משפט פרמה האחרון - דוח התקדמות
(חלק שני)

מאת: בנימין ווייס, המכון למתמטיקה

בחלק הראשון של מאמר זה הבאנו את המשפט של פלטינגס המהווה פריצת דרך חדשה בנסיונות להוכיח את משפט פרמה האחרון.

משפטו של פלטינגס (Faltings) הוא:

מ ש פ ט: לכל $n \geq 3$ יש לכל היותר מספר סופי של פיתרונות פרימיטיביים בשלמים למשוואה $x^n + y^n = z^n$.

נזכיר, כי פיתרון נקראה פ ר י מ י ט י ב י כשאין מחלק משותף למספרים x,y,z. ללא הגבלה זאת אפשר לקבל מכל פיתרון (x_0,y_0,z_0) אין-סוף פיתרונות על-ידי כפל ב-k שלם, כי

$$x_0^n + y_0^n = z_0^n \Rightarrow (kx_0)^n + (ky_0)^n = (kz_0)^n$$

בהחשך, הכוונה תמיד לפיתרונות פרימיטיביים, גם אם אין זה נאמר במפורש.

הסברנו גם את המושג "כמעט כל מספר טבעי", ואמרנו כי אפשר להסיק מהמשפט של פלטינגס את המשפט של פרמה כמעט לכל מספר טבעי. בחלק הזה של המאמר נפרט את המעבר הזה. הרעיון העיקרי מתבטא כבר בטענה הבאה, המראה כיצד משפט על מספר סופי של פיתרונות יכול להביא לתוצאה של חוסר פתרונות.

ט ע נ ה: אם בשביל p מסויים יש למשוואה $x^p + y^p = z^p$ רק מספר סופי של פיתרונות בשלמים, אזי בשביל j מספיק גדול אין למשוואה

$$x^{jp} + y^{jp} = z^{jp} \qquad (*)$$

פיתרונות בשלמים השונים כולם מאפס.

הוכחה: נעיר תחילה, כי אם יש ל (*) פיתרון בשלמים, אזי z הוא בוודאי לכל הפחות 2 (בעצם אפשר להוכיח בקלות כי $jp < z$ - ראה נספח - I - אך החסם הפשוט 2 מספיק לנו כאן). נשים כעת לב לעובדה, שאם (x_0,y_0,z_0) פיתרון של המשוואה (*), אזי $(x_0{}^j,y_0{}^j,z_0{}^j)$ הוא פיתרון למשוואה המקורית $x^p + y^p = z^p$ אם יש רק מספר סופי של פיתרונות למשוואה האחרונה, אזי יש חסם עליון לערכים של z היכולים להיות פיתרון, נאמר z_1; אז לכל j המקיים $2^j > z_1$ לא ייתכן פיתרון בשלמים השונים כולם מאפס למשוואה (*).

כתוצאה מן הטענה הזאת, אנחנו יכולים לשכוח בעצם ממשוואת פרמה, כי התוצאה המבוקשת שלנו היא מסקנה מתוצאה כללית יותר שאותה אפשר לנסח כך:

מ ש פ ט: תהי A קבוצה של מספרים טבעיים המקיימת: לכל מספר ראשוני $p \geq 3$, קיים k_p כך שבשביל כל $k \geq k_p$ מתקיים $kp \in A$. אזי ל- A צפיפות אחת.

ואכן, משפט פלטניגס והטענה שהוכחנו לעיל מראים, כי אם A היא קבוצת ה-n-ים שבשבילם נכון משפט פרמה האחרון, אזי A מקיימת את תנאי המשפט דלעיל.

נסביר עכשיו בקיצור מדוע משפט זה נכון, ואחרי-כן נביא את הפרטים.

