Équation de Pell-Fermat

P. Caldero, J. Germoni, *Histoires hédonistes de groupes et de géométries, Tome second*, Calvage & Mounet. Proposition 1.5 page 388.

Recasage : 126.

Théorème 1

Soit $d \geq 2$ sans facteur carré et soit $\mathscr{H}$ l'hyperbole ayant pour équation $X^2 - dY^2 = 1$ dans le repère OXY du plan $\mathbb{R}^2$. Soit $M_0 = (1,0)$. On admet qu'il existe $M_1 = (X_1, Y_1) \in \mathscr{H}$ avec $X_1, Y_1 \in \mathbb{N}^*$ et Y_1 aussi petit que possible. Alors, l'ensemble des points entiers de la branche de $\mathscr{H}$ qui contient M_0 est le groupe engendré par M_1. L'ensemble des points entiers de $\mathscr{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

▷ *– Étape 1 : coordonnées de la loi de groupe.* Soit $\varphi : M \in \mathscr{H} \mapsto M_1 * M$. Calculons les coordonnées de $\varphi(M)$. Pour cela, on change de repère en posant :

$$\begin{cases} x = X + \sqrt{d}Y \\ y = X - \sqrt{d}Y \end{cases}$$

de sorte que $(x,y) \in \mathscr{H} \Leftrightarrow xy = 1$. Dans le repère Oxy, M_0 a pour coordonnées $(1,1)$ et notons (x_1, y_1) les coordonnées de M_1. Si $M \in \mathscr{H}$ a pour coordonnées (x,y) dans Oxy, alors $\varphi(M)$ a pour coordonnées $(x_1 x, y_1 y)$. En effet, la droite $\Delta_{M_1 M}$ a pour équation dans Oxy :

$$\bar{y} - 1 = \frac{y - y_1}{x - x_1}(\bar{x} - 1).$$

Ainsi, les coordonnées $(\bar{x}, \bar{y})$ de $\varphi(M)$ dans Oxy doivent satisfaire cette équation ainsi que $\bar{x}\bar{y} = 1$. On en déduit le résultat. Un calcul montre que dans le repère OXY, le point $\varphi(M)$ a pour équation $(XX_1 + dYY_1, X_1 Y + XY_1)$.

– Étape 2 : sous-groupe et définition d'un ordre. Notons $\mathscr{H}_0$ la branche de l'hyperbole contenant M_0. On a $(x,y) \in \mathscr{H}_0 \Leftrightarrow xy = 1$ et $x > 0$. Alors, le calcul de coordonnées effectué pour φ montre que $\mathscr{H}_0$ est un sous-groupe de $(\mathscr{H}, *)$, de même que $\mathscr{H}_0 \cap \mathbb{Z}^2$. De plus, la projection $(x,y) \in \mathscr{H}_0 \mapsto x \in \mathbb{R}_+^*$ est bijective donc on peut transporter l'ordre de $\mathbb{R}_+^*$ à $\mathscr{H}_0$. Remarquons que l'ordre peut se lire dans le repère Oxy sur la coordonnée x et dans le repère OXY sur la coordonnée Y en vertu de la relation $x = \sqrt{1 + dY^2} + \sqrt{d}Y$ (cette fonction de Y étant strictement croissante). Comme $x_1 > 1$, φ est strictement croissante.

– Étape 3 : $\mathscr{H}_0 \cap \mathbb{Z}^2$ est engendré par M_1. Pour $n \in \mathbb{Z}$, notons $M_n = M_1^n = \varphi^n(M_1) = (X_n, Y_n)$ dans OXY. Par définition de M_0, on a $M_{-1} = (X_1, -Y_1)$ et, par récurrence, $Y_{-n} = -Y_n$, $\forall n \in \mathbb{N}$.

Comme φ est strictement croissante et $\forall n \in \mathbb{Z}$, $M_{n+1} = \varphi(M_n)$, la suite $(M_n)_{n\in\mathbb{Z}}$ est strictement croissante. De plus, comme $\forall n \in \mathbb{N}$, $X_n \geq 1$ et $Y_1 \geq 1$, on a $Y_{n+1} > Y_n$ $\forall n \in \mathbb{Z}$. Comme $(Y_n)_{n\in\mathbb{N}} \subset \mathbb{N}$, on en déduit que $Y_n \xrightarrow[n\to\pm\infty]{} \pm\infty$.

Soit alors $M = (X,Y)$ un point entier de $\mathscr{H}_0$. D'après ce qui précède, il existe $n \in \mathbb{Z}$ tel que $Y_n \leq Y < Y_{n+1}$. Soit $M' = M_{-n} * M$. Comme φ est strictement croissante, φ^{-n} l'est également donc $M_0 \leq M' < M_1$. Comme on a supposé que M_1 était solution minimale de l'équation de Pell-Fermat, $M' = M_0$ et $M = M_n$. Ainsi, $\mathscr{H}_0 \cap \mathbb{Z}^2 = \langle M_1 \rangle$.

– Étape 4 : Ensemble des points entiers de $\mathscr{H}$. La réflexion $(X,Y) \mapsto (-X,Y)$ échange les branches et préserve $\mathbb{Z}^2$ donc $\mathscr{H} \cap \mathbb{Z}^2 = \{(\pm X_n, Y_n),\ n \in \mathbb{Z}\}$. On vérifie alors que l'application :

$$\begin{array}{ccc} \{\pm 1\} \times \mathbb{Z} & \to & \mathscr{H} \cap \mathbb{Z}^2 \\ (\varepsilon, n) & \mapsto & (\pm X_n, Y_n) \end{array}$$

est un isomorphisme (loi produit pour le premier groupe). □

Corollaire 2

Soit $d \geq 2$ sans facteur carré. Il existe une solution fondamentale (X_1, Y_1), coordonnée de $x_1 = X_1 + \sqrt{d}Y_1$ dans $\mathbb{Z}[\sqrt{d}]$, de l'équation de Pell-Fermat $X^2 - dY^2 = 1$ telle que l'ensemble des solutions soit les coordonnées dans $\mathbb{Z}[\sqrt{d}]$ de $\{\pm x_1^n,\ n \in \mathbb{Z}\}$.

Corollaire 3

Soit $d \geq 2$ sans facteur carré tel que -1 ne soit pas un carré modulo d. Alors $\mathbb{Z}[\sqrt{d}]^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

▷ Dans ce cas, un élément est inversible si et seulement si sa norme $X^2 - dY^2$ est égale à 1 : équation de Pell-Fermat. □