# Développement: Équation de Mordell

Arthur Maritch-Roy

Une *équation de Mordell* est une équation diophantienne de la forme

$$y^2 = x^3 + k$$

pour $k \in \mathbb{Z}$. Mordell à démontré en 1920 que ces équations avaient toujours un nombre fini de solutions.

Pour résoudre ces équations, on les met souvent sous la forme

$$x^3 = (y - \sqrt{k})(y + \sqrt{k})$$

avec $\sqrt{k} = \mathrm{i}\sqrt{-k}$ si $k$ est négatif. Cette forme invite donc à se placer dans l'anneau $\mathbb{Z}[\sqrt{k}]$. Lorsque celui-ci possède de bonnes propriétés, on a bon espoir de pouvoir résoudre l'équation.

**Théorème 1.** L'anneau $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ est euclidien donc principal donc factoriel.

***Démonstration.*** On considère la norme $N(z = a + \mathrm{i}\sqrt{2}b) = a^2 + 2b^2$. C'est une application multiplicative à valeurs positives et qui vaut 0 si et seulement si $z = 0$. On montre que les inversibles de $Z[\mathrm{i}\sqrt{2}]$ sont les éléments de norme inversible dans $\mathbb{Z}$ donc les éléments de norme 1 donc $\pm 1$. Si $z$ et $w$ sont deux éléments de $\mathbb{Z}[\mathrm{i}\sqrt{2}]$ avec $w$ non nul, on note $\frac{z}{w} =: x + \mathrm{i}y\sqrt{2}$. On considère alors $q := c + \mathrm{i}d\sqrt{2}$ avec $c$ et $d$ les entiers les plus proches respectivement de $x$ et $y$. On a alors :

$$\left|\frac{z}{w} - q\right|^2 = |x - c|^2 + 2|y - d|^2 \leq \frac{1}{4} + \frac{2}{4} < 1$$

donc si $r := z - qw$, alors

$$N(r) = N(w)\left|\frac{z}{w} - q\right| < N(w).$$

Ainsi $z = qw + r$ est une division euclidienne de $z$ par $w$ pour la jauge $N$, ce qui montre que notre anneau est bien euclidien. □

**Théorème 2.** L'équation de Mordell pour $k = -2$ a pour uniques solutions $(3, 5)$ et $(3, -5)$.

***Démonstration.*** Supposons qu'il existe une solution $(x, y)$. On cherche alors des premières informations sur $x$ et $y$. Supposons que $x$ soit pair, on a :

$$y^2 \equiv 6 \mod 8$$

on peut alors vérifier que 6 n'est pas un carré dans $\mathbb{Z}/8\mathbb{Z}$ donc $x$ est impair. Maintenant, on se ramène comme annoncé à $\mathbb{Z}[\mathrm{i}\sqrt{2}]$. On part donc de

$$x^3 = y^2 + 2 = (y + \mathrm{i}\sqrt{2})(y - \mathrm{i}\sqrt{2}).$$

Montrons alors que $y \pm \mathrm{i}\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[\mathrm{i}\sqrt{2}]$. On considère pour cela $p \in \mathbb{Z}[\mathrm{i}\sqrt{2}]$ un diviseur commun à $y + \mathrm{i}\sqrt{2}$ et $y + \mathrm{i}\sqrt{2}$. Ainsi $p$ divise leur différence donc $p|2\mathrm{i}\sqrt{2}$. En passant à la norme et en utilisant sa multiplicativité, on obtient $N(p)|8$. Or $N(p)$ est un nombre impair puisque l'on a par ailleurs $N(p)|N(y + \mathrm{i}\sqrt{2}) = x^3$. Nécessairement, $N(p) = 1$ donc $p$ est inversible, on a donc bien la primalité relative. Par unicité de la décomposition en produit

d'irréductibles, $y + \mathrm{i}\sqrt{2}$ et $y - \mathrm{i}\sqrt{2}$ sont donc associés à des cubes puisqu'ils sont premiers entre eux et que leur produit est un cube. On écrit alors

$$y + \mathrm{i}\sqrt{2} = u\alpha^3 \text{ et } y - \mathrm{i}\sqrt{2} = v\beta^3$$

avec $u$ et $v$ inversibles et $\alpha$ et $\beta$ dans $\mathbb{Z}[\mathrm{i}\sqrt{2}]$. On peut donc écrire $y + \mathrm{i}\sqrt{2} = (m + \mathrm{i}n\sqrt{2})^3$ et identifier parties réelle et imaginaire :

$$y = m^3 - 6mn^2 = m(m^2 - 6n^2) \text{ et } 1 = 3m^2n - 2n^3 = (3m^2 - 2n^2)n.$$

On voit directement que $n = \pm 1$. Si $n = 1$, on alors $3m^2 - 2 = 1$ donc $m = \pm 1$ *i.e.* $y = \pm 5$. Si $n = -1$ alors $1 = 3m^2$ ce qui n'est pas possible. Par conséquent $y = \pm 5$ donc $x = 3$. On vérifie réciproquement que ce sont bien des solutions. □

**Remarque 1.** La preuve du caractère euclidien puis la résolution de l'équation remplissent le format du développement. On aurait pu aussi résoudre de la même manière le cas $k = -1$ mais cela serait trop rapide et cela permet d'introduire un anneau encore différent.

**Théorème 3.** L'équation de Mordell pour $k - 1$ admet pour unique solution $(1, 0)$.

***Démonstration.*** On se place dans $\mathbb{Z}[\mathrm{i}]$ et tout est alors similaire jusqu'à arriver à $y + \mathrm{i} = (m+\mathrm{i}n)^3$. On identifie alors encore les parties réelle et imaginaire ; les valeurs changent légèrement, mais on conclut de manière simple comme dans le cas précédent. □

**Référence :** Duverney, *Théorie des nombres.*