Résolution de l'équation $x^3+y^3=2z^3$ dans $\mathbb{Z}^3$

(précédée d'un lemme)

http://alain.pichereau.pages.perso-orange.fr
marc.pichereau@wanadoo.fr

Enoncé

Lemme

Si u et v sont deux entiers relatifs premiers entre eux, de parités différentes, et tels que u^2+3v^2 soit le cube d'un entier relatif,
alors il existe deux autres entiers relatifs n et m premiers entre eux tels que
$u+iv\sqrt{3}=(n+im\sqrt{3})^3$.
Evidemment $u+iv\sqrt{3}=(n+im\sqrt{3})^3 \Leftrightarrow u=n(n^2-9m^2)$ et $v=3m(n^2-m^2)$.
Et $u+iv\sqrt{3}=(n+im\sqrt{3})^3 \Rightarrow u^2+3v^2=(n^2+3m^2)^3$ (on prend le carré du module des deux membres).

Remarque 1

En fait les hypothèses du lemme permettent aussi de conclure à l'existence de deux entiers relatifs a et b tels que
$2u=(2a+b)(a-b)(a+2b), 2v=3ab(a+b)$ et $u^2+3v^2=(a^2+ab+b^2)^3$.
Cet aspect ne sera pas utilisé ici.

Remarque 2

Pour tout (α,β) dans $\mathbb{Z}^2$, il existe (u,v) dans $\mathbb{Z}^2$ tels que $\alpha^2+\alpha+3\beta^2+3\beta+1=u^2+3v^2$:
si $\alpha-\beta$ est pair, $u=\pm(2\beta+1+\frac{\alpha-\beta}{2})$ et $v=\pm\frac{\alpha-\beta}{2}$ conviennent,
si $\alpha-\beta$ est impair, $u=\pm(2\beta+1-\frac{\alpha+\beta+1}{2})$ et $v=\pm\frac{\alpha+\beta+1}{2}$ conviennent.
Vérification laissée au lecteur qui pourra regarder le problème du concours général 2001.

preuve : on va travailler dans l'anneau $E=\{\frac{a}{2}+\frac{b}{2}i\sqrt{3}\,;a,b$ dans $\mathbb{Z}$ et de même parité$\}$: c'est l'anneau d'Eisenstein.
Bien entendu cet anneau E contient le sous-anneau $A=\{a+bi\sqrt{3}\,;a,b$ dans $\mathbb{Z}\}$, mais il contient aussi $j=\frac{-1+i\sqrt{3}}{2}$ et $j^2=\frac{-1-i\sqrt{3}}{2}$ qui ne sont pas dans A.
En fait $E=\{a+bj\,;\ a,b$ dans $\mathbb{Z}\}$ puisque pour tout a et b dans $\mathbb{Z}, a+bj=\frac{2a-b}{2}+\frac{b}{2}i\sqrt{3}\in E$ car $2a-b$ et b ont même parité et réciproquement si $\frac{a}{2}+\frac{b}{2}i\sqrt{3}\in E,\ \frac{a}{2}+\frac{b}{2}i\sqrt{3}=\frac{a+b}{2}+bj$ où $\frac{a+b}{2}$ est effectivement entier.
De la même manière on prouve aussi que $E=\{a+b\frac{1+i\sqrt{3}}{2}\ ;\ a,b$ dans $\mathbb{Z}\}$

Note : actuellement, il semblerait que l'on note $E=\mathbb{Z}[j]$ ou $E=\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ et $A=\mathbb{Z}[i\sqrt{3}]$, mais dans le temps...., disons il y a 25 ans..., on notait $\mathbb{Z}[\sqrt{d}]$ (d dans $\mathbb{Z}$ sans facteur

carré) l'anneau des entiers du corps quadratique $\mathbb{Q}[\sqrt{d}] = \{\alpha + \beta\sqrt{d}\,;\ \alpha, \beta \text{ dans } \mathbb{Q}\}$ et donc, à ce titre E était noté $\mathbb{Z}[\sqrt{-3}] = Z[i\sqrt{3}]$, ce que fait d'ailleurs Hellegouarch en 1997 (voir référence 1).

La plupart des résultats sur cet anneau E utilisés ici seront cités sans démonstration.

Un outil très utile pour travailler dans cet anneau est la norme : si $\frac{a}{2} + \frac{b}{2}i\sqrt{3}$ est un élément de E on pose $N(\frac{a}{2} + \frac{b}{2}i\sqrt{3}) = |\frac{a}{2} + \frac{b}{2}i\sqrt{3}|^2 = \frac{a^2}{4} + \frac{3b^2}{4} \in \mathbb{N}$.

On a, pour deux éléments quelconques z, z' de E, $N(zz') = N(z)N(z')$ et donc si d divise (dans E) z, alors $N(d)$ divise (dans $\mathbb{N}$) $N(z)$.

Cet anneau admet six inversibles (ou unités) : $\pm 1, \pm j, \pm j^2$; ceci vient du fait qu'un élément $z = \frac{a}{2} + \frac{b}{2}i\sqrt{3}$ de E est inversible est équivalent à $N(z) = 1$, soit $a^2 + 3b^2 = 4$.

Enfin, c'est un anneau euclidien, donc principal, donc factoriel.

Par contre le sous-anneau A de E n'est pas factoriel (contrairement à ce que pensait Euler) :

en effet $2 \times 2 = (1 - i\sqrt{3})(1 + i\sqrt{3}))$, donc 2 divise $(1 - i\sqrt{3})(1 + i\sqrt{3})$ mais ne divise aucun des facteurs, donc 2 n'est pas premier, mais 2 est irréductible (utiliser la norme $a^2 + 3b^2$ et montrer que les seuls diviseurs de 2 sont $\pm 1, \pm 2$), et dans un anneau factoriel tout élément irréductible est forcément premier, donc A n'est pas factoriel .

Notons w l'entier dont le cube est $u^2 + 3v^2$.

Tout d'abord on remarque que (dans $\mathbb{Z}$) 3 ne divise pas u, sinon 3 divise $u^2 + 3v^2 = w^3$, donc 3 divise w et 9 divise $u^2 - w^3 = -3v^2$, donc 3 divise v^2, soit 3 divise v, et u et v ne sont pas premiers entre eux, ce qui est contraire à l'hypothèse.

On en déduit que u^2et $3v^2$ sont premiers entre eux, car sinon il existe un nombre premier p divisant u^2 et $3v^2$, mais p divisant u, p ne peut être 3 d'après ce qui précéde, donc p divise v^2, donc v et on arrive encore à u et v non premiers entre eux, ce qui est impossible par hypothèse.

Le passage dans E s'obtient tout naturellement puisque $u^2 + 3v^2 = w^3$ équivaut à $(u + iv\sqrt{3})(u - iv\sqrt{3}) = w^3$ qui est une égalité dans E.

Mais avant de conclure à $(u + iv\sqrt{3})$ est un cube dans E, grâce au fait que cet anneau est factoriel, il faut montrer que $u + iv\sqrt{3}$ et $u - iv\sqrt{3}$ sont premiers entre eux dans E (dans $\mathbb{N}$, 7×7^2 est un cube, mais pas 7).

Supposons qu'il existe $d \in E$ divisant $u + iv\sqrt{3}$ et $u - iv\sqrt{3}$: on va montrer que nécessairement d est une des six unités de E.

d divise la somme et la différence de ces deux nombres soit $2u$ et $2iv\sqrt{3}$ et donc $N(d)$ divise $N(2u), N(2iv\sqrt{3})$