יהיו $p_1 < p_2 < p_3 < \dots$ המספרים הראשוניים האי-זוגיים $(3 < 5 < 7 < \dots)$. צפיפות המספרים המתחלקים ב-p_k היא כמובן $\frac{1}{p_k}$, ולכן $(1 - \frac{1}{p_k})$ היא צפיפות המספרים שאינם מתחלקים ב p_k. יתר על כן, בהיות ה-p_i-ים ראשוניים, קבוצות אלו מתנהגות כאילו הן מאורעות בלתי תלויים (במובן ההסתברותי)

ו $d_n = \prod_{k=1}^{N} (1- \frac{1}{p_k})$ היא צפיפות המספרים שאינם מתחלקים באף אחד מה-p_i-ים כאשר $1 \leq i \leq N$. עתה, העובדה ש $\sum_1^{\infty} \frac{1}{p_k} = +\infty$ (ראה להלן) גוררת $d_n \to 0$,

ולכן "רוב המספרים" מתחלקים בלפחות אחד מה-p_i-ים, $1 \le i \le N$, ופרט למספר סופי של מכפולות אלו - כולם נמצאים ב-A. יוצא כי ל-A הצפיפות 1.

להוכחה שתורטטה לעיל, ושאותה נפרט עכשיו צעד-צעד, שני מרכיבים. האחד - בעל אופי חשבוני, וקשור לתכונות החשבוניות של המספרים הראשוניים, והאחר בעל אופי אנליטי. ננסח תחילה את המרכיב הראשון, כלומר:

ל מ ה: אם $p_1 < p_1 < \dots < p_N$ מספרים ראשוניים, אזי צפיפות קבוצת המספרים הטבעיים שאינם מתחלקים באף אחד מהם היא $(1-\frac{1}{p_1}) \dots (1-\frac{1}{p_n})$.

הוכחה: הקבוצה שאנו דנים בה היא מחזורית, ומחזורה הוא $p_1 p_2 \dots p_N$.

נבדוק תחילה את המקרה $N = 1$. כאן הטענה היא ברורה, כי רק הכפולות של p_1 מתחלקים ב p_1, והצפיפות של $\{1,2,\dots, p_1 - 1, p_1 + 1,\dots\}$ שווה ל $\frac{p_1 - 1}{p_1} = 1 - \frac{1}{p_1}$.

כאשר $N = 2$, מבין המספרים, $1,2,\dots,p_1p_2$ אנו משמיטים את הכפולות של p_1 ואת הכפולות של p_2, ולכן היינו צריכים לקבל $1 - \frac{1}{p_1} - \frac{1}{p_2}$. אלא שאת p_1p_2 אנו "השמטנו פעמיים" ולכן צריך להוסיף $\frac{1}{p_1p_2}$

ונקבל בדרך זו $(1 - \frac{1}{p_2})(1 - \frac{1}{p_1}) = 1 - \frac{1}{p_1} - \frac{1}{p_2} + \frac{1}{p_1p_2}$.

אפשר להמשיך בדרך זאת, ולהוכיח את הלמה בהסתמך על העובדה שהמספרים היחידים המתחלקים על ידי $p_{i_1}, \dots, p_{i_k}$ הם הכפולות של $p_{i_1} \dots p_{i_k}$. במקום זה ניתן הוכחה קצרה יותר באינדוקציה על N. נשתמש בעובדה הבאה (את הוכחתה תמצא בנספח II).

אם P ו-Q זרים אז לכל a, מבין המספרים $a, a + P, a + 2P, \ldots, a + (Q - 1)P$ בדיוק אחד מתחלק ע"י Q.

נסמן ב P את המכפלה $p_1 p_2 \cdots p_{N-1}$. לפי הנחת האינדוקציה

$m = \prod_{i=1}^{N-1} (1 - \frac{1}{p_i}) \cdot P$ מבין המספרים $\{1, 2, \ldots, P\}$ אינם מתחלקים באף אחד מה p_i-ים, $1 \le i \le N - 1$. נסמן את m המספרים הללו ב $a_1 < a_2 < \ldots < a_m$.
מכאן, שהמספרים בטווח $\{1, \ldots, p_1 \cdots p_N - 1\}$ שאינם מתחלקים באף אחד מה p_i-ים, $1 \le i \le N$, נמצאים בקבוצות

$\{a_j, a_j + P, a_j + 2P, \ldots, a_j + (p_{N-1} - 1)P\}, \quad 1 \le j \le m$

המכילות את כל המספרים בטווח הנ"ל שאינם מתחלקים באף אחד מה p_i-ים, $1 \le i \le N - 1$.

p_N ו- P זרים, ולכן העובדה שניסחנו לעיל מבטיחה כי בדיוק $(1 - \frac{1}{p_N})$ מבין אלו אינם מתחלקים ע"י ב- p_N ומכאן נכונות הנוסחה בשביל N.

