

משוואת פל - Pell's equation

נתון $D \in \mathbb{N}$, D לא ריבוע (לא קיים $k \in \mathbb{N}$ כזה ש- $k^2 = D$).

מוסיף למצוא את כל הפתרונות היא טריוויאלים למשוואה - $x^2 - Dy^2 = 1$ ($x, y \in \mathbb{Z}$)

כאשר הפיתרון הטריוויאלי הוא $(x, y) = (\pm 1, 0)$

דוגמה - $D=2$, מוסיף לפתור את $x^2 - 2y^2 = 1$

פתרון אחד - $(3, 2)$

אפשר לקבל מפתרון זה פתרונות נוספים באופן הבא:
נשים לב ש- (x, y) פתרון, אז כל $(\pm x, \pm y)$ פתרון גם.

$$1 = x^2 - Dy^2 = (x + \sqrt{D}y)(x - \sqrt{D}y)$$

$$1^2 = 1 = (x + \sqrt{D}y)^2 (x - \sqrt{D}y)^2 = (x^2 + Dy^2)^2 - (2xy)^2 D$$

הצגה של $D=2$, $(x, y) = (3, 2)$ אז $2xy = 12$, $x^2 + Dy^2 = 17$.
גם $(17, 12)$ פתרון!

טענה - אם x, y פתרון למשוואת פל, אז לכל n חסמים:

אז $\bar{x}_n = x_n^2$, $\bar{y}_n = y_n^2$ כאשר x_n, y_n הם פתרונות למשוואת פל.

הוכחה - נאמן $(x + y\sqrt{D})^n = X + Y\sqrt{D}$

X, Y מקבלים דרך ביטוי נטון, והפוכות חזקות בזוגיות ואי בזוגיות

$$(x - y\sqrt{D})^n = X - Y\sqrt{D}$$

$$1 = 1^n = (x^2 - y^2 D) = (x + y\sqrt{D})^n (x - y\sqrt{D})^n = (x + Y\sqrt{D})(x - Y\sqrt{D}) =$$

$$= \underbrace{x^2}_{\bar{x}} - \underbrace{y^2 D}_{\bar{y}}$$

משפט 1 - לכל D כזה, יש למשוואת פל פתרון טריוויאלי.

משפט 2 - לכל D כזה ש- D אינו ריבוע, יש למשוואת פל פתרונות טריוויאליים, וההפך נכון.

כמו כן, קיים פתרון לא טריוויאלי (x_0, y_0) וכל פתרון אחר הוא מהצורה: $(\pm x_n, \pm y_n)$ כאשר x_n, y_n הם כאלו בטבלה.

הוכחת משפט 1

נמסן $\alpha = \sqrt{D}$. אז $\alpha \notin \mathbb{Q}$. ולפי משפט זיורסר, יש אינסוף זוגות מספרים p, q המקיימים:

$$(*) \quad \left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$$

(עדין את הביטוי $|p^2 - q^2 D|$ המקיים $(*)$)

$$|p^2 - q^2 D| = |p + q\alpha| |p - q\alpha| < |p + q\alpha| \cdot \frac{1}{q} = \left| \frac{p}{q} + \alpha \right| \leq \left| \frac{p}{q} - \alpha \right| + 2\alpha$$

שאלה $\alpha > 0$
חסום

הראינו שיש M כן שעל כן p, q המקיימים $(*)$, $|p^2 - q^2 D| \leq M$

המספרים $p^2 - q^2 D$ שלמים ושלם $p^2 - q^2 D = M$ איננו p, q עבורם $M \neq 0$.
כן שיש אינסוף p, q עבורם $M \neq 0$.

מספר המחלקות האפשריות $(p \bmod M, q \bmod M)$ הוא סופי ושלם p, q איננו p_i, q_i המקיימים $p_i^2 - q_i^2 D = M$ ושקיימים $p_i \equiv p_j \pmod{M}$ ו $q_i \equiv q_j \pmod{M}$.

$$\alpha + b\sqrt{D} = \frac{p_i - q_i \sqrt{D}}{p_j - q_j \sqrt{D}} = \frac{(p_i - q_i \sqrt{D})(p_j + q_j \sqrt{D})}{(p_j - q_j \sqrt{D})(p_j + q_j \sqrt{D})} = \frac{p_i p_j - q_i q_j D + (p_i q_j - p_j q_i) \sqrt{D}}{p_j^2 - q_j^2 D}$$

$$= \frac{p_i p_j - q_i q_j D + (p_i q_j - p_j q_i) \sqrt{D}}{M}$$

$$a = (p_i p_j - q_i q_j D) / M$$

$$b = (p_i q_j - p_j q_i) / M$$

$a + b\sqrt{D} \in \mathbb{Z}$ נבדוק שהיא שלם a והוא שלם b מתחלק a ב- M , זה ייתן לנו $p_i p_j - q_i q_j D \equiv p_i^2 - q_i^2 D \equiv M \equiv 0 \pmod{M}$ הוא a והוא שלם a מתחלק a ב- M , ולכן a שלם.

$$p_i q_j - p_j q_i \equiv p_i q_1 - p_1 q_i \equiv 0 \pmod{M}$$

הוא שלם b והוא שלם b .

~~הוכחה~~

סדרת עשר - $a + b\sqrt{D} = z \in \mathbb{Q}(\sqrt{D})$, $a - b\sqrt{D} = z'$ (הזוג z, z')
אם z היה מתחלק מכל צד את שני הצדדים.

$$\left(\frac{p_i - q_i \sqrt{D}}{p_j - q_j \sqrt{D}} \right) \left(\frac{p_i + q_i \sqrt{D}}{p_j + q_j \sqrt{D}} \right) = (a + b\sqrt{D})(a + b\sqrt{D})' = a^2 - b^2 D$$

$$= \frac{(p_i + q_i \sqrt{D})(p_i - q_i \sqrt{D})}{(p_j + q_j \sqrt{D})(p_j - q_j \sqrt{D})} = \frac{p_i^2 - q_i^2 D}{p_j^2 - q_j^2 D} = \frac{M}{M} = 1$$