Équation diophantienne $x^2 + 2y^2 = n$.

2013 – 2014

Référence : Daniel Perrin, *Cours d'algèbre*, Ellipses, 1996, p.56.

Il s'agit de donner une condition nécessaire et suffisante sur $n \in \mathbb{N}$ pour que l'équation diophantienne $x^2 + 2y^2 = n$ admette une solution.

On pose $\Sigma := \{a^2+2b^2 \mid a, b \in \mathbb{Z}\}$ et on considère $\mathbb{Z}[i\sqrt{2}]$ muni de $N : z \mapsto z\bar{z}$, *i.e.* $N(a + ib\sqrt{2}) = a^2 + 2b^2$. On a alors $N(\mathbb{Z}[i\sqrt{2}]) = \Sigma$.

N est multiplicative donc Σ est stable par multiplication.

Théorème.
Soit p premier, alors

$$p \in \Sigma \iff p = 2 \text{ ou } p \equiv 1 \text{ ou } 3[8].$$

Lemme.
$p \in \Sigma \iff$ *p n'est pas irréductible dans $\mathbb{Z}[i\sqrt{2}]$.*

Démonstration. On commence par remarquer que pour $z \in \mathbb{Z}[i\sqrt{2}], z$ est inversible si et seulement si $N(z) = 1$. En effet, si $N(z) = 1$, alors $z\bar{z} = 1$ donc z est inversible. Réciproquement, si $zz' = 1$, alors $N(z)N(z') = N(1) = 1$ donc $N(z) = 1$.

- $\Rightarrow$: Si $p = a^2 + 2b^2$, on a $p = N(z) = z\bar{z}$ avec $z = a + ib\sqrt{2}$ et $N(z) = N(\bar{z}) \neq 1$ (car p est premier) donc z et $\bar{z}$ ne sont pas inversibles et p n'est pas irréductible dans $\mathbb{Z}[i\sqrt{2}]$.
- $\Leftarrow$: Si $p = zz'$ avec $z, z' \notin \mathbb{Z}[i\sqrt{2}]^\times$, on a $N(p) = N(z)N(z') = p^2$ et $N(z), N(z') \neq 1$, donc $p = N(z)$ (car p est premier), donc $p \in \Sigma$.

□

Démonstration du théorème. $2 = 0^2 + 2 \times 1^2$ donc $2 \in \Sigma$.

On suppose p premier impair.

$\mathbb{Z}[i\sqrt{2}]$ est factoriel (car euclidien) donc

$$\begin{aligned} p \text{ est réductible} &\iff (p) \text{ n'est pas premier} \\ &\iff \mathbb{Z}[i\sqrt{2}]/(p) \text{ n'est pas intègre.} \end{aligned}$$

Or $\mathbb{Z}[i\sqrt{2}] \simeq \mathbb{Z}[X]/(X^2 + 2)$ donc

$$\mathbb{Z}[i\sqrt{2}]/(p) \simeq \mathbb{Z}[X]/(X^2 + 2, p) \simeq \mathbb{F}_p[X]/(X^2 + 2).$$

D'où

$$\begin{aligned}(p) \text{ n'est pas premier} &\iff X^2+2 \text{ est réductible sur } \mathbb{F}_p \\ &\iff X^2+2 \text{ admet une racine dans } \mathbb{F}_p \\ &\iff -2 \text{ est un carré de } \mathbb{F}_p \\ &\iff \left(\frac{-2}{p}\right) = 1.\end{aligned}$$

Or

$$\left(\frac{-2}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} (-1)^{\frac{p^2-1}{8}}.$$

On a alors $(-1)^{\frac{p-1}{2}} = 1 \iff p \equiv 1[4]$ et $(-1)^{\frac{p^2-1}{8}} = 1 \iff p \equiv \pm 1[8]$, donc

$$\left(\frac{-2}{p}\right) = 1 \iff p \equiv 1 \text{ ou } 3[8].$$

□

Théorème.
Soit $n \geq 2$ et $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ sa décomposition en facteurs premiers.

Alors $n \in \Sigma$ si et seulement si pour tout $p \in \mathcal{P}$ vérifiant $p \equiv -1$ ou $-3[8]$, $v_p(n)$ est pair.

Démonstration. $\Leftarrow$: Σ est stable par multiplication et un carré est dans Σ.

$\Rightarrow$: Soit $p \equiv -1$ ou $-3[8]$, montrons le résultat par récurrence sur $v_p(n)$.

Si $v_p(n) = 0$, alors $v_p(n)$ est pair.

Sinon, p divise $n = a^2 + 2b^2 = (a + ib\sqrt{2})(a - ib\sqrt{2})$ et p est irréductible dans $\mathbb{Z}[i\sqrt{2}]$ (car $p \notin \Sigma$) donc on peut supposer sans perdre en généralité que p divise $a + ib\sqrt{2}$. Or $p \in \mathbb{Z}$ donc $p \mid a$ et $p \mid b$, donc $p^2 \mid n$.

Si on pose $a = pa'$ et $b = pb'$, alors $\frac{n}{p^2} = a'^2 + 2b'^2 \in \Sigma$ et $v_p\left(\frac{n}{p^2}\right) = v_p(n) - 2 \equiv 0[2]$ par hypothèse de récurrence.

Donc $v_p(n) \equiv 0[2]$.

□

Remarque. Cette démonstration s'adapte pour traiter l'équation $x^2 - dy^2 = p$ dès que $\mathbb{Z}[\sqrt{d}]$ (avec convention $\sqrt{-1} = i$) est euclidien, il suffit alors de calculer $\left(\frac{d}{p}\right)$ pour avoir le résultat. C'est le cas pour $d = -2, -1, 2, 3, 6, 7, 11, 19$. Toutefois, pour $d > 0$, on va seulement avoir p réductible dans $\mathbb{Z}[\sqrt{d}] \iff \pm p \in \Sigma$, ce qui ne donnera l'existence de solutions que pour $\pm p$. Cela vient du fait que la norme d'un élément de $\mathbb{Z}[\sqrt{d}]$ peut-être négative pour $d > 0$. Par exemple, pour $d = 3$, 3 est bien réductible dans $\mathbb{Z}[\sqrt{3}]$ mais $x^2 - 3y^2 = 3$ n'a pas de solutions car en réduisant modulo 3 on obtient que $3 \mid x$, donc $x^2 - 3y^2 = 3$ a des solutions si et seulement si $3x^2 - y^2 = 1$ en a, or en réduisant à nouveau modulo 3 on trouve que $y^2 \equiv -1[3]$, ce qui n'est pas possible. Par contre, $x^2 - 3y^2 = -3$ a une solution triviale.

Détails supplémentaires

– $\mathbb{Z}[i\sqrt{2}]$ est euclidien :
Soit $t, z \in \mathbb{Z}[i\sqrt{2}] \setminus \{0\}$, alors $\frac{z}{t} = x + iy\sqrt{2} \in \mathbb{C}$.
Soit $q = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ tel que $|x - a| \leq \frac{1}{2}$ et $|y - b| \leq \frac{1}{2}$.
Alors

$$\left|\frac{z}{t} - q\right| \leq \sqrt{\frac{1}{4} + \frac{1}{2}} < 1.$$

Soit $r := z - qt \in \mathbb{Z}[i\sqrt{2}]$, alors

$$|r| = |t| \left|\frac{z}{t} - q\right| < |t|$$

donc $N(r) < N(t)$.
D'où $z = qt + r$ avec $N(r) < N(t)$.