Corentin Bergeron ENS Rennes

L'unique entier entre un carré et un cube

Développement un peu original portant sur la résolution d'une équation diophantienne, avec une application rigolotte porant sur le nombre 26. J'ai fournit une première version avec une alternative, suivant les leçons. La preuve repose sur des arguments basiques de résolutions d'équations diophantiennes, et est à mettre en parallèle avec par exemple le développement sur $\mathbb{Z}[i]$ et les sommes de deux carrés.

Côté recasage, la première version convient très bien pour les leçons 127 et 142. Cela rentre cependant un peu moins bien pour la leçon 122, d'où la version alternative qui corrige le pas (mais qui utulise des théorèmes un peu avancés, et qui ne conviendrait pas à tous les candidats).

I - Le développement

Théorème 1

$\mathbb{Z}[i\sqrt{2}]$ est un anneau euclidien.

Preuve :

Pour $a,\ b \in \mathbb{Z}[i\sqrt{2}]$, $b \neq 0$, considérons les rationnels $x,\ y \in \mathbb{Q}$ tels que $\frac{a}{b} = x + i\sqrt{2}y$. On cherche $q \in \mathbb{Z}[i\sqrt{2}]$ vérifiant l'inégalité :

$$\left|\frac{a}{b} - q\right| < 1.$$

Pour cela, posons

$$q = \lfloor x + 1/2 \rfloor + i\sqrt{2}\lfloor y + 1/2 \rfloor.$$

On obtient alors l'inégalité souhaitée :

$$\left|\frac{a}{b} - q\right|^2 = (x - \lfloor x + 1/2 \rfloor)^2 + 2(y - \lfloor y + 1/2 \rfloor)^2 \leq \left(\frac{1}{2}\right)^2 + 2\left(\frac{1}{2}\right)^2 = \frac{3}{4} < 1.$$

En posant alors $r = a - bq \in \mathbb{Z}[i\sqrt{2}]$, on a alors $a = bq + r$ et $|r|^2 < |b|^2$. Donc $\mathbb{Z}[i\sqrt{2}]$ est bien un anneau euclidien pour le stathm $|\cdot|^2$.

Propriété 2

$\mathbb{Z}[i\sqrt{2}]^\times = \{1, -1\}$.

Preuve :

Soit $z = a + i\sqrt{2}b \in \mathbb{Z}[i\sqrt{2}]^\times$. Alors $1 = |z \cdot z^{-1}|^2 = |z|^2 \cdot |z^{-1}|^2$. Comme $|z|^2$ et $|z^{-1}|^2$ sont des entiers naturels, on a $|z|^2 = 1 = a^2 + 2b^2$, d'où $z = \pm 1$. Réciproquement, 1 et -1 sont bien inversibles.

Lemme 3

$i\sqrt{2}$ est irréductible.

Preuve :

Si $i\sqrt{2} = z \cdot w$, alors $|z|^2 \cdot |w|^2 = 2$. Comme 2 est premier, on a $|z|^2 = 1$ ou $|w|^2 = 1$, ce qui signifie d'après la preuve de la propriété précédente, que z ou w est inversible.

Théorème 4

L'équation diophantienne $x^2 + 2 = y^3$ admet comme solutions entières $(\pm 5, 3)$.

Preuve :

Soit $(x, y) \in \mathbb{Z}^2$ une solution de l'équation. Plaçons-nous dans l'anneau $\mathbb{Z}[i\sqrt{2}]$. On a alors $x^2 + 2 = (x + i\sqrt{2})(x - i\sqrt{2}) = y^3$. Nous allons d'abord montrer que $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux. Soit δ un pgcd (qui existe puisque l'anneau est euclidien). On a :

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

On en déduit que δ est de la forme $\pm(i\sqrt{2})^k$ avec $k \in \{0, 1, 2, 3\}$, puisque $i\sqrt{2}$ est un irréductible et que $\mathbb{Z}[i\sqrt{2}]$ est factoriel.

Supposons que $\delta \neq \pm 1$ (c'est-à-dire $k \neq 0$). Alors $i\sqrt{2} | \delta$ et donc $(i\sqrt{2})^2$ divise $(x + i\sqrt{2})(x - i\sqrt{2}) = y^3$. Il existe donc $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $y^3 = -2q$, ce qui conduit à avoir $q \in \mathbb{Z}$ et donc d'avoir la divisibilité de y^3 par 2 dans $\mathbb{Z}$ et finalement d'avoir $2|y$. En réduisant l'équation modulo 4, il vient alors la contradiction (regarder les carrés mod. 4) :

$$x^2 + 2 \equiv 0[4].$$

On en déduit donc que $\delta = \pm 1$, et donc $x + i\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux. Leur produit étant un cube, on en déduit que ce sont eux aussi des cubes (par factorialité) : il existe $a,\ b \in \mathbb{Z}$ tels que

$$x + i\sqrt{2} = (a + i\sqrt{2}b)^3 = a^3 - 6ab^2 + i\sqrt{2}(3a^2b - 2b^3).$$

Cela amène à avoir le système :

$$\begin{cases} x = a^3 - 6ab^2 \\ 1 = 3a^2b - 2b^3 \end{cases}.$$

La seconde ligne amène à avoir $b = 1$ (par divisibilité dans $\mathbb{Z}$ et le fait que $3a^2b - 2b^3$ doit être positif) puis à $a = \pm 1$. En insérant dans la première ligne et en utilisant l'équation diophantienne vérifiée par notre couple (x, y), on obtient $x = \pm 5$ et $y = 3$.

