# משוואות פל – הרצאה

$$x^2 - dy^2 = \pm 1$$

משוואה ממש מגניבה, חקרו אותה הרבה אנשים – בראהמגופטה במאה ה7 בהודו, פרמה, לאגרנז', אוילר (שקרא למשוואה הזו על שם פל כי הוא חשב שהוא היה קשור...)

חוג ריבועי $\mathbb{Z}[\sqrt{d}]$ - מורכב מאיברים $x + y\sqrt{d}$ כאשר $x, y \in \mathbb{Z}$ .

כפל – אם $\alpha = x + y\sqrt{d}, \quad \beta = z + w\sqrt{d}$ אז

$$\alpha \cdot \beta = (xz + d \cdot yt) + (xt + yz)\sqrt{d}$$

הצמדה - עבור $\alpha = x + y\sqrt{d}$ אז מגדירים $\bar{\alpha} = x - y\sqrt{d}$ .

נורמה - $x^2 - dy^2 = N(x + y\sqrt{d})$ זה $N(\alpha) = \alpha \cdot \bar{\alpha}$ .

הנורמה היא כפלית $N(\alpha\beta) = N(\alpha)N(\beta)$.

פתרון למשוואת פל $x^2 - dy^2 = \pm 1$ זה אותו דבר כמו $\alpha = x + y\sqrt{d}$ שהוא **הפיך** ב$\mathbb{Z}[\sqrt{d}]$.

לפתרונות יש מבנה של *חבורה*.

**למה (דיריכלה)** לכל מספר ממשי $\xi$ ולכל $M$ טבעי יש מספר $m \leq M$ ו$n$ כך ש

$$\left|\xi - \frac{n}{m}\right| \leq \frac{1}{Mm}$$

**הוכחה**: זה שקול ל$\frac{1}{M} \leq \|m\xi\|$ (מרחק ממספר שלם). מחלקים ל$M$ קטעים באורך $\frac{1}{M}$ את המספרים מודולו 1 ואז משובך יונים 2 מבין ה$m\xi$ נופלים באותו שובך ו$m = m_1 - m_2$ יעשה את העבודה.■

**הערה:** זה מקרה פרטי של למה של מינקובסקי עבור מקבילית במישור ואנחנו נמצא ממש נוסחה ל$\frac{n}{m}$ כאלה בהמשך (שברים משולבים).

**משפט:** יש פתרון למשוואת פל $x^2 - dy^2 = 1$ **.**

**הוכחה:** נשתמש בלמה ונמצא הרבה $\frac{x}{y}$ שמקרבים את $\sqrt{d}$ . המסקנה ש

$$\left|x - y\sqrt{d}\right| < \frac{1}{y}$$

עבור כאלה זוגות מתקבל ש $\left|N\left(x + y\sqrt{d}\right)\right| < C$ לאיזשהו קבוע.

משובך – יש $\alpha, \beta$ ש $N(\alpha) = N(\beta) = r$ וגם $\alpha \equiv \beta \ (mod\ r)$ . ואז $\alpha \cdot \bar{\beta}$ מתחלק ב$r$ ולכן $u = \frac{\alpha \cdot \bar{\beta}}{r}$ הוא ב$\mathbb{Z}[\sqrt{d}]$ ועם נורמה 1 כנדרש. ■

נסתכל על הפתרונות (בה"כ $x, y > 0$) ונסדר אותם לפי קורדינטת $y$ . נניח ש $\xi = u + v\sqrt{d}$ הוא עם ה$v$ הכי קטן.

בהינתן פתרון $\alpha = x + y\sqrt{d}$ נסתכל על

$$\frac{\alpha}{\xi} = \alpha \cdot \bar{\xi} = (xu - dyv) + (uy - vx)\sqrt{d}$$

$$uy - vx = \sqrt{1 + dv^2} \cdot y - v\sqrt{1 + dy^2} = \frac{y^2 - v^2}{\sqrt{y^2 + dv^2y^2} + \sqrt{v^2 + dv^2y^2}}$$

וזה גדול מ0 וקטן ממש מ $y$ .

