Équation de Fermat pour n=3

Akita

ENS Rennes, 2013-2014

Référence : *Théorie des nombres*, Duverney

Développement pour les leçons :
- 122. Anneaux principaux. Exemples et applications.
- 126. Exemples d'équations diophantiennes.

Théorème :

L'équation $x^3 + y^3 + z^3 = 0$ ne possède pas de solution telle que $xyz \neq 0$.

preuve :

Nous aurons besoin du lemme suivant :

Lemme : $\forall x \in \mathbb{Z}[j],\ \exists \varepsilon \in \mathbb{Z}[j]^\times,\ \exists y \in \mathbb{Z}[i\sqrt{3}]\ :\ x = \varepsilon y$.

Supposons qu'il existe $x, y, z \in \mathbb{Z}$ tels que $x^3 + y^3 + z^3 = 0$ et $xyz \neq 0$. Commençons par remarquer que si p premier divise deux des trois entiers x, y et z alors $\left(\frac{x}{p}, \frac{y}{p}, \frac{z}{p}\right)$ est solution. Donc nous pouvons supposer que x, y et z sont deux à deux premiers entre eux. Puis notons que sur les trois variables il y en a exactement une qui doit être paire. Quitte à échanger les variables, nous supposerons que y est pair et que x et z sont impairs. Choisissons une telle solution avec $|y|$ minimum.

Posons maintenant $a := \frac{x+z}{2}$ et $b := \frac{x-z}{2}$. D'où $x = a+b$ et $z = a-b$, donc l'équation devient $2a(a^2 + 3b^2) = -y^3$. Comme x et z sont premiers entre eux, a et b le sont également. De l'équation vérifiée par a, b et y, nous en déduisons que a est pair. Et ainsi b est impair.

Puisque a et b sont de parités différentes, a^2+3b^2 est impair. Aussi tout diviseur commun à $2a$ et a^2+3b^2 est impair, donc divise a puis $3b^2$. Il en résulte alors : pgcd($2a$,a^2+3b^2)=1 ou 3.

Premier cas : pgcd($2a$,a^2+3b^2)=1.

Alors, en regardant la factorisation en nombres premiers, $\exists r, s \in \mathbb{Z}$ tels que $2a = r^3$ et $a^2+3b^2=s^3$. Maintenant, nous allons travailler dans l'anneau euclidien (et donc principal !) $\mathbb{Z}[j]$, où $j = \mathrm{e}^{i\frac{2\pi}{3}} = -\frac{1}{2} + \frac{i\sqrt{3}}{2}$. Notons que $i\sqrt{3} = 2j+1$. Factorisons dans $\mathbb{Z}[j]$: $(a+ib\sqrt{3})(a-ib\sqrt{3}) = s^3$.

Or si p premier dans $\mathbb{Z}[j]$ divise $a+ib\sqrt{3}$ et $a-ib\sqrt{3}$ alors il divise $2a$ puis $N(p) \mid 4a^2$ dans $\mathbb{Z}$; sauf que $N(p)$ divise a^2+3b^2 impair donc $N(p) \mid a^2$ et $N(p) \mid a^2+3b^2$, ce qui est absurde car a et a^2+3b^2 sont premiers entre eux.

Donc $a+ib\sqrt{3}$ et $a-ib\sqrt{3}$ sont premiers entre eux dans $\mathbb{Z}[j]$ et il existe $\eta \in \mathbb{Z}[j]^\times$ et $t \in \mathbb{Z}[j]$ tels que $a+ib\sqrt{3} = \eta t^3$. Comme -1=$(-1)^3$, nous pouvons supposer que $\eta \in \left\{1, \frac{1}{2}(1+i\sqrt{3}), \frac{1}{2}(1-i\sqrt{3})\right\}$.

D'après le lemme, il existe $\varepsilon \in \mathbb{Z}[j]^\times$ tel que $\varepsilon t \in \mathbb{Z}[i\sqrt{3}]$. Comme $\varepsilon^6 = 1$, alors $\varepsilon^{-3} = \pm 1$. Alors $a+ib\sqrt{3} = \eta\varepsilon^{-3}(\varepsilon t)^3 = \eta(\pm\varepsilon t)^3 = \eta(u+iv\sqrt{3})^3$, avec $u, v \in \mathbb{Z}$. En développant, il vient :

$$a+ib\sqrt{3} = \eta[u(u+3v)(u-3v) + 3v(u-v)(u+v)i\sqrt{3}].$$

Si $\eta = j+1$ alors en développant l'expression précédente et en identifiant les termes nous obtenons :

$$\begin{cases} a &= \frac{1}{2}[u(u+3v)(u-3v) - 9v(u-v)(u+v)] \\ b &= \frac{1}{2}[3v(u-v)(u+v) + u(u+3v)(u-3v)] \end{cases}.$$

