Notation / propriétés:

- $N(z) = |z|^2$

Equation de Mordell

Leçons: 122, 126.

Réf:
- Théorie des nombres, D. Duverney

Proposition

Soit $z \in \mathbb{Z}[i\sqrt{2}]$. Alors $z \in \mathbb{Z}[i\sqrt{2}]^\times$ si et seulement si $N(z) = 1$

Corollaire

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

Théorème

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

Preuve:

Soient $z \in \mathbb{Z}[i\sqrt{2}]$ et $\omega \in \mathbb{Z}[i\sqrt{2}] \setminus \{0\}$. Alors il existe x, y dans $\mathbb{Q}$ uniques tels que

$$\frac{z}{\omega} = x + yi\sqrt{2}$$

Soient α et β les entiers les plus proches de x et y, c-à-d tels que

$$|x - \alpha| \leq \frac{1}{2} \quad \text{et} \quad |y - \beta| \leq \frac{1}{2}$$

Notons q l'élément $\alpha + i\beta\sqrt{2}$ et r l'élément $z - \omega q$.

On a alors

$$\left|\frac{z}{\omega} - q\right|^2 = \left|x - \alpha + i\sqrt{2}(y - \beta)\right|^2 = (x-\alpha)^2 + 2(y-\beta)^2$$

$$\leq \frac{1}{4} + 2 \times \frac{1}{4} = \frac{3}{4} < 1$$

c-à-d $N(r) = N(\omega) N\left(\frac{z}{\omega} - q\right) < N(\omega)$.

Ainsi on a la décomposition

$$z = \omega q + r$$

avec $N(r) < N(\omega)$. De plus, (q, r) est bien unique.

Cela conclut ∎

Théorème

L'équation de Mordell

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

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

Preuve :

Il est clair que $(3,5)$ et $(3,-5)$ sont solutions de l'équation.

Soit $(x,y) \in \mathbb{Z}^2$ tel que $y^2 = x^3 - 2$.

Etape 1 : x est impair

Si x est pair alors on obtient

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

Comme les carrés de $\frac{\mathbb{Z}}{8\mathbb{Z}}$ sont 0, 1 et 4 d'après les calculs

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

Contradiction ↯ Nécessairement x est impair.

Etape 2 : l'équation se réécrit

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

Montrons que $(y-i\sqrt{2})$ 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 $y-i\sqrt{2}$.

Alors p divise leur différence $2i\sqrt{2}$ et donc $N(p)$ divise 8

Par ailleurs $N(p)$ est impair car il divise $y^2+2 = x^3$ impair

D'où $N(p) = 1$ et donc $p \in \mathbb{Z}[i\sqrt{2}]^\times$

Cela donne la primalité.

Etape 3 : décomposition dans $\mathbb{Z}[i\sqrt{2}]$ factoriel.

Par unicité de la décomposition, il existe α, β dans $\mathbb{Z}$ tels

que $y+i\sqrt{2} = (\alpha+i\beta\sqrt{2})^3$. En développant, on obtient

$$y+i\sqrt{2} = \alpha^3 - 6\alpha\beta^2 + i\sqrt{2}(\beta\alpha^2 - 2\beta^3)$$

et puis $y = \alpha(\alpha^2 - 6\beta^2)$ et $1 = \beta(3\alpha^2 - 2\beta^2)$

On en déduit que β divise 1 et que $3\alpha^2 - 2 = 1$ c-à-d $\alpha^2 = 1$.

Si $\alpha = 1$ alors $y = 1 - 6 = -5$ et donc $x = 3$.

Sinon $\alpha = -1$ et alors $y = -(1-6) = 5$.

Cela conclut ■

Rmq: on a le résultat plus général (et plus poussé) suivant:

Théorème

Soit k un entier strictement inférieur à -1, sans facteur carré tel que $k \equiv 2 \bmod 4$ ou $k \equiv 3 \bmod 4$.

Supposons que le nombre des classes $h(\mathbb{Q}(\sqrt{k}))$ ne soit pas divisible par 3.

Alors l'équation

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

d'inconnue (x, y) dans $\mathbb{Z}^2$, admet des solutions si et seulement s'il existe $a \in \mathbb{N}^*$ tel que $k = \pm 1 - 3a^2$.

Dans ce cas, les solutions sont

$$(a^2 - k, a(a^2 - 3k)) \text{ et } (a^2 - k, -a(a^2 - 3k))$$

Preuve:

($\Leftarrow$): Supposons qu'il existe $a \in \mathbb{N}^*$ tel que $k = \pm 1 - 3a^2$.

On vérifie par les calculs que $(a^2 - k, a(a^2 - 3k))$ et $(a^2 - k, -a(a^2 - 3k))$ sont solutions de l'équation.

($\Rightarrow$): Supposons qu'il existe $(x, y) \in \mathbb{Z}^2$ tel que $x^3 + k = y^2$.

Etape 1: x et y sont premiers entre eux.

En effet, supposons que cela ne soit pas le cas. Soit p un nombre

premier divisant x et y. Alors p^2 divise $y^2 - x^3$, c-à-d p^2 divise k
Cela contredit l'hypothèse faite sur k et ses facteurs carrés.

Etape 2 : x est impair.

Si ce n'est pas le cas alors 4 divise x^3 et on obtient

$$y^2 \equiv k \bmod 4 \quad (\equiv 2 \text{ ou } 3 \bmod 4)$$

Or les carrés modulo 4 sont 0 et 1. Donc nécessairement x est impair.