מכאן, אפשר להמשיך ולחלק וככה הפתרון קטן עד שנגיע לפתרון הבסיסי.

**מסקנה:** למשוואת פל $x^2 - dy^2 = 1$ יש פתרון בסיסי $u^2 - dv^2 = 1$ , כל שאר הפתרונות הם (עד כדי סימן)

$$u_n + v_n\sqrt{d} = \left(u + v\sqrt{d}\right)^n$$

$$u_n = \frac{\left(u + v\sqrt{d}\right)^n + \left(u - v\sqrt{d}\right)^n}{2}$$

$$v_n = \frac{\left(u + v\sqrt{d}\right)^n - \left(u - v\sqrt{d}\right)^n}{2d}$$

ואפשר לקשר לפולינום צ'בישב -

$$u_n = T_n(u) \quad ; \quad T_n\left(\cos x\right) = \cos nx$$

נשים לב ש$u_k$ למשל מקיימת רקורסיה - $u_{k+2} = u_{k+1} \cdot u + u_k$ .

מפה אפשר לקבל נוסחאות דומות לנוסחאות על מספרי פיבונאצ'י - $u_{2r} = 2u_r^2 - 1$ .

אני רוצה לספר עוד תיאוריה שלא נשתמש בה אבל היא ממש מגניבה.

<u>שברים משולבים</u>: (תסתכלו בהרצאת שברים משולבים)

ההגדרה -

$$\xi = [\xi] + \{\xi\} = a_0 + \frac{1}{(1/\{\xi\})} = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}$$

נסמן את הביטויים הסופיים ב-$[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}$ וזה נקרא השבר המשולב.
מגדירים גם לפעמים את הסדרה $\xi_k = [a_k, a_{k+1}, \dots]$.

נוח להשתמש בוקטור $u_n = (p_n, q_n)$ . מתקיים ש $u_n = u_{n-2} + a_n u_{n-1}$ .

מה שאנחנו עושים זה להסתכל במישור על הישר $y = \xi \cdot x$ ובאופן חמדני אנחנו מקרבים אותו עם וקטורים $u_n, u_{n-1}$ - הזוגיים מתחת לישר והאיזוגיים מעליו. בכל שלב אנחנו לוקחים אחד מהם ומוסיפים כפולה של הקודם עד כמה שאפשר – לקחת את הכפולה הרלוונטית זה חלק שלם, להפוך בין הכיוונים זה לעשות $\frac{1}{x}$.

(שברי פארי – זה פשוט להסתכל על הסכום בכל שלב במקום לעשות עד כמה שאפשר, זה סדרה ארוכה יותר)

בפרט בכל שלב $u_n, u_{n-1}$ מייצר מקבילית ריקה - $p_n q_{n-1} - q_n p_{n-1} = \pm 1$.

כמו גם ש$|q\xi - p|$ זה פשוט המרחק של הוקטור מהישר. מקבלים שהקירובים נהיים טובים יותר וגם ש

$$|p_n - q_n \xi| < \frac{1}{q_{n+1}}$$

(זה כי $\left|\frac{p_n}{q_n} - \frac{p_{n+1}}{q_{n+1}}\right| \geq \frac{1}{q_n q_{n+1}}$ ממש יותר מהמרחק של $\left|\frac{p_n}{q_n} - \xi\right|$ כי הישר נמצא בין הוקטורים).

נשים לב שאם יש שבר $\frac{p}{q}$ כך ש

$$|p - \xi q| < |p_n - \xi q_n|$$

אז $q \geq q_{n+1}$ לכל הפחות. אכן להיות יותר קרוב לישר האדום ונמוך מ$u_{n+1}$ אומר שהוא בתוך הצלב הסגור משמע על השפה ואם הוא לא $u_{n+1}$ אז $u_n$ קרוב יותר בהכרח.