המרכיב האנליטי, ככל שהוא נוגע למספרים הראשוניים, מקורו בשיפור של L. Euler למשפט המפורסם של אוקלידוס על קיום מספר אין-סופי של מספרים ראשוניים. אוילר הוכיח, כי הטור $\sum_{i=1}^{\infty} \frac{1}{p_i}$ מתבדר, ומכך נובע בפרט, כי יש בו אין סוף איברים!

תוצאה זאת מוכרת דיה, כך שלא נקדיש לה מקום רב, ונשרטט רק בקוים כלליים את הוכחה המקובלת. כידוע, הטור $\sum \frac{1}{n^s}$ מתכנס כאשר $s > 1$, ומתבדר כאשר $s = 1$.
לעובדה שיש פירוק יחיד של מספר לגורמים ראשוניים, יש ביטוי אנליטי בזהות

$$(1+\frac{1}{2^s}+\frac{1}{2^{2s}}+\dots)(1+\frac{1}{3^s}+\frac{1}{3^{2s}}+\dots)\dots(1+\frac{1}{p^s}+\frac{1}{p^{2s}}+\dots)=\sum_1^\infty\frac{1}{n^s}$$

את כל אחד מהמרכיבים בצד שמאל אפשר לסכם לפי נוסחת סכום של טור הנדסי אין-סופי. מקבלים:

$$\prod_p\left(\frac{1}{1-\frac{1}{p^s}}\right)=\sum_1^\infty\frac{1}{n^s}$$

כאשר המכפלה באגף שמאל לקוחה על כל הראשוניים $2,3,5,\dots$. כאשר s שואף לאחד, הטור באגף ימין מתבדר, ולכן $\lim_{s\to1}\frac{1}{\sum\frac{1}{n^s}}=0$. מכאן נובע $\lim_{s\to1}\prod_1(1-\frac{1}{p^s})=0$

ומזה קל להסיק בשיטות הרגילות של החשבון האינפיניטיסימלי,

$$\lim_{N\to\infty}\prod_1^N(1-\frac{1}{p_j})=0$$

טענת אוילר על התבדרות הטור $\sum\frac{1}{p_i}$ נובעת מהגבול האחרון כאשר משתמשים באי-השויון $1-x\ge e^{-10x}$ הנכון לכל $0\le x\le\frac{1}{2}$.

נחזור כעת למשפט הכללי על קבוצה A שבה כנגד ראשוני $p\ge3$, קיים k_p כך שלכל $j\ge k_p$ מתקיים $j_p\in A$. יש להראות, כי הצפיפות של A שווה לאחד. למטרה זו, נראה כי לכל $\varepsilon>0$, הצפיפות של A גדולה או שווה ל $1-\varepsilon$. ואמנם, בהינתן $\varepsilon>0$, נמצא לפי משפטו של אוילר N מספיק גדול כך ש $\prod_{i=1}^N(1-\frac{1}{p_i})<\varepsilon$. יהי $K=\max(k_{p_1},\dots,k_{p_n})$ המובטחים בתנאי המשפט.

אזי A מכילה כל מספר הגדול מ Kp_N המתחלק בלפחות אחד מהמספרים $p_1,p_2,\dots,p_n$. לקבוצה זאת, השונה אך במספר סופי של אברים מהקבוצה המתאורת בלמה, צפיפות שהיא לפחות $1-\varepsilon$, ועל כן לקבוצה A צפיפות הגדולה מ $1-\varepsilon$. נכונות טענה זו

לכל ε מסיימת את הוכחת המשפט העיקרי שלנו:

משפט פרמה האחרון נכון כמעט לכל מספר טבעי n.

