Équation de Nagell-Ramanujan

Références : Francinou, Gianella, *Exercices de mathématiques pour l'agrégation - Algèbre 1*, p 166-171
Un corrigé de partiel sur la page de Lionel Fourquaux : `https://www.normalesup.org/~fourquau/pro/teaching/2011-2012/thno/exam1-corrige.pdf`

Théorème.

L'équation diophantienne $x^2 + 3 = 2^n$ n'admet que deux solutions (x, n) : $(1, 2)$ et $(-1, 2)$.

Démonstration. • On commence par remarque que x doit être impair et que $n \geqslant 2$.
Supposons que $n = 2p$ soit pair. Alors on peut factoriser l'équation en $3 = (2^p - x)(2^p + x)$.
Les seuls diviseurs de 3 étant 1 et 3, on a seulement deux solutions : $(1, 2)$ et $(-1, 2)$.

• On prend n impair plus grand que 3, d'où $x^2 + 3 \equiv 0[4]$.
L'équation est équivalente à $\dfrac{x^2+3}{4} = \dfrac{x+i\sqrt{3}}{2}\dfrac{x-i\sqrt{3}}{2} = 2^m$ avec $m = n - 2$.
Comme x est impair, on peut l'écrire $x = 2k + 1$ et on a $(k + j)(k + j^2) = 2^m$.
On a besoin d'un lemme pour continuer.

Lemme.

L'anneau $\mathbb{Z}[j]$ est euclidien et $\mathbb{Z}[j]^\times = \{\pm 1, \pm j, \pm j^2\}$.

Démonstration. • La norme N est celle du corps quadratique $\mathbb{Q}(i\sqrt{3})$ associé à $\mathbb{Z}[j]$, elle est définie par

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

Soient $x, y \in \mathbb{Q}$, montrons que l'on peut trouver $z_0 = x_0 + jy_0 \in \mathbb{Z}[j]$ tel que $N(z - z_0) < 1$, avec $z = x + i\sqrt{3}y$.
On a

$$N(z - z_0) = \left(x - x_0 + \frac{y_0}{2}\right)^2 + 3\left(y - \frac{y_0}{2}\right)^2.$$

On choisit donc y_0 l'entier le plus proche de $2y$, puis x_0 l'entier le plus proche de $x - \dfrac{y_0}{2}$, ainsi on a

$$\begin{aligned} N(z - z_0) &\leqslant \left(\frac{1}{2}\right)^2 + 3\left(\frac{1}{4}\right)^2 \\ &\leqslant \frac{1}{4} + \frac{3}{16} = \frac{7}{16} < 1. \end{aligned}$$

Maintenant prenons z_1 et z_2 dans $\mathbb{Z}[j]$, et prenons $z_0 \in \mathbb{Z}[j]$ tel que $N\left(\dfrac{z_1}{z_2} - z_0\right) < 1$.
Alors il vient $z_1 = z_0 z_2 + z_2\left(\dfrac{z_1}{z_2} - z_0\right)$ et $N\left(z_2\left(\dfrac{z_1}{z_2} - z_0\right)\right) = N(z_2)N\left(\dfrac{z_1}{z_2} - z_0\right) < N(z_2)$.
L'anneau $\mathbb{Z}[j]$ est bien euclidien.

• Pour trouver les unités, il suffit de résoudre $N(x + yj) = 1$.
Cela donne $\left(x - \dfrac{y}{2}\right)^2 + \dfrac{3y^2}{4} = 1$.
D'où $x^2 + y^2 - xy = 1$.
Puis

$$1 = |x^2 + y^2 - xy| \geqslant x^2 + y^2 - |xy| \geqslant \frac{x^2 + y^2}{2}.$$

Donc $x^2 + y^2 \leqslant 2$ et les seuls cas possibles sont $x, y \in \{-1, 0, 1\}$.
On retrouve bien l'ensemble $\{\pm 1, \pm j, \pm j^2\}$. □

• Montrons que 2 est irréductible dans $\mathbb{Z}[j]$.
Si $2 = ab$, avec $N(a)$, $N(b) \neq 1$, alors $4 = N(2) = N(a)N(b)$, donc $N(a) = N(b) = 2$. Mais il n'existe pas d'élément de $\mathbb{Z}[j]$ de norme 2.
En effet, si $N(x + jy) = 2$, on a $x^2 + y^2 - xy = 2$, donc $x^2 + y^2 \leqslant 4$. Donc x et y sont entre -2 et 2. On vérifie qu'aucun des nombres possibles n'est de norme 2.

• Comme $\mathbb{Z}[j]$ est euclidien, il est factoriel, donc par unicité de la décomposition en irréductibles, l'équation $(k + j)(k + j^2) = 2^m$ donne $k + j = \alpha 2^l$ et $k + j^2 = \alpha^{-1}2^{m-l}$ avec $0 \leqslant l \leqslant m$.
α ne peut être réel, donc c'est soit $\pm j$, soit $\pm j^2$.
Or dans ce cas, en prenant la partie imaginaire, on a $\pm\dfrac{\sqrt{3}}{2} = \dfrac{\sqrt{3}}{2}2^l$ et $\pm\dfrac{\sqrt{3}}{2} = \dfrac{\sqrt{3}}{2}2^{m-l}$.
Comme on ne peut avoir $l = m - l = 0$, on a une absurdité, ce qui conclut la preuve. □

Remarques : • Tristement, il y a une manière triviale de résoudre cette équation. En effet, dans $\mathbb{F}_3$, l'équation diophantienne est $x^2 = (-1)^n$. Donc si n est impair, -1 est un carré modulo 3, ce qui est faux.
On peut tout de même garder ce développement car la vraie équation de Nagell-Ramanujan est $x^2 + 7 = 2^n$. Pour celle-ci, il n'y a plus d'absurdité mais le raisonnement est trop complexe pour tenir en 15 minutes.
• Ce développement ressemble au théorème des deux carrés dans les outils utilisés. Je ne pense pas que faire les deux en développement soit une bonne idée.
• Rappelons l'idée de pourquoi l'anneau des entiers algébriques de $\mathbb{Q}(\sqrt{d})$ est $\mathbb{Z}[\sqrt{d}]$ si $d \equiv 2, 3[4]$ et $\mathbb{Z}\left[\dfrac{1+\sqrt{d}}{2}\right]$ si $d \equiv 1[4]$.
Si on prend un élément non rationnel, son polynôme minimal est $X^2 - \mathrm{Tr}(\alpha)X + N(\alpha)$. Les entiers algébriques sont donc les éléments de trace et de norme entière.
Il s'agit ensuite de détailler ce que cela veut dire sur α et on trouve le résultat.

Adapté du travail de Alexandre Bailleul.