Équation de Pell-Fermat

Références : Caldero, Germoni, *Histoires hédonistes de groupes et de géométrie - Tome 2*, p 388

L'objectif est de résoudre l'équation de Pell-Fermat, i.e chercher les couples d'entiers (x, y) vérifiant $x^2 - dy^2 = 1$ avec d un entier supérieur ou égal à 2 sans facteur carré.

Théorème.

Soit d un entier naturel sans facteur carré et soit $\mathcal{H}$ l'hyperbole d'équation $X^2 - dY^2 = 1$ dans le plan $\mathbb{R}^2$. Soit $E = M_0 = (1, 0)$. **On admet l'existence de** $M_1 = (X_1, Y_1)$, un point de $\mathcal{H}$ où X_1 et Y_1 sont des entiers naturels avec $X_1^2 + Y_1^2$ aussi petit que possible. Alors l'ensemble des points entiers de la branche de $\mathcal{H}$ qui contient M_0 est le groupe engendré par M_1. L'ensemble des points entiers de $\mathcal{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Démonstration. • On calcule, en coordonnées, l'application $\varphi : M \in \mathcal{H} \mapsto M_1 \star M \in \mathcal{H}$. On pourrait le faire directement mais c'est compliqué. On va faire un changement de repère. On passe au repère OXY où M_0 a pour coordonnées $(1, 1)$, en posant

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

Notons (x_1, y_1) les coordonnées de M_1 dans ce repère. Si un point M a pour coordonnées (X, Y) dans le premier repère et (x, y) dans le deuxième, alors $M_1 \star M$ a pour coordonnées $(x_1 x, y_1 y)$ dans le deuxième repère et

$$(X', Y') = (X_1 X + dY_1 Y, Y_1 X + X Y_1)$$

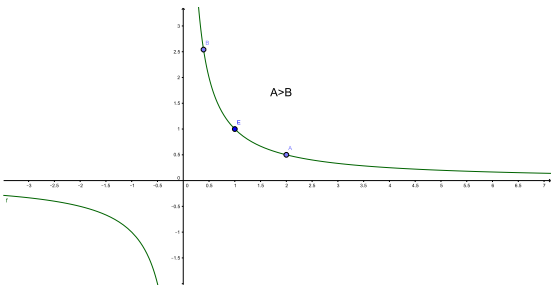
dans le premier.
En effet, la droite parallèle à $(M_1 M)$ passant par E a pour équation

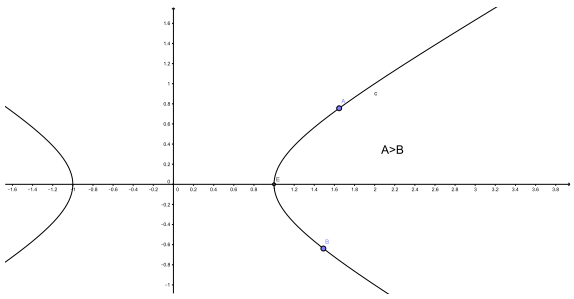
$$\tilde{y} - 1 = \frac{y - y_1}{x - x_1}(\tilde{x} - 1).$$

$\varphi(M)$ est donc l'intersection de cette droite avec l'hyperbole $\tilde{y} = \dfrac{1}{\tilde{x}}$. On trouve facilement le résultat attendu après quelques calculs.

• L'hyperbole $\mathcal{H}$ est la réunion de deux branches. On appelle $\mathcal{H}_0$ celle qui contient E.
On remarque que $(x, y) \in \mathcal{H}_0$ si et seulement si $(x, y) \in \mathcal{H}$ et $x > 0$. Comme $x_1 > 0$, il s'ensuit que $\mathcal{H}_0$ est stable par φ et forme même un sous-groupe de $\mathcal{H}$ pour $*$.

• On remarque que $p : (x, y) \in \mathcal{H}_0 \mapsto x \in \mathbb{R}^{+*}$ est bijective. On peut donc mettre l'ordre de $\mathbb{R}^{+*}$ sur $\mathcal{H}_0$.
De plus, $x = \sqrt{1 - dY^2} + \sqrt{d}Y$ (car $X^2 - dY^2 = 1$). Cette fonction de Y est strictement croissante donc l'ordre se lit indifféremment sur la coordonnée x ou sur la coordonnée Y.
Pour cet ordre, la fonction φ est strictement croissante sur $\mathcal{H}_0$ car $x_1 > 1$ (car $X_1 \geqslant 1$ et $Y_1 \geqslant 0$).





• Pour tout n entier, posons $M_n = M_1^n = (X_n, Y_n)$. Il est immédiat que $M_{-1} = (X_1, -Y_1)$ d'où on tire par récurrence que $Y_{-n} = -Y_n$ pour tout n entier. Comme φ est strictement croissante et que $M_{n+1} = \varphi(M_n)$, la

suite (M_n) est strictement croissante. De plus, comme $X_1 \geqslant 1$, $Y_1 > 0$ et $X_n \geqslant 1$ pour tout n, $Y_{n+1} > Y_n$ pour tout $n \in \mathbb{Z}$. Comme les Y_n sont entiers, (Y_n) diverge vers $+\infty$.

