עקומים אליפטיים, גבהים והשערת מליון הדולר

אמנון בסר

14 בדצמבר 2010

השערת Birch Swinnerton-Dyer

- השערת בשטח הגאומטריה האריתמטית
- עוסקת בפתרונות במספרים רציונליים למשוואות הנקראות עקומים אליפטיים.
- ההשערה משלבת תחומים מתמטיים רבים, גיאומטריה, תורת המספרים, אנליזה מרוכבת..
- היא אחת מבעיות המילניום - פתרונה מזכה במליון דולרים.

מקרה ראשון: משוואה אחת בנעלם אחד: $x^n + a_{n-1}x^{n-1} + \cdots a_1x + a_0 = 0$.
מספר סופי של פתרונות.
n משוואות ב- n נעלמים: שוב מספר סופי של פתרונות (בדרך כלל)
מציאתם ביעילות מסתמכת על תורת בסיסי גרבנר.

עקומים - משוואה אחת בשני נעלמים.

$$f(x,y) = 0$$

אוסף הפתרונות עם x, y מרוכבים נראה כמו כדור עם g חורים

g נקרא הגנוס.
אנחנו מחפשים נקודות רציונליות - פתרונות x, y למשוואה כאשר גם x וגם y רציונליים.

עקומים מגנוס 0 ושלשות פיתגוראיות

$g = 0$ - שפת כדור
למשל $x^2 + y^2 = 1$
במקרה זה אם יש נקודה רציונלית יש אינסוף כאלה וקל למצוא אותן.

טענה

אוסף הפתרונות הרציונליים למשוואה $x^2 + y^2 = 1$ הוא כל הזוגות

$$(x, y) = \left(\frac{1 - t^2}{1 + t^2}, \frac{2t}{1 + t^2}\right)$$

עבור t רציונלי.

הוכחה: נעביר קו בשיפוע t דרך הנקודה $(-1,0)$
משוואתו $y=t(x+1)$ נמצא את נקודת החיתוך השניה ע"י הצבה

$$1=t^2(x+1)^2+x^2=(1+t^2)x^2+2t^2x+t^2$$
$$0=x^2+\frac{2t^2}{1+t^2}x+\frac{t^2}{1+t^2}-1$$

סכום שני השרשים הוא מינוס המקדם של x. אחד מהם הוא -1 לכן השני הוא גם רציונלי. במדויק

$$x=1-\frac{2t^2}{1+t^2}=\frac{1-t^2}{1+t^2}$$

ו-

$$y=t(x+1)=\frac{2t}{1+t^2}$$

להיפך, אם (x,y) נקודה רציונלית אז שיפוע הקו בינה לבין $(-1,0)$ רציונלי

עקומים מגנוס 2 ומעלה ומשפט Faltings

כאשר הגנוס גדול מ- 1 יש משפט מפורסם מאד של המתמטיקאי הגרמני Faltings מ- 1983

משפט

למשוואה מגנוס גדול מ- 1 יש מספר סופי של פתרונות רציונליים

משפט זה היה ידוע קודם כהשערה של המתמטיקאי Mordell מתחילת המאה ה- 20

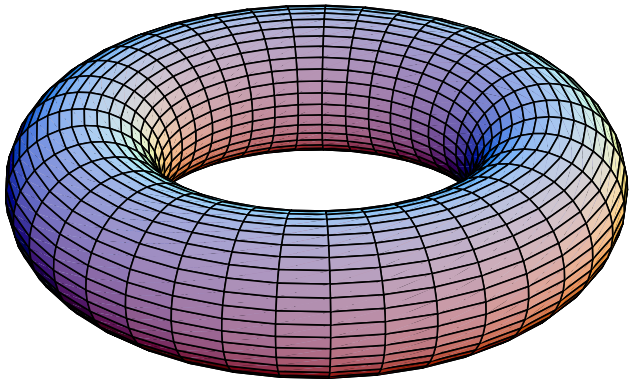
דוגמה

השערת פרמה: למשוואה $x^n + y^n = z^n$ כאשר $n > 2$ אין פתרונות ב- x, y, z שלמים חוץ מכאשר אחד מהם 0.

