Equation de Mordell pour $k = 2$ et anneau $\mathbb{Z}[i\sqrt{2}]$

Dorian Cacitti-Holland

2020-2021

Références.

1. Théorie des nombres de Daniel Duverney

Leçons.

1. 122 Anneaux principaux, applications
2. 126 Exemples d'équations en arithmétique

Théorême. L'anneau $\mathbb{Z}[i\sqrt{2}]$ est euclidien, donc principal, donc factoriel.

Démonstration.
L'anneau $\mathbb{Z}[i\sqrt{2}]$ est unitaire commutatif et intègre par intégrité de $\mathbb{C}$.
Puis on considère, pour $z \in \mathbb{Z}[i\sqrt{2}]$, $N(z) := z\overline{z}$ ie si $z = a + bi\sqrt{2}$ alors

$$N(z) = a^2 + 2b^2$$

Soit $z \in \mathbb{Z}[i\sqrt{2}]$ et $w \in \mathbb{Z}[i\sqrt{2}]\backslash\{0\}$, alors il existe $x, y \in \mathbb{R}$ (uniques) tels que

$$\frac{z}{w} = x + iy\sqrt{2}$$

On considère $q = c + id\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ avec c et d les entiers les plus proches de x et y ie

$$|x - c| \leq \frac{1}{2}, |y - d| \leq \frac{1}{2}$$

D'où

$$\left|\frac{z}{w} - q\right|^2 = \left|x - c + i\sqrt{2}(y - d)\right|^2 = |x - c|^2 + 2|y - d|^2 \leq \frac{1}{4} + \frac{2}{4} = \frac{3}{4} < 1$$

On considère de plus $r = z - qw \in \mathbb{Z}[i]$, ainsi

$$N(r) = N(w)\left|\frac{z}{w} - q\right| < N(w) \times 1$$

D'où $z = qw + r$ est une division euclidienne de z par w, ce qui montre que $\mathbb{Z}[i\sqrt{2}]$ est euclidien. $\square$

Théorême. L'équation de Mordell (pour $k = 2$)

$$y^2 = x^3 - 2$$

d'inconnue $(x, y) \in \mathbb{Z}^2$ a pour uniques solutions $(3, 5)$ et $(3, -5)$.

Démonstration.
Soit $(x, y) \in \mathbb{Z}^2$ tel que

$$y^2 = x^3 - 2$$

Etape 1 : x est impair
On suppose par l'absurde que x est pair, alors

$$y^2 \equiv -2[8] \equiv 6[8]$$

ce qui n'est pas pas possible car, dans $\mathbb{Z}/8\mathbb{Z}$,

$$0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 1, 4^2 = 0, 5^2 = 1, 6^2 = 4, 7^2 = 1$$

D'où x est impair.
Etape 2 : Se ramner à l'anneau $\mathbb{Z}[i\sqrt{2}]$
On a

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

Etape 3 : $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux dans $\mathbb{Z}[i\sqrt{2}]$
Soit $p \in \mathbb{Z}[i\sqrt{2}]$ un diviseur commun à $y + i\sqrt{2}$ et $y - i\sqrt{2}$.
Donc

$$p \mid y + i\sqrt{2} - (y - i\sqrt{2}) = 2i\sqrt{2}$$

Ainsi, dans $\mathbb{N}$ (car $d = -2 < 0$),

$$N(p) \mid N(2i\sqrt{2}) = 8$$

De plus, dans $\mathbb{N}$,

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

avec x^3 impair d'après ce qui précède, donc $N(p)$ impair.
D'où $N(p) = 1$ puis, en écrivant $p = a + bi\sqrt{2}$ et $N(p) = a^2 + 2b^2$, on en déduit $p \in \mathbb{Z}[i\sqrt{2}]^\times$.
Ainsi $y + i\sqrt{2}$ et $y - i\sqrt{2}$ sont premiers entre eux.
Etape 4 : Utilisation de la factorialité de $\mathbb{Z}[i\sqrt{2}]$
Comme $\mathbb{Z}[i\sqrt{2}]$ est euclidien, $\mathbb{Z}[i\sqrt{2}]$ est principal donc factoriel.
Ainsi, de $x^3 = (y + i\sqrt{2})(y - i\sqrt{2})$, on en déduit qu'il existe $(u, v) \in (\mathbb{Z}[i\sqrt{2}]^\times)^2$ et $(\alpha, \beta) \in (\mathbb{Z}[i\sqrt{2}])^2$ tel que

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

Or on a $N(u) = N(v) = 1$, puis, en décomposant u et v en $a + bi\sqrt{2}$, on en déduit

$$u = \pm 1, v = \pm 1$$

Ainsi on peut écrire

$$y + i\sqrt{2} = (m + ni\sqrt{2})^3$$

avec $(m,n) \in \mathbb{Z}^2$.
D'où
$$y + i\sqrt{2} = m^3 - 6mn^2 + i\sqrt{2}(3m^2n - 2n^3)$$
Puis par unicité des parties réelle et imaginaire dans $\mathbb{C}$,
$$y = m^3 - 6mn^2 = m(m^2 - 6n^2), 1 = 3m^2n - 2n^3 = (3m^2 - 2n^2)n$$
Ainsi, de la deuxième équation, on en déduit $n = \pm 1$, puis distinguons les cas :

— Si $n = 1$ alors $1 = 3m^2 - 2$, d'où $m = \pm 1$, puis
$$y = \pm 5$$
— Si $n = -1$ alors $1 = -(3m^2 - 2)$, d'où $1 = 3m^2$ ce qui n'est pas possible dans $\mathbb{Z}$ car 3 ne divise pas 1 et $m^2 \in \mathbb{Z}$.

Par conséquent $y = \pm 5$ puis $x^3 = y^2 + 2 = 27$, d'où
$$x = 3$$
Etape 5 : Vérification

Réciproquement $(3,5)$ et $(3,-5)$ vérifient $x^3 = y^2 + 2$. $\square$