משוואת פל - Pell's equation

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

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

כאשר הפיתרון הטריוויאלי הוא $(x,y)=(\pm1,0)$

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

פתרון אחד - $(3,2)$

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

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

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

בדוגמה שלנו $D=2$, $(x,y)=(3,2)$
אז $x^2+Dy^2=17$, $2xy=12$. גם $(17,12)$ פיתרון!

טענה - אם x,y פיתרון למשוואת פל, אז לכל n טבעיים:

$$\overline{x_n}+\overline{y_n}\sqrt{D}\,(x+y\sqrt{D})^n(x-y\sqrt{D})^n$$

אז $\overline{x_n}=x_n^2$, $\overline{y_n}=y_n^2$
כאשר x_n,y_n שלמים הם פתרונות למשוואת פל.

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

(X,Y מקבלים רק בינום ניוטון, והפרדת חזקות זוגיות ואי זוגיות)

אז $(x-y\sqrt{D})^n=X-Y\sqrt{D}$

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

$$=\underset{\overline{x}}{\underset{\downarrow}{X}}{}^2-\underset{\overline{y}}{\underset{\downarrow}{Y}}{}^2D$$

משפט 1 - לכל D כנ"ל, יש למשוואת פל פיתרון לא טריוויאלי.

משפט 2 - לכל D כנ"ל כל הפתרונות הלא טריוויאלים של משוואת פל מתקבלים מהטענה, ומהחלפת סימנים.
כלומר, קיים פיתרון לא טריוויאלי (x_0,y_0) וכל פיתרון אחר הוא מהצורה: $(\pm x_n,\pm y_n)$
כאשר x_n,y_n הם כמו בטענה.

הוכחת משפט 1

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

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

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

$$|p^2-q^2D|=|p+q\alpha||p-q\alpha|<|p+q\alpha|\cdot\frac{1}{q}=\left|\frac{p}{q}+\alpha\right|\le\underbrace{\left|\frac{p}{q}-\alpha\right|}_{\text{שואף ל-}0}+2\alpha$$

חסום.

הראינו שיש M_0 כך שלכל p,q המקיימים $(**)$, $|p^2-q^2D|\le M_0$

המספרים p^2-q^2D שלמים ולכן יש $m\in\mathbb{Z}$, $|m|\le M_0$ כך שיש אינסוף p,q עבורם $p^2-q^2D=m$.

מספר המחלקות האפשריות $(p \bmod m, q \bmod m)$ הוא סופי, ולכן יש אינסוף (p_i,q_i) שמקיימים $p_i^2-q_i^2D=m$, ולכן $i\ne j$
$p_i\equiv p_j \pmod{m}$
$q_i\equiv q_j \pmod{m}$

נקח $j<i$ ונבצע חילוק:

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

$$=\frac{p_ip_j-q_iq_jD+(p_iq_j-p_jq_i)\sqrt{D}}{m}$$

כאמר
$a=(p_ip_j-q_iq_jD)/m$
$b=(p_iq_j-p_jq_iD)/m$

נבדוק שהמונה של a המונה של b מתחלקים ב-m, זה ייתן לנו $a+b\in\mathbb{Z}$
המונה של a הוא $p_ip_j-q_iq_jD\equiv p_i^2-q_i^2D\equiv m\equiv 0 \pmod{m}$

כלומר המונה של a מתחלק ב-m, ולכן a שלם.

המונה של b הוא $p_iq_j-p_jq_i\equiv p_iq_i-p_iq_i\equiv 0 \pmod{m}$
ושוב b שלם.

טענת עזר - לכל $a+b\sqrt{D}=z\in\mathbb{Q}(\sqrt{D})$, נסמן $z'=a-b\sqrt{D}$ (הצמוד של z)
אז פעולת הצמדה מכבדת את פעולות השדה.

אז נקבל

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

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