**מסקנה** (סיכום שברים משולבים):

- בכל שלב $u_n, u_{n-1}$ מייצר מקבילית ריקה - $p_n q_{n-1} - q_n p_{n-1} = \pm 1$.
- הקירובים נהיים טובים יותר ו - $|p_n - q_n \xi| < \frac{1}{q_{n+1}}$.
- זה הקירוב הכי טוב עד מכנה מסויים: לשבר $\frac{p}{q}$ כך ש $|p - \xi q| < |p_n - \xi q_n|$ אז $q \geq q_{n+1}$ .
- קירוב טוב הוא שבר משולב: אם יש לנו קירוב $\frac{a}{b}$ שמקיים $\left|\xi - \frac{a}{b}\right| < \frac{1}{2b^2}$ אז בהכרח $\frac{a}{b} = \frac{p_n}{q_n}$ לאיזשהו $n$ .

הסבר לטענה האחרונה - ניקח $n$ כך ש $q_n < b < q_{n+1}$ ואז מהלמה הקודמת $|\xi q_n - p_n| < |b\xi - a| < \frac{1}{2b}$ ולכן:

$$\frac{1}{bq_n} \leq \left|\frac{a}{b} - \frac{p_n}{q_n}\right| \leq \left|\frac{a}{b} - \xi\right| + \left|\xi - \frac{p_n}{q_n}\right| < \frac{1}{2b^2} + \frac{1}{2q_n b}$$

שזה סתירה. ■

<u>שברים משולבים מחזוריים ומשוואת פל</u>

נתחיל מדוגמה – אנחנו רוצים לפתור משוואת פל $x^2 - 19y^2 = 1$ . אז נשים לב ש$\sqrt{19}$ ממש קרוב ל$\frac{x}{y}$ - ברמה שהוא אחד מהשברים המשולבים.

בואו נתחיל לעשות שבר משולב –

$$\xi_0 = \sqrt{19},\ a_0 = 4$$

$$\xi_1 = \frac{1}{\sqrt{19} - 4} = \frac{\sqrt{19} + 4}{3},\ a_1 = 2$$

$$\xi_2 = \frac{1}{\left(\frac{\sqrt{19} + 4}{3} - 2\right)} = \frac{3}{\sqrt{19} - 2} = \frac{\sqrt{19} + 2}{5},\ a_2 = 1$$

$$\xi_3 = \frac{1}{\left(\frac{\sqrt{19} + 2}{5} - 1\right)} = \frac{5}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{2},\ a_3 = 3$$

$$\xi_4 = \frac{1}{\left(\frac{\sqrt{19} + 3}{2} - 3\right)} = \frac{2}{\sqrt{19} - 3} = \frac{\sqrt{19} + 3}{5},\ a_4 = 1$$

$$\xi_5 = \frac{1}{\left(\frac{\sqrt{19}+3}{5} - 1\right)} = \frac{5}{\sqrt{19}-2} = \frac{\sqrt{19}+2}{3},\ \ a_5 = 2$$

$$\xi_6 = \frac{1}{\left(\frac{\sqrt{19}+2}{3} - 2\right)} = \frac{3}{\sqrt{19}-4} = \sqrt{19}+4,\ \ a_6 = 8$$

ולכן $\xi_7 = \xi_1$ . נסיק שהשבר המשולב של $\sqrt{19}$ הוא מחזורי! למעשה -

$$\sqrt{19} = [4, \overline{2,1,3,1,2,8}]$$

נשים לב גם ש

$$[4,2,1,3,1,2] = \frac{170}{39},\ \ 170^2 - 19 \cdot 39^2 = 1$$

פתרון למשוואת פל. זה אפילו הפתרון היסודי. שימו לב גם ש$8$ זה פעמיים ה$4$ ושחוץ מזה הסדרה היא פלינדרום.

מה שראינו בכל הדוגמה האחרונה זה תופעה כללית – נוכיח זאת עכשיו.

