אם (x_0,y_0) פותר את המשוואה בשלמים, אז לכל n גם $(x_0 + nb, y_0 - na)$ פותר את המשוואה. במשוואות ממעלה ראשונה בכל מספר של נעלמים, וגם בכל מספר של משוואות התופעה דומה: ישנם תנאים פשוטים ההכרחיים לקיום פיתרון, ואז (אם רק מספר הנעלמים עולה על מספר המשוואות) יש אין-סוף פיתרונות.

כאשר מעלת המשוואה גדולה מאחת, המצב מורכב יותר. לפעמים קיימים אין-סוף פיתרונות בשלמים. למשל, למשוואה

$$x^2 - 2y^2 = 1$$

מכל פיתרון (x_0,y_0) אפשר למצוא פיתרון נוסף על פי הנוסחאות

$$x_1 = 3x_0 + 4y_0 \quad , \quad y_1 = 2x_0 + 3y_0$$

ואם נתחיל בפיתרון (3,2), נקבל ממנו אין-סוף פיתרונות. לעומת זאת, לפעמים קיימים פיתרונות, אך מספרם מוגבל. למשל, למשוואה

$$x^2 + y^2 = 5$$

יש פיתרונות בשלמים - אך כולם נוצרים מ $(\pm1,\pm2)$ ולכן מספרם סופי. ישנן גם משוואות בלי פיתרון בשלמים. למשל

$$x^2 + 3y^2 = 2$$

לפני כחמישים שנה, L.J. Mordell שיער השערה כללית על משפחה רחבה מאוד של משוואות אשר לכל אחת מהן רק מספר סופי של פיתרונות (השערתו מדברת על מספרים רציונליים, אך אנו ממשיכים לנסח את הכל במונחים של שלמים; בהמשך, כאשר נדון בצורה מפורטת יותר בהשערתו, נסביר את הקשר). ב 1984 ג. פלטינגס הוכיח את ההשערה הזאת, וכמסקנה פרטית אחת הוא קיבל את התוצאה דלהלן:

משפט (פלטינגס): לכל $n \geq 3$, יש לכל היותר מספר סופי של פיתרונות בשלמים למשוואה

$$x^n + y^n = z^n$$

אין בתוצאה הזאת כלשונה כדי להוכיח את משפט פרמה אפילו בשביל n אחד, אך בכל זאת אפשר להסיק מכאן מסקנה מפתיעה:

משפט: בשביל כמעט כל מספר טבעי n אין פיתרון בשלמים (השונים כולם מאפס) למשוואה

$$x^n + y^n = z^n$$

את יתרת החלק הזה של הדו"ח נקדיש להבהרת המושג "כ מ ע ט כ ל מ ס פ ר ט ב ע י". בחלק הבא נסביר כיצד משפט זה נובע ממשפט פלטינגס, ובחלק האחרון של המאמר אנו נסביר את ניסוח השערת מורדל.

על משמעות המושג "כמעט כל מספר טבעי" נעמוד תוך כדי ניסיון לענות על השאלה הכללית - כיצד מודדים את הגודל של קבוצה של מספרים טבעיים. אם הקבוצה סופית, אזי אפשר פשוט לספור את איבריה, ומספר זה עונה בוודאי על השאלה. אך אם הקבוצה אין-סופית, אז התחשיב שקנטור פיתח לגדלים אין-סופיים מראה כי לכל הקבוצות האין-סופיות של טבעיים א ו ת ו מ ס פ ר של איברים. למרות תוצאה זאת, כל אחד מרגיש שהקבוצה המכילה רק את המספרים הזוגיים היא ק ט נ ה י ו ת ר מקבוצת כל הטבעיים, ושקבוצת הרבועים $\{1,4,9,16,25,...\}$ קטנה עוד יותר.

כדי לתת ביטוי כמותי לתחושה הזאת, נשנה את השאלה ובמקום לנסות לברר את הגודל המוחלט של הקבוצה, ננסה למדוד את גודלה יחסית לכל הטבעיים. במלים אחרות, במקום השאלה "כמה מספרים זוגיים ישנם", נשאל: "איזה אחוז של כלל המספרים הטבעיים תופסים המספרים הזוגיים". תשובה אחת לשאלה הזאת ניתנת על ידי המושג של צ פ י פ ו ת של קבוצה A. ניעזר במושג הגבול ונגדיר את הצפיפות של A כגבול (בתנאי כמובן שגבול זה קיים) כאשר n שואף לאין-סוף של היחס של מספר איברי A בין 1 ל n, ו n עצמו. בצורה פורמלית יותר, נסמן ע"י c_n את מספר האיברים ב A הנמצאים בין 1 ו n ונגדיר אז

$$\text{צפיפות של } A = \lim_{n\to\infty} \frac{c_n}{n}$$

דוגמאות:

א. אם A המספרים הזוגיים, אזי $c_n = [n/2]$ (כאשר $[b]$ מסמן את השלם הגדול ביותר שאיננו עולה על b), והצפיפות שווה לגבול $\lim_{n\to\infty} \frac{[n/2]}{n}$ השווה ל $1/2$.

ב. באופן כללי, אם A סדרה חשבונית

$$A = \{a_0 , a_0 + d , a_0 + 2d, ...\}$$

אזי הצפיפות של A שווה ל- $1/d$.

ג. את דוגמה ב. אפשר להכליל לכל קבוצה שהיא מחזורית החל ממקום מסויים, כלומר כאשר קיימים a_0 ו d, כך שלכל $k \geq 0$ המשותף של A עם הקטע $[a_0 + kd, a_0 + (k + 1)d)$ הוא הזזה של החתוך של A עם הקטע $[a_0,a_0 + d)$. במקרה זה קל לראות, כי הצפיפות של A שווה לגודל היחסי של A בקטע הבסיסי $[a_0, a_0 + d)$.