D'où : $b-a = 6v(u-v)(u+v)$, ce qui est absurde car a est pair et b impair. Nous obtenons de même une contradiction si $\eta = j$. Ainsi $\eta = 1$ et nous avons $a = u(u+3v)(u-3v)$ et $b = 3v(u-v)(u+v)$. Mais a est pair, b est impair et a et b sont premiers entre eux donc u est pair, v est impair et $2u$ et $3v$ sont premiers entre eux. Nous en déduisons que $2u, u+3v$ et $u-3v$ sont deux à deux premiers entre eux. Or $2a = r^3$, donc il existe $l, m, n \in \mathbb{Z}$ tels que $2u = l^3$, $u+3v = m^3$ et $u-3v = n^3$. D'où : $m^3+n^3+(-l)^3 = 0$ avec l pair. Enfin remarquons que :

$$|y^3| = |2a(a^2+3b^2)| = |l^3(u^2-9v^2)(a^2+3b^2)| \geq 3|l^3| > |l^3|.$$

Donc $0 < |l| < |y|$, ce qui est absurde.

Second cas : pgcd$(2a, a^2+3b^2)$=3.

Posons $a = 3c$. L'équation devient : $18c(3c^2+b^2) = -y^3$. Si $p \in \mathbb{Z}$ premier divise $18c$ et $3c^2+b$ alors, comme le deuxième terme est impair, p divise $9c$. Si $p = 3$ alors p divise b et a, ce qui est absurde. De même si p divise c. Donc $18c$ et $3c^2+b$ sont premiers entre eux. Ainsi il existe $r, s \in \mathbb{Z}$ tels que $18c = r^3$ et $3c^2+b = s^3$. Avec le même raisonnement que pour le premier cas, nous obtenons $b = u(u+3v)(u-3v)$ et $c = 3v(u-v)(u+v)$ avec u impair, v pair et u et v premiers entre eux. Remarquons que r est divisible par 3 donc il existe $r' \in \mathbb{Z}$ tel que $r = 3r'$. Alors $r'^3 = 2v(u-v)(u+v)$. Comme ces trois facteurs sont deux à deux premiers entre eux il existe $l, m, n \in \mathbb{Z}$ tels que $l^3 = 2v$, $m^3 = u-v$ et $n^3 = u+v$. Ainsi nous obtenons : $l^3+m^3+(-n)^3$ et

$$|y^3| = |18c(3c^2+b^2)| = |27l^3(u^2-v^2)(3c^2+b^2)| \geq 27|l^3| > |l^3| \ : \text{ contradiction!}$$

Et le théorème est ainsi démontré.

Preuve du lemme :

Soit $x \in \mathbb{Z}[j]$. Il existe $a, b \in \mathbb{Z}$ tels que $x = a+bj = \dfrac{2a-b+ib\sqrt{3}}{2}$. Écrivons $u := 2a-b$ et $v := b$. Remarquons que u et v sont de même parité. S'ils sont tous les deux pairs alors le résultat voulu est vrai. Maintenant s'ils sont tous les deux pairs :

premier cas : $u \equiv 1$ (mod 4) et $v \equiv -1$ (mod 4) :

$$\frac{u+iv\sqrt{3}}{2}(1+j) = \frac{1}{4}[(u-3v)+i\sqrt{3}(u+v)] \in \mathbb{Z}[i\sqrt{3}],$$

deuxième cas : $u \equiv -1$ (mod 4) et $v \equiv 1$ (mod 4) :

$\dfrac{u+iv\sqrt{3}}{2}(-1-j) = \dfrac{-u-iv\sqrt{3}}{2}(1+j)$ et nous sommes ramenés au premier cas,

troisième cas : $u \equiv -1$ (mod 4) et $v \equiv -1$ (mod 4) :

$\dfrac{u+iv\sqrt{3}}{2}j$ est le conjugué de $\dfrac{u-iv\sqrt{3}}{2}(-1-j) \in \mathbb{Z}[i\sqrt{3}]$,

quatrième cas : $u \equiv 1$ (mod 4) et $v \equiv 1$ (mod 4) :

$\frac{u+iv\sqrt{3}}{2} \times (-j) = \frac{-u-iv\sqrt{3}}{2} j$ et nous sommes ramenés au troisième cas.

Le lemme est prouvé.

Remarques :
- en fait nous avons montré un peu plus : l'équation de Fermat n'admet pas de solutions non triviales pour n égal à un multiple de 3,
- développement un peu long ; on peut faire le premier cas et dire que le deuxième cas est similaire.