**למה**: אם $\xi$ בעל שבר משולב מחזורי החל ממקום מסויים אז הוא אלגברי ממעלה 2.

**הוכחה**: מספיק להוכיח למחזורי. נשים לב ש

$$[a_0, \dots, a_{n-1}, x] = \frac{p_{n-1}x + p_{n-2}}{q_{n-1}x + q_{n-2}}$$

ולכן אם $\xi = [a_0, \dots, a_{n-1}, \xi]$ אז $\xi$ מקיים משוואה ממעלה 2. ■

נרצה לעשות הפוך, בהשראת הדוגמה ניקח את ה$\xi$ שלנו ונרשום בתור $\xi = \xi_0 = \frac{m_0+\sqrt{d}}{\Delta_0}$ כאשר $\Delta_0 | d - m_0^2$. [נניח בה"כ ש$\Delta_0, m_0 \geq 0$]

נרשום $a_i = [\xi_i]\ , \xi_i = \frac{m_i+\sqrt{d}}{\Delta_i}$

אז נשים לב ש

$$\xi_{i+1} = \frac{1}{\xi_i - a_i} = \frac{1}{\frac{m_i - a_i\Delta_i + \sqrt{d}}{\Delta_i}} = \frac{\Delta_i}{m_i - a_i\Delta_i + \sqrt{d}}$$

$$= \frac{a_i\Delta_i - m_i + \sqrt{d}}{(d - (a_i\Delta_i - m_i)^2)/\Delta_i} = \frac{m_{i+1} + \sqrt{d}}{\Delta_{i+1}}$$

כאשר מגדירים אינדוקטיבית -

$$m_{i+1} = a_i\Delta_i - m_i \ , \Delta_{i+1} = \frac{d - m_{i+1}^2}{\Delta_i}$$

באינדוקציה קל להראות ש$\Delta_i$ הם מספרים שלמים ו $m_i^2 \equiv d \ (mod \ \Delta_i)$ .

בואו נוכיח ש$\Delta_i > 0$ החל ממקום מסויים – הסבר לכך הוא ש$\xi_0 = \frac{\xi_n p_{n-1} + p_{n-2}}{\xi_n q_{n-1} + q_{n-2}}$ ולכן אם ניקח את הצמוד ונפתור אז נקבל $\overline{\xi_n} = -\frac{q_{n-2}}{q_{n-1}} \cdot \left(\frac{\overline{\xi_0} - p_{n-2}/q_{n-2}}{\overline{\xi_0} - p_{n-1}/q_{n-1}}\right)$ ולכן שניקח גבול אז ה$\xi_0 \to \frac{p_n}{q_n}$ ששונה מהצמוד שלו ולכן הסוגריים מתכנסים ל1 ולכן ממקום מסויים ה$-1 < \overline{\xi_n} < 0$ [כי ה$q$ים עולים].

בפרט נובע ש$\xi_n - \overline{\xi_n} > 0$ ו $\xi_n + \overline{\xi_n} > 0$ החל ממקום מסויים, מה שמוכיח ש $m_n, \Delta_n > 0$ .

נשים לב שלפי הגדרה $a_i + 1 > \frac{m_i + \sqrt{d}}{\Delta_i} \geq a_i$ ולכן $m_{i+1} + \Delta_i > \sqrt{d} \geq m_{i+1}$ .

מכיוון ש$\Delta_i\Delta_{i+1} = d - m_{i+1}^2$ אז נובע באינדוקציה ש$\sqrt{d} \geq |m_i|$וכן $\Delta_i \leq d$ .

באינדוקציה גם קל לראות ש$\sqrt{d} \geq m_i \geq 0$ ו $d > \Delta_i > 0$, אכן לפי הגדרה שמסביר זאת. לכן יש מספר סופי של אופציות ל$\xi_i$ מה שמסביר מחזוריות.

נשים לב שראינו גם שאם מחזוריים באופן מלא אז $\xi > 1$ וגם $-1 < \bar{\xi} < 0$ . אכן ראינו זאת ל$\xi_n$ החל ממקום מסויים, משמע ל$\xi$ .