אם נחלק ב- z^n נראה שזה אותו דבר כמו לומר שלמשוואה $x^n + y^n = 1$ אין פתרונות רציונליים חוץ מ- $(1,0), (0,1)$.

המשפט אומר שלפחות יש רק מספר סופי של פתרונות עבור $n \geq 5$.

$g = 1$ - בייגל



הגדרה

עקום אליפטי מעל הרציונליים הוא משוואה מגנוס 1

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

כאשר a ו- b רציונליים.

חוק החבורה של עקום אליפטי

אוסף הנקודות הרציונליות של עקום אליפטי הוא חבורה אבלית (יש דרך לחבר נקודות שהיא קומוטטיבית ואסוציאטיבית ולכל איבר יש איבר נגדי).
ליתר דיוק, יש להוסיף "נקודה באינסוף" והיא דווקא האיבר הנייטרלי 0

כללי החיבור

- $0 + (x, y) = (x, y)$
- $(x, y) + (x, -y) = 0$
- $(x_1, y_1) + (x_2, y_2) = (x_3, -y_3)$ כאשר (x_3, y_3) היא נקודת החיתוך השלישית עם העקום של הקו
  - המחבר את $(x_1, y_1), (x_2, y_2)$ אם אלה שתי נקודות שונות
  - המשיק לנקודה (x_1, y_1) אם $(x_1, y_1) = (x_2, y_2)$

עובדות יסודיות על החבורה של העקום האליפטי

משפט

החבורה של העקום האליפטי נוצרת סופית

משפט זה, המכונה משפט Mordell-Weil אומר למעשה כי קיימת קבוצה סופית של פתרונות $P_1, \ldots, P_k$ אשר מהן אפשר לקבל את כל הפתרונות על ידי פעולות של חיבור וחיסור.

הגדרה

המספר המינימלי k של נקודות מהן ניתן ליצור (כמעט) את כל הנקודות נקרא הדרגה של העקום האליפטי.

ליתר דיוק, החבורה של העקום האליפטי מקיימת

$$E(\mathbb{Q}) \cong \mathbb{Z}^k \oplus E(\mathbb{Q})_{\text{tor}}$$

משפט

הגודל של $E(\mathbb{Q})_{\text{tor}}$ הוא לכל היותר 16 (משפט Mazur)

הגובה של מספר רציונלי

הגובה הוא מדד לסיבוך של מספר.

הגדרה

הגובה של מספר רציונלי x ניתן כך: רושמים את x כשבר מצומצם $x = \frac{r}{s}$ ואז

$$H(x) = \max(|r|, |s|)$$

הגובה הלוגריתמי של x ניתן על ידי

$$h(x) = \ln(H(x))$$

טענה

לכל ממשי M יש מספר סופי של רציונליים x עם $h(x) < M$.

הוכחה

יש מספר סופי של r, s עם $|r|, |s| < e^M$ □

פונקצית הגובה של עקום אליפטי

הגדרה

הגובה (הלוגריתמי) של נקודה $P = (x, y)$ בעקום אליפטי מוגדר על ידי

$$h(P) = h(x)$$

מסקנה

לכל ממשי M יש מספר סופי של נקודות על העקום האליפטי P עם $h(P) < M$.

הוכחה

לכל x רציונלי יש לכל היותר שני y עבורם (x, y) נקודה רציונלית על העקום. $\square$

תכונת הריבועיות של הגובה והגובה הקנוני

לגובה h על עקום אליפטי E יש תכונות המזכירות תכונה של נורמה בריבוע על מרחב מכפלה פנימית (תבנית ריבועית).

בפרט, ל- $\sqrt{h}$ יש תכונות של נורמה

1. $\sqrt{(h(nP)} \sim n\sqrt{h(P)}$
2. יש אי שוויון משולש $\sqrt{h(P+Q)} \leq\sim \sqrt{h(P)} + \sqrt{h(Q)}$

כאשר $\sim$ משמעותו עד כדי פונקציה חסומה.

טענה

הגבול $\lim_{k\to\infty} \frac{\sqrt{h(2^k P)}}{2^k}$ *קיים ואם נסמנו* $\sqrt{\hat{h}(P)}$ *אז* $\sqrt{\hat{h}}$ *מקיימת את תכונות הנורמה* 1 *ו-* 2 *במדויק ללא* $\sim$

ההוכחה היא תרגיל פשוט בחדו"א. $\hat{h}$ נקרא *הגובה הקנוני* והוא נבדל מהגובה הרגיל בפונקציה חסומה.