• Soit $M = (X, Y)$ un point entier de $\mathcal{H}_0$. D'après ce qui précède, il existe un entier n tel que $Y_n \leqslant Y < Y_{n+1}$, donc $M_n \leqslant M < M_{n+1}$. Notons $M' = (X', Y') = M_{-n} \star M$. Grâce à la croissance stricte de φ, donc de φ^{-n}, on a $M_0 \leqslant M' < M_1$. Mais, par hypothèse, M_1 est la solution entière minimale de l'équation de Pell-Fermat, donc $M' = M_0$ puis $M = M_n$.

• On remarque pour terminer que la réflexion $\sigma : (X, Y) \mapsto (-X, Y)$ échange les deux branches de $\mathcal{H}$ et préserve $\mathbb{Z}^2$, et on peut affirmer que les points entiers de $\mathcal{H}$ sont les $(\pm X_n, Y_n)$ pour $n \in \mathbb{Z}$.
Comme les Y_n sont symétriques, on peut même dire que les points entiers sont les $\pm M_n$ pour $n \in \mathbb{Z}$.
On pose l'application

$$\begin{array}{rcl} \Gamma & \to & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \\ \varepsilon M_n & \mapsto & (\varepsilon, n) \end{array}$$

et on vérifie qu'elle forme bien un morphisme de groupes.
L'ensemble des points entiers de $\mathcal{H}$ forme donc bien un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. □

Corollaire.

Soit d un entier naturel supérieur ou égal à 2 et sans facteur carré, alors il existe une solution fondamentale $x_1 = X_1 + \sqrt{d}Y_1$ solution de l'équation de Pell-Fermat $X^2 - dY^2 = 1$ telle que l'ensemble des solutions soit $\{\pm x_1^n, n \in \mathbb{Z}\}$.

Démonstration. Les solutions de l'équation de Pell-Fermat sont exactement les points entiers de l'hyperbole précédente. □

Corollaire.

Soit d un entier naturel supérieur ou égal à 2 et sans facteur carré et tel que (-1) ne soit pas un carré modulo d, soit $A = \mathbb{Z}[\sqrt{d}]$, alors $A^\times \simeq \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Démonstration. Les inversibles de A sont les éléments de norme ± 1, en prenant la norme de $\mathbb{Q}(\sqrt{d})$ [1].
Les inversibles sont donc les points entiers des hyperboles $X^2 - dY^2 = \pm 1$. On connaît les points entiers de $X^2 - dY^2 = 1$. L'idée est donc de montrer qu'il n'y a pas de points entiers non triviaux sur $X^2 - dY^2 = -1$.
Si c'était le cas, on aurait $X^2 \equiv -1[d]$, ce qui est absurde car (-1) n'est pas un carré modulo d. □

Remarques : • Le problème des bœufs d'Hélios se résout à l'aide d'une équation de Pell-Fermat. L'entier d correspondant est de l'ordre de 10^{14}...
• La solution fondamentale de $X^2 - 15Y^2 = 1$ est $(4, 1)$. On peut ainsi trouver toutes les solutions. Pour cela, on écrit $x_n = x_1^n$ et soit on développe, soit on trouve une relation de récurrence suivie par X_n et Y_n.
Ici on a

$$x_{n+1} = (4 + \sqrt{15})x_n = (4 + \sqrt{15})(X_n + \sqrt{15}Y_n) = (4X_n + 15Y_n) + \sqrt{15}(X_n + 4Y_n),$$

d'où

$$\begin{array}{l} X_{n+1} = 4X_n + 15Y_n \\ Y_{n+1} = X_n + 4Y_n \end{array}.$$

• La solution fondamentale de $X^2 - 19Y^2 = 1$ est $(170, 39)$. C'est plus difficile à trouver. Il y a donc encore du travail à faire.
Pour prouver l'existence de la solution fondamentale, on utilise des développements en fraction continue. Cela donne explicitement (X_1, Y_1), mais c'est compliqué...
• Si d est premier et $d \equiv 3[4]$, on sait que (-1) n'est pas un carré modulo d. On a donc les exemples $d = 3, 7, 11, 19, ...$
Si $d = 15$, on a $\left(\dfrac{-1}{15}\right) = -1$ donc (-1) n'est pas un carré modulo 15. On peut donc aussi appliquer le corollaire dans ce cas là.

1. A n'est pas toujours l'anneau des entiers de $\mathbb{Q}(\sqrt{d})$, mais ça ne change rien à la caractérisation de ses inversibles. On a toujours $A^\times \subset \mathcal{O}(\mathbb{Q}(\sqrt{d}))^\times$. L'inverse reste le conjugué.

• En fait, le corollaire reste vrai même quand (-1) est un carré modulo d, c'est le théorème des unités de Dirichlet, mais c'est plus difficile à prouver.

Adapté du travail de Paul Alphonse.