גם להפך זה נכון – הסיבה ש$\xi_n - a_n = \frac{1}{\xi_{n+1}}$ שניקח צמוד נקבל ש $\overline{\xi_n} - a_n = \frac{1}{\overline{\xi_{n+1}}}$

ומפה קל להסיק שגם $\xi_n > 1$ ו $-1 < \overline{\xi_n} < 0$ באינדוקציה.

כמו כן מהנוסחה עכשיו נסיק ש $a_n = \left\lfloor -\frac{1}{\overline{\xi_{n+1}}} \right\rfloor$ ולכן אפשר לשחזר $a_n$ מה$\xi$ עם אינדקס גדול יותר. ולכן מחזוריות החל ממקום מסויים גוררת מחזוריות מלאה.

נשים לב שגם קיבלנו שאם $\xi$ הוא מחזורי באופן מלא ומתאים ל$[\overline{a_0, \dots, a_n}]$ אז עבור $-\frac{1}{\bar{\xi}}$ הוא גם מחזורי באופן מלא ומתאים ל$[\overline{a_n, \dots, a_0}]$.

נתבונן כעת $\sqrt{d}$ . נשים לב ש$\xi = \sqrt{d} + [\sqrt{d}]$ מקיים את התנאי על ההצמדה ולכן מקבלים ש $\sqrt{d} = \left\lfloor \overline{[\sqrt{d}], a_1, a_2, \dots, a_r, 2 \cdot [\sqrt{d}]} \right\rfloor$.

אם נסתכל על ה$\xi_n$ וה $m_n, \Delta_n$ אז $\Delta_0 = 1, m_0 = [\sqrt{d}]$ . נשים לב שאם $\Delta_n = 1$ אז אנחנו בדיוק במחזור כי מקבל $\xi_n = m_n + \sqrt{d}$ וגם להפך כי אם $[\sqrt{d}] + \sqrt{d} = \frac{m+\sqrt{d}}{\Delta}$ אז מהשוואת המקדמים $\Delta = 1$.

נשים לב עוד ש$-1/\left(\overline{\sqrt{d} - [\sqrt{d}]}\right) = \frac{1}{\sqrt{d}-[\sqrt{d}]}$ ולכן אם נשתמש במסקנה הקודמת נקבל ש$a_1, \dots, a_r$ סדרה פילנדרומית - $a_r = a_1, a_2 = a_{r-1}, \dots$ .

נסתכל כעת על השבר המשולב $\frac{p_n}{q_n}$ . אז נשים לב ש

**למה**: $p_n^2 - d \cdot q_n^2 = (-1)^{n-1}\Delta_{n+1}$

**הוכחה**:

$$\sqrt{d} = \xi_0 = \frac{\xi_{n+1}p_n + p_{n-1}}{\xi_{n+1}q_n + q_{n-1}} = \frac{\left(m_{n+1} + \sqrt{d}\right)p_n + \Delta_{n+1}p_{n-1}}{\left(m_{n+1} + \sqrt{d}\right)q_n + \Delta_{n+1}q_{n-1}}$$

נעביר אגפים ונקבל

$$(\Delta_{n+1}q_{n-1} + m_{n+1}q_n) \cdot \sqrt{d} + d \cdot q_n = p_n\sqrt{d} + m_{n+1}p_n + \Delta_{n+1}p_{n-1}$$

משמע

$$p_n = \Delta_{n+1}q_{n-1} + m_{n+1}q_n$$

$$d \cdot q_n = \Delta_{n+1}p_{n-1} + m_{n+1}p_n$$

נכפיל ב$p_n$ משוואה ראשונה וב$q_n$ משוואה שנייה ונחסיר, יחד עם זאת ש $p_n q_{n-1} - q_{n-1}p_n = (-1)^{n-1}$ ונקבל $p_n^2 - d \cdot q_n^2 = (-1)^{n-1}\Delta_{n+1}$ . ■

בפרט נקבל ש$(p_{nr-1}, q_{nr-1})$ פתרונות למשוואת הפל.