Etape 3 : arithmétique des idéaux dans $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$.

On se donne une racine de k, que l'on note $\sqrt{k}$.
Alors, dans $\mathbb{Q}(\sqrt{k})$ on a la factorisation suivante

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

et donc $\langle x \rangle^3 = \langle y - \sqrt{k} \rangle \langle y + \sqrt{k} \rangle$ dans $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$.

Soit $\mathcal{P}$ un idéal premier de $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$ divisant $\langle y + \sqrt{k} \rangle$ et $\langle y - \sqrt{k} \rangle$, c-à-d tel que

$$\langle y - \sqrt{k} \rangle \subseteq \mathcal{P} \quad \text{et} \quad \langle y + \sqrt{k} \rangle \subseteq \mathcal{P}$$

Alors $y + \sqrt{k}$ et $y - \sqrt{k}$ sont des éléments de $\mathcal{P}$, donc

$$2y = y - \sqrt{k} + y + \sqrt{k}$$

est aussi dans $\mathcal{P}$, soit on a

$$\langle 2y \rangle \subseteq \mathcal{P}$$

De plus, on obtient aussi que $\langle x \rangle$ est inclus dans $\mathcal{P}$.
En considérant la norme N sur les idéaux de $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$ on obtient

$$N(\mathcal{P}) \mid 4y^2 \quad \text{et} \quad N(\mathcal{P}) \mid x^2$$

Comme x est impair, $N(\mathcal{P})$ est aussi impair donc divise y^2.
Comme $\mathcal{P}$ est un idéal premier, $N(\mathcal{P})$ est premier. On en déduit que x et y ont un facteur premier commun.
Nécessairement, les idéaux $\langle y - \sqrt{k} \rangle$ et $\langle y + \sqrt{k} \rangle$ sont premiers entre eux

Par unicité de la décomposition en produit d'idéaux premiers on obtient qu'il existe un idéal I de $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$ tel que

$$I^3 = \langle y + \sqrt{k} \rangle$$

On utilise alors le lemme suivant:

Lemme

Soit I un idéal de $\mathcal{O}_{\mathbb{Q}(\sqrt{k})}$ et p un nombre entier premier tel que I^p soit principal.

Si p ne divise pas $h(\mathbb{Q}(\sqrt{k}))$ alors I est principal.

Preuve du lemme:

Dire que I^p est principal revient à dire que l'ordre de la classe de I dans le groupe des classes divise p.

Comme p est premier, cet ordre est alors soit 1 soit p.

Le groupe des classes étant fini, le théorème de Lagrange assure que l'ordre de la classe de I est égal à 1 car p ne peut pas diviser $h(\mathbb{Q}(\sqrt{k}))$.

Donc I est principal. ■

Par le lemme, on obtient que I est principal.

Comme k est sans facteur carré et n'est pas congru à 1 modulo 4 on a $\mathcal{O}_{\mathbb{Q}(\sqrt{k})} = \mathbb{Z}[\sqrt{k}]$.

Il s'en suit qu'il existe a, b dans $\mathbb{Z}$ tels que

$$I = \langle a + b\sqrt{k} \rangle$$

et donc tel que $\langle y + \sqrt{k} \rangle = \langle (a + b\sqrt{k})^3 \rangle$. Ainsi il existe $\varepsilon \in \mathbb{Z}[\sqrt{k}]^\times$ tel que $y + \sqrt{k} = \varepsilon (a + b\sqrt{k})^3$.

Or comme $k < -1$ les unités de $\mathbb{Z}[\sqrt{k}]$ sont seulement 1 et -1. Donc on obtient

$$y + \sqrt{k} = -(a + b\sqrt{k})^3 \quad \text{ou} \quad y + \sqrt{k} = (a + b\sqrt{k})^3$$

et ensuite les systèmes

$$\begin{cases} y = -a(a^2+3kb^2) \\ 1 = -b(3a^2+b^2k) \end{cases} \quad \text{ou} \quad \begin{cases} y = a(a^2+3kb^2) \\ 1 = b(3a^2+b^2k) \end{cases}$$

On obtient ensuite $b \in \{-1,1\}$ et $k \in \{1-3a^2, -1-3a^2\}$. des dernières lignes.

Il s'en suit $y \in \{ a(a^2+3k), -a(a^2+3k) \}$

Enfin on en déduit

$$x^3 = y^2 - k = a^2(a^2+3k)^2 - k$$
$$= a^6 + 6a^4k + 9k^2a^2 - k$$

Comme $(k+3a^2)^2 = 1$, on obtient

$$k = k(k+3a^2)^2 = k^3 + 6k^2a^2 + 9a^4k$$

et donc

$$x^3 = a^6 - 3a^4k + 3k^2a^2 - k^3 = (a^2-k)^3.$$

Cela conclut ■

Dans le cas précédent on a $k=-2$. On vérifie bien

$$k \equiv 2 \mod 4$$

et 3 ne divise pas $h(\mathbb{Q}(\sqrt{-2})) = 1$ ($\mathbb{Z}[\sqrt{-2}]$ est principal).
Comme $k = 1-3\times(1)^2$ on en déduit que les solutions de l'équation

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

sont $(3,-5)$ et $(3,5)$.

NB: le calcul de $h(\mathbb{Q}(\sqrt{k}))$ peut s'avérer compliqué en général.