כל עוד אין במשפט של פלטינגס הערכות מפורשות למספרם ולגודלם של הפיתרונות האפשריים, אין ביכולתנו לקבוע את גודל ה-k_p-ים במשפט העזר שהוכח לעיל, ולכן אין ביכולתנו להוכיח בדרכים הללו את נכונות משפט פרמה אפילו ל- n מסויים אחד. סיימנו כאן את החלק הקל - דהיינו הסקת התוצאה על משפט פרמה האחרון ממשפט פלטינגס. את החלק השלישי של המאמר נקדיש לניסוח מדוייק של המשפט הכללי של פלטינגס, שתוצאה זאת היא רק אחת משימושיו.

ההמשך בגיליון הבא.

:

נספח I

אם משפט פרמה האחרון איננו נכון בשביל n מסויים, אז אפשר לשאול מהו ה- z הקטן ביותר, נקרא לו $z(n)$, שבשבילו קיימים x ו-y המקיימים את המשוואה

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

אנו נראה כאן, ע"י שיקול פשוט, כי הוא לכל הפחות n. אפשר להגדיל את החסם הזה בעזרת שיקולים מסובכים יותר, אך עד כה לא הצליחו להוכיח את המשפט בשביל n מסויים על-ידי שכלול הגישה הזאת.

בלי הגבלת הכלליות נניח כי $x \le y < z$, נכתוב $z = y + a$ ונשתמש בנוסחת הבינום:

$$x^n + y^n = z^n = (y + a)^n = y^n + ny^{n-1} a + \dots.$$

מכאן, על-ידי הגדלת אגף שמאל והקטנת אגף ימין נקבל את אי-השויון

$$y^n + y^n > y^n + ny^{n-1}a$$

או

$$y > na \ge n$$

כי a הוא לכל הפחות 1.

נספח II

אם P ו-Q זרים אזי לכל a, בדיוק אחד מבין המספרים

$$a, a + P, \dots, a + (Q - 1)P$$

מתחלק ב-Q.

הוכחה: לכל $0 \le k < Q$ נסמן ב- r_k את השארית בחילוק של $a + k P$, כלומר נכתוב $0 \le r_k < Q$, $a + kP = u_kQ + r_k$.

אני טוען כי כאשר $j \ne k$, מתקיים $r_j \ne r_k$, כי אחרת על-ידי חיסור היינו מקבלים $(k - j) \underline{P} = (u_k - u_j)Q$. אבל Q ו- $\underline{P}$ זרים, ולכן Q חייב לחלק את $k - j \ne 0$. אבל $|k - j|$ קטן מ Q, וזאת סתירה, כי הדבר אפשרי רק כאשר $k - j = 0$. מכאן, שהמספרים r_k, $0 \le k < Q$, כולם שונים, וכולם נמצאים בקטע $[0,Q)$. לכן כל מספר מתקבל בדיוק פעם אחת, ובפרט יש בדיוק k אחד שבשבילו $r_k = 0$ כלומר $a + k P$ מתחלק ב Q.

ספרות

מספר אנשים שמו לב לשימוש שהסברנו כאן של משפט פלטינגס. ד. שנקס מיחס את
התוצאה לוושינגטון, אך נמנע מלתת הוכחה בספרו, כי הוא לא ידע אם המאמר של
וושינגטון פורסם. אני לא ראיתי פרסום של וושינגטון, אך ראיתי מאמר של
הית-בראון שבו נמצאת הוכחה השונה קצת מזו שהבאתי כאן.

Solved and Unsolved Problems in Number Theory by D. Shanks,
Chelsea N.Y, 3rd Edition, 1985.

Fermat's Last Theorem for "Almost All" Exponents, D.R. Heath - Brown
Bull. London Math. Society, v.17 (1985), pp. 15-16.