Réciproquement, on vérifie facilement que ce sont des solutions.

Théorème 5

26 est l'unique entier entre un carré et un cube.

Preuve :

Soit $n \in \mathbb{N}$ tel que $n-1 = x^2$ et $n+1 = y^3$. Alors $x^2+2 = y^3$, et d'après ce qui précède $n = x^2+1 = 25+1 = 26$.



II - Une variante pour les plus à l'aise

Voici une variante du développement afin de démontrer que x+i$\sqrt{2}$ et $x - i\sqrt{2}$ sont premiers entre eux. Cette variante nécéssite une connaissance de la forme normale de Smith, ce qui peut être assez dur pour certains candidats, mais elle a le mérite d'éviter la démonstration des inversibles de $\mathbb{Z}[i\sqrt{2}]$ et de l'irréductibilité de $i\sqrt{2}$. L'idée est de chercher une relation de Bézout entre $x + i\sqrt{2}$ et $x - i\sqrt{2}$. Cela revient à chercher $a, b, c, d \in \mathbb{Z}$ tels que :

$$(a + ib\sqrt{2})(x + i\sqrt{2}) + (c + id\sqrt{2})(x - i\sqrt{2}) = 1.$$

i.e.

$$\begin{cases} ax - 2b + cx + 2d = 1 \\ bx + a - c + dx = 0 \end{cases}$$

i.e.

$$\begin{pmatrix} x & -2 & x & 2 \\ 1 & x & -1 & x \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Essayons ainsi de trouver la forme de Smith de $\begin{pmatrix} x & -2 & x & 2 \\ 1 & x & -1 & x \end{pmatrix} \in M_{2,4}(\mathbb{Z})$.

On effectue les opérations élémentaires suivantes :

$$\begin{pmatrix} x & -2 & x & 2 \\ 1 & x & -1 & x \end{pmatrix} \xrightarrow{L_1 \leftrightarrow L_2} \begin{pmatrix} 1 & x & -1 & x \\ x & -2 & x & 2 \end{pmatrix} \xrightarrow[C_3 \leftarrow C_3 + C_1]{C_2 \leftarrow C_2 - xC_1 \\ C_4 \leftarrow C_4 - xC_1}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ x & -2-x^2 & 2x & 2-x^2 \end{pmatrix} \xrightarrow{L_2 \leftarrow L_2 - xL_1} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2-x^2 & 2x & 2-x^2 \end{pmatrix} \xrightarrow{C_4 \leftarrow C_4 - C_2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & -2-x^2 & 2x & 4 \end{pmatrix}.$$

Remarquons que $2 \nmid x$. En effet, si c'était le cas, alors $2 \mid y$ et modulo 4, l'équation donne :

$$2 + 0 \equiv 0\ [4],$$

ce qui n'est pas possible. Ainsi, $\text{pgcd}(-2-x^2, 4) = 1$ (car $-2-x^2$ est impair). En faisant un algorithme d'Euclide, on obtient au final la matrice :

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix},$$

qui est la forme normale de Smith recherchée. En particulier, on en déduit que la matrice initiale est surjective, d'où l'existence d'un 4-uplet tel que

$$\begin{pmatrix} x & -2 & x & 2 \\ 1 & x & -1 & x \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

III - Remarques

1 - Je ne conseillerai la variante que pour la leçon 122, et que si vous maitrisez la forme de Smith (et si vous la faite aussi en développement, c'est encore mieux !). Le problème de ce développement pour la leçon 122, est qu'on n'utilise pas vraiment de propriétés d'anneaux principaux, juste des propriétés d'anneaux factoriels (c'est le même problème que pour le développement sur les premiers somme de deux carrés). Ainsi, certains jurys pourraient y voir un inconvénient (pas de panique cependant pour les autres, je pense que dans les faits, un jury n'y accordera pas beaucoup d'importance et sera satisfait de la première version pour la 122).

2 - Pour montrer que $\mathbb{Z}[i\sqrt{2}]$ est euclidien, n'hésitez pas à ne pas faire les calculs, et de juste faire un dessin pour convaincre le jury.

3 - Il faut savoir résoudre de la même manière d'autres équations diophantienne. Un exemple plus dur de la même trempe se trouve dans le [Cal-Per]. Le [131] fourni aussi quelques conseils sur ce développement et donne d'autres équations à résoudre. Il peut être utilise de connaître l'équation de Pell-Fermat, et ses solutions (pas forcément de savoir la résoudre par contre, c'est difficile).

IV - Références

[Cal-Per] : *Carnet de voyage en Algébrie*, Phillipe Caldero, Marie Peronnier
[131] : *131 développements pour l'oral*, Didier Lesesvre, Pierre Montagnon