ד. אם A קבוצת הריבועים, אזי $[\sqrt{n}] = c_n$ וקל לראות כי $\lim_{n\to\infty} \frac{[\sqrt{n}]}{n} = 0$.

נאמר כעת שתכונה מסוימת מתקיימת כמעט ל כ ל מ ס פ ר ט ב ע י אם לקבוצת הטבעיים שבשבילה היא מתקיימת יש צ פ י פ ו ת א ח ד. למשל:

ה. כמעט כל מספר הוא גדול ממיליון, כי במקרה זה

$$n - 10^6 = c_n$$

ומתקיים

$$\lim_{n\to\infty} \frac{n - 10^6}{n} = 1$$

ו. כמעט כל מספר א י נ נ ו ריבוע, כי במקרה זה $n - [\sqrt{n}] = c_n$, ומתקיים

$$\lim_{n\to\infty} \frac{n - [\sqrt{n}]}{n} = 1$$

(השווה דוגמה ד).

בזה סיימנו את ההסבר של משמעות התוצאה החדשה על משפט פרמה. כעת ידוע, כי הוא נכון כ מ ע ט ל כ ל n . אולם, מידע זה אי-אפשר לקבל תוצאה מפורשת אפילו על n אחד! כל מה שהיא אומרת הוא, שהמשפט נכון למספרים רבים מאוד, אבל מעצם ההוכחה, כפי שנראה בהמשך, אין להסיק יותר.

ספרות:

1) Fermat's Last Theorem, H.M. Edwards, New York, 1977.
2) Solved and Unsolved Problems in Number Theory, D. Shanks, Third Edition, New York, 1985.

נספח I

נשים לב תחילה לעובדה שאם (x_0,y_0,z_0) פיתרון למשוואה $x^2 + y^2 = z^2$, אזי לכל k שלם גם (kx_0,ky_0,kz_0) נותן פיתרון. למשל, מהפיתרון (3,4,5) אפשר לגזור את הפיתרונות (6,8,10) , (9,12,15) , (12,16,20) וכו'.

נותר, אם כן, לתאר את הפיתרונות הבסיסיים, כלומר הפיתרונות שבהם אין מחלק משותף שונה מ 1 ל (x_0,y_0,z_0). מסתבר שבכל פיתרון כזה אחד המספרים x_0,y_0 הוא זוגי. נסדר כך ש y_0 יהיה זוגי, ואז כל פיתרון כזה מתקבל מהנוסחאות

$$x_0 = u^2 - v^2 \ , \ y_0 = 2uv \ , \ z_0 = u^2 + v^2$$

כאשר u,v הם שלמים ללא מחלק משותף. למשל, הפיתרונות (3,4,5) , (5,12,13) (15,8,17) מתקבלים מהזוגות (2,1) , (3,2) , (4,1) בהתאמה.

קל לבדוק שהנוסחאות אמנם נותנות פיתרון של המשוואה. ההוכחה שכל פיתרון מתקבל מנוסחאות אלו איננה קשה ומופיעה בכמעט כל ספר על תורת המספרים. הנה הרעיון העיקרי של ההוכחה: שיקולים פשוטים מראים, כי z_0 אי-זוגי וכי אחד המספרים x_0,y_0 - נאמר x_0 - אי-זוגי, בעוד ש y_0 זוגי - נאמר $y_0 = 2w$. אז קיים

$$w^2 = \frac{z_0^2 - x_0^2}{4} = \left(\frac{z_0 + x_0}{2}\right)\left(\frac{z_0 - x_0}{2}\right)$$

כעת מתברר כי ההנחה שאין מחלק משותף ל x_0,z_0 גוררת כי אין מחלק משותף ל $\frac{z_0 + x_0}{2}$, $\frac{z_0 - x_0}{2}$ ולכן (זאת נקודה הטעונה הוכחה) גם $\frac{z_0 + x_0}{2}$ וגם $\frac{z_0 - x_0}{2}$ ריבועים, והמספרים u,v הם השורשים שלהם.

נספח II

נתבונן במשוואה $ax + by = c$ ונחפש פיתרון לה בשלמים. אם p מחלק את a ואת b ואם קיים פיתרון בכלל, אזי p חייב לחלק גם את c. נחלק ב p ונמשיך עד שנגיע למצב שבו אין ל a ול b מחלק משותף. אז נראה כי למשוואה $ax + by = 1$ יש פיתרון בשלמים. מפיתרון אפשר לקבל פיתרון של המשוואה $ax + by = c$ עם אגף ימני שרירותי על-ידי מכפלה. למטרה זאת נסתכל בקבוצת כל המספרים ה ח י ו ב י י ם שצורתם $an + bm$, כאשר n,m שלמים (גם חיוביים וגם שליליים) ונסמן ב d את הקטן מביניהם. כלומר קיימים שלמים n_0,m_0 כך ש

$$an_0 + bm_0 = d$$

אך לכל שלם $0 < d' < d$ אין בנמצא הצגה כזאת. אנו טוענים כי $d = 1$, וזה נותן לנו את הפיתרון הדרוש.

ואמנם, נניח כי d איננו מחלק את a. אז בוודאי d קטן מ a, ואז אפשר לכתוב את החילוק של a ב d עם שארית

$$a = qd + r$$

כאשר $0 < r < d$. אך אז $a - q(an_0 + bm_0) = r$, $(1 - qn_0)a - qbm_0 = r$ בסתירה להגדרה של d כמספר הקטן ביותר בעל הצורה $an + bm$. באופן דומה רואים כי d מחלק את b, ואז ההנחה שאין ל a ול b מחלק משותף מביאה אותנו למסקנה ש $d = 1$.