1. מראים שקיימת קבוצה סופית $\{P_1, \ldots, P_m\}$ כך שלכל נקודה $P \in E(\mathbb{Q})$ יש $Q \in E(\mathbb{Q})$ כך שמתקיים $P = 2Q + P_i$ עבור איזשהו i.
2. לפי הריבועיות של הגובה

$$\sqrt{\hat{h}(Q)} = \frac{1}{2}\sqrt{\hat{h}(P - P_i)} \leq \frac{1}{2}\left(\sqrt{\hat{h}(P)} + \sqrt{\hat{h}(P_i)}\right)$$

ומכאן שאם $\sqrt{\hat{h}(P)}$ מספיק גדול ביחס ל- $\sqrt{\hat{h}(P_i)}$ אז $\sqrt{\hat{h}(Q)} < \sqrt{\hat{h}(P)}$ (ירידה Descent)

3. מסיקים שאחרי מספר צעדים אפשר להגיע ל Q עם $h(Q)$ קטן ולכן בקבוצה סופית לפי מסקנה קודמת. כך כל P נרשם כסכום של P_i ואיברים בקבוצה סופית זו.

נקודות על עקום אליפטי מודולו ראשוני

נתון העקום האליפטי $E : y^2 = x^3 + ax + b$
נניח שגם a וגם b שלמים.

בעיה

כמה פתרונות יש למשוואה בשדה המספרים מודולו ראשוני p?

הערכה ממוצעת: לחצי מאברי $\mathbb{Z}/p$ יש שורש ריבועי. אם ל- $x^3 + ax + b$ יש שורש אז גם הוא וגם המינוס שלו נותנים פתרונות. לכן בממוצע יש p פתרונות.

הגדרה

נסמן את מספר הפתרונות ב- $p - a_p$

משפט

מתקיים $|a_p| \leq 2\sqrt{p}$

שמושים בשטח ההצפנה

- הנקודות של עקום אליפטי מודולו ראשוני מהוות חבורה לפי אותם כללים כמו מעל הרציונליים.
- אפשר להשתמש בחבורה זו לצורך הצפנה
- שיטת ההצפנה בטוחה הרבה יותר משיטות אחרות (RSA)
- נכנסת לשמוש ביותר ויותר מקומות, כמו הדרכונים של מספר ארצות אירופאיות
- לבחירת עקומים טובים להצפנה נדרשות שיטות מתמטיות מורכבות שרובן פותחו בעשור האחרון
- הכל נלמד בקורס: שיטות אריתמטיות בקריפטוגרפיה

פונקצית L של עקום אליפטי

הגדרה

לעקום אליפטי E מעל הרציונליים מגדירים את פונקציית ה- L שלו על ידי

$$L_E(s) = \prod_p (1 - a_p p^{-s} + p^{1-2s})^{-1}$$

כאשר s הוא משתנה מרוכב ו- p עובר על כל הראשוניים (כאן יש רמאות קטנה).

המכפלה המגדירה את פונקציית ה- L של עקום אליפטי מתכנסת עבור $\mathrm{Re}(s)$ מספיק גדול.

משערים שניתן להרחיב אותה לפונקציה על כל המרוכבים (המשכה אנליטית).

זה אכן נכון כפי שנראה בהמשך.

פונקצית L של עקום אליפטי דומה מבחינת הצורה שלה לפונקצית זיתא של רימן

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

ההשערה

ההשערה של Birch ו- Swinnerton-Dyer עוסקת בהתנהגות של $L_E(s)$ ליד $s = 1$.

קיים r שלם אי שלילי יחיד כך ש- $\alpha = \lim_{s\to 1}(s-1)^{-r}L_E(s) \neq 0$

להשערה שני חלקים

1. r שווה לדרגה של חבורת הנקודות הרציונליות של העקום E.
2. ניתנת נוסחה לערך של α. הנוסחה נתונה בצורה לא לחלוטין מדויקת כ- $\alpha = cR_\infty\omega_\infty$ כאשר c הוא רציונלי (מסובך לחישוב), ω_∞ הוא ממשי קל לחישוב הנקרא המחזור הממשי. R_∞ נקרא הרגולטור. במקרה של $r = 1$ הוא פשוט $R_\infty = \hat{h}(P)$ כאשר P נקודה מסדר אינסופי.

בעיית המספרים הקונגרואנטיים

הגדרה

מספר טבעי n נקרא מספר קונגרואנטי אם קיים משולש ישר זוית שאורך כל צלעותיו רציונליים ששטחו n.

בעיה

איך להחליט האם מספר נתון n הוא קונגרואנטי או לא?

בעיה זו עניינה כבר את היוונים. התברר כי 1 (פרמה) 2 3 ו- 4 אינם קונגרואנטיים ואילו 5 6 7 (אוילר) ו- 8 הם כן. הבעיה הכללית עדיין פתוחה.
עבודה של Tunnel פותרת את הבעיה בהנחת השערת Birch Swinnerton-Dyer

טענה

הטבעי n הוא מספר קונגרואנטי אם ורק אם קיימת נקודה רציונלית מסדר אינסופי על העקום האליפטי E_n המוגדר על ידי המשוואה $y^2 = x^3 - n^2x$

הוכחה: צריך a, b, c רציונליים כך ש-

$$a^2 + b^2 = c^2 \ , ab = 2n$$

לכן יש t רציונלי כך ש-

$$\frac{a}{c} = \frac{1-t^2}{1+t^2} \ , \ \frac{b}{c} = \frac{2t}{1+t^2}$$

ולכן

$$a = d(1-t^2) \ , \ b = 2dt \quad (d = \frac{c}{1+t^2}) \ , n = d^2t(1-t^2)$$

הקשר לעקומים אליפטיים

נציב

$$x = -nt \ , \ y = \frac{n^2}{d}$$

ונקבל

$$x^3 - n^2x = x(x^2 - n^2) = -nt(n^2t^2 - n^2) = n^3t(1 - t^2) = n^3\frac{n}{d^2} = y^2$$

אפשר למצוא את כל נקודות הפיתול על העקום ולהסיק שהנקודה (x, y) מסדר אינסופי.

קריטריון למספרים קונגרואנטיים

Tunnel השתמש בקשר לעקומים אליפטיים ובהשערת Birch Swinnerton-Dyer כדי לקבל את הקריטריון הבא למספרים קונגרואנטיים:

משפט

אם ההשערה נכונה, יהי n מספר אי זוגי חופשי מריבועים. אז

1. *n קונגרואנטי אם ורק אם מספר השלשות (x, y, z) של שלמים המקיימות*
   $2x^2 + y^2 + 8z^2 = n$ *כפול ממספר השלשות המקיימות*
   $2x^2 + y^2 + 32z^2 = n$
2. *$2n$ קונגרואנטי אם ורק אם מספר השלשות (x, y, z) של שלמים המקיימות*
   $4x^2 + y^2 + 8z^2 = n$ *כפול ממספר השלשות המקיימות*
   $4x^2 + y^2 + 32z^2 = n$

בשני המקרים כיוון הרק אם אינו תלוי בהשערה.

מקרים ידועים של ההשערה- נקודות היגנר

ב - Wiles 1995 הוכיח את השערת פרמה

בעצם הוא (כמעט) הוכיח את השערת Shimura-Taniyama ממנה נובע

- שפונקצית L של עקום אליפטי אכן ניתנת להגדרה לכל המרוכבים.
- שקיימת פונקציה "טובה"

$$\phi : H \to E(\mathbb{C})$$

כאשר H הוא אוסף המרוכבים עם חלק מרוכב חיובי.

אם D טבעי אפשר לקבל מ- $\phi(i\sqrt{D})$ נקודה רציונלית P_D על העקום האליפטי הנקראת נקודת Heegner

משפט מסובך מאד של Gross ו- Zagier קושר את $\hat{h}(P_D)$ ל- $L_E(1)$ ונובע שההשערה של Birch ו- Swinnerton-Dyer נכונה במקרה ש- $r = 0$ (וגם במקרה ש- $r = 1$)