**למה**: פתרון ל $x^2 - dy^2 = N$ כאשר $|N| < \sqrt{d}$ הוא מהצורה $(p_n, q_n)$ ל$n$ מסויים.

**הוכחה**: נשים לב ש

$$\left|\frac{x}{y} - \sqrt{d}\right| = \frac{|x^2 - dy^2|}{y(x + y\sqrt{d})} \leq \frac{\sqrt{d}}{y\left(x + y\sqrt{d}\right)} = \frac{1}{y\left(\frac{x}{\sqrt{d}} + y\right)} < \frac{1}{2y^2}$$

ולכן מהטענה על שברים משולבים נקבל את הרצוי. ■

בפרט נקבל שפתרון למשוואת הפל הוא בהכרח $(p_n, q_n)$ ש$\Delta_{n+1} = 1$ ולכן זה בדיוק במחזור. מכאן הוכחנו את המשפט הבא:

**משפט:** $\sqrt{d} = [a_0, \overline{a_1, a_2, \dots, a_r, 2 \cdot a_0}]$ הכתיב כשבר משולב. הסדרה $a_1, \dots, a_r$ היא פילנדרומית.

מתקיים ש $(p_{r-1}, q_{r-1})$ זה הפתרון היסודי למשוואת פל (אולי השלילית – בתלות בזוגיות $r$). כל הפתרונות למשוואת הפל זה $(p_{nr-1}, q_{nr-1})$ עבור $n \geq 1$.

■

**הערה על נוסחאות לייצור פתרון**: אפשר לייצר נוסחה טריגונומטרית שנותנת פתרון למשוואת פל. הדוגמה הפשוטה היא ש$\mathbb{Z}[\sqrt{p}] \subset \mathbb{Z}[\zeta_p]$ כאשר $p \equiv 1\ (4)$ . עכשיו אפשר לקחת את $1 - \zeta_p$ שהוא יוצר של הראשוני, לעשות לו נורמה לשדה הזה. מקבלים $\prod_{\left(\frac{k}{p}\right)=-1}(1 - \zeta_p^k)$ . נחלק את האיבר הזה ב$\sqrt{p}$ ונקבל $u$ יחידה בשדה.

הclass number formula מתרגם לעובדה שזה $\epsilon^h$ (אולי $2h$ לא לתבוע אותי) כאשר $h$ זה הclass number של $\mathbb{Z}[\sqrt{p}]$ .

באופן כללי לחוג שלמים יש את משפט היחידות של דירכלה שנותן את המבנה של היחידות - $O_K^\times = \mu_K \oplus \mathbb{Z}^{r+s-1}$ כאשר $\mu_K$ זה שורשי היחידה ו$r$ זה כמות השיכונים הממשים, ו$2s$ כמות השיכונים המרוכבים.

משפט Ljunggern (סעיף 18ב') – החלק שהוא $x^2 - 2y^4 = -1$ לא טריוויאלי בכלל, יש את הפתרון

$$239^2 - 2 \cdot 13^4 = -1$$

הערה על מעלה 3 – יש משפט בכללי ש$x^3 - dy^3 = 1$ הפתרון הוא רק הfundemental unit של $\mathbb{Z}[d^{1/3}]$ במידה והוא בצורה $\epsilon = x + y \cdot d^{\frac{1}{3}}$ .

בכללי יש את השאלה על משוואות נורמה ודומותיהן. יש כל מיני דרכים להתמודד – יש דרך $p$-אדית של סקולם . הרעיון שסדרות $n \mapsto c_1\alpha_1^n + \cdots + c_r\alpha_r^n$ אפשר להציב במקום $n$ שלם להציב $n$ ב$\mathbb{Z}_p$ לאיזשהו $p$ וכתוב פה פונקציה אנליטית ואז יהיה לה כמות סופית של פתרונות. למעשה אפשר בעזרת עקרון Rouché לחסום את כמות הפתרונות.
יש דרכים של קירובים דיופנטים - יש דרך צירופים לינארים של $\log$ של אלן בייקרס.
יש דרך קירובים דיופנטים של רות'.

כל אחד מאלו זה הרצאה מלאה [מאוד] בפני עצמו, יש גם התקדמויות חדשות בנושאים האלה.