DVP Équation de Pell-Fermat

Antoine Dequay

21 septembre 2022

Notes

— Prof : .

— Leçons : 108, 126, 191.

— Références :

  — H2G2 tome 2.

Théorème 1 Soit $d \in \mathbb{N}$ sans facteur carré et $\mathcal{H}$ l'hyperbole ayant pour équation $X^2 - dY^2 = 1$ dans $\mathbb{R}^2$. Soit $M_0 = (1,0)$. On admet l'existence de $M_1 = (X_1, Y_1) \in \mathcal{H}$ point à coordonnées entières avec $X_1^2 + Y_1^2$ minimal. 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 de $\mathcal{H}$ forme un sous-groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Preuve. On calcule en coordonnées l'application $\varphi : \begin{pmatrix} \mathcal{H} & \longrightarrow & \mathcal{H} \\ M & \longmapsto & M_1 * M \end{pmatrix}$. Pour simplifier les calculs, au lieu de se placer dans le repère, on choisit le repère Oxy tel que $\mathcal{H}$ ait pour équation $xy = 1$ et $M_0 = (1,1)$. Pour cela, on pose :

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

On note $M_1 = (x_1, y_1)$ dans ce repère. Pour $M = (X, Y)$ dans le premier repère, (x, y) dans le second, $M_1 * M = (x_1 x, y_1 y)$ dans ce dernier, et $(X', Y') = (X_1 X + dY_1 Y, Y_1 X + dX_1 Y)$ dans le premier, car on doit résoudre le système

$$\begin{cases} \tilde{y} - 1 = \dfrac{y - y_1}{x - x_1}(\tilde{x} - 1) \text{ équation de la droite parallèle à } (M_1 M) \text{ passant pas } M_0, \\ \tilde{y}\tilde{x} = 1. \end{cases}$$

On remarque que

$$X' + \sqrt{d}Y' = (X_1 + \sqrt{Y_1})(X + \sqrt{d}Y).$$

L'hyperbole $\mathcal{H}$ est la réunion de 2 branches (ses composantes connexes). On appelle $\mathcal{H}_0$ celle contenant M_0.

On remarque que $(x, y) \in \mathcal{H}_0$ ssi $(x, y) \in \mathcal{H}$ et $x > 0$. Comme $x_1 > 0$, $\mathcal{H}_0$ est stable par φ, et forme même un sous-groupe de $(\mathcal{H}, *)$.

On remarque que $p : (x, y) \in \mathcal{H}_0 \mapsto x \in \mathbb{R}^{+*}$ est bijective, donc on peut mettre l'ordre de $\mathbb{R}^{+*}$ sur $\mathcal{H}_0$. De plus, $x = \sqrt{1 - dY^2} + \sqrt{d}Y$. Cette fonctionne est strictement croissante en Y, donc l'ordre peut se lire selon x ou Y. Faire dessin

On note pour $n \in \mathbb{Z}$ $M_n := M_1^n = (X_n, Y_n)$. On a $M_{-1} = (X_1, -Y_1)$, donc il vient par récurrence $Y_{-n} = -Y_n$. Par définition de l'ordre et de φ, φ est strictement croissante, et comme $M_{n+1} = \varphi(M_n)$, M_n est strictement croissante.

De plus, comme $X_1 \geq 1$, $Y_1 > 0$ et $X_n \geq 1$, il vient $Y_{n+1} > Y_n$. Les Y_n étant entiers, la suite tend vers $+\infty$.

Ainsi, pour tout $M = (X, Y) \in \mathcal{H}_0$ à coordonnées entières, il existe $n \in \mathbb{N}$ tel que $Y_n \leq Y < Y_{n+1}$, donc $M_n \leq M < M_{n+1}$. En notant $M' = (X', Y') = M_{-n} * M$, comme φ est strictement croissante (donc φ^{-n} l'est), on a $M_0 \leq M < M_1$. Par minimalité de M_1, $M' = M_0$, donc

$M = M_n$. Cela montre le premier point du théorème.

Enfin, comme $\sigma : (X, Y) \mapsto (-X, Y)$ échange les deux branches de $\mathcal{H}$ tout en préservant $\mathbb{Z}^2$, les points entiers de $\mathcal{H}$ sont exactement les $(\pm X_n, Y_n)_{n\in\mathbb{Z}}$. Par symétricité des Y_n, ces points sont même exactement les $\pm M_n$. L'isomorphisme recherché est donc

$$\begin{pmatrix} \mathcal{H} & \longrightarrow & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z} \\ \varepsilon M_n & \longmapsto & (\varepsilon, n) \end{pmatrix}.$$

□

Corollaire 2 Soit $d \in \mathbb{N}\backslash\{0, 1\}$ sans facteur carré, alors il existe une solution fondamentale $x_1 = X_1 + \sqrt{d}Y_1$ de $X^2 + dY^2 = 1$ telle que l'ensemble solution soit $\{\pm x_1, n \in \mathbb{Z}\}$.

Preuve. Immédiat.

□

Corollaire 3 Soit $d \in \mathbb{N}\backslash\{0, 1\}$ sans facteur carré tel que -1 ne soit pas un carré modulo d et soit $A = \mathbb{Z}[\sqrt{d}]$. Alors $A^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

Preuve. Les inversibles de A sont des éléments de norme ± 1 pour la norme $\mathbb{Q}(\sqrt{d})$. Ce sont donc les solutions de $X^2 - dY^2 = \pm 1$. Par ce qui précède, il reste à montrer que $X^2 - dY^2 = -1$ ne possède pas de solutions entières non triviales. Si c'était le cas, on aurait $X^2 \equiv -1 \ (mod\ d)$, ce qui est absurde, d'où le résultat.

□

Remarque Cf. `https://agreg-maths.fr/uploads/versions/866/Equation_Pell_Fermat.pdf` + théorème des unités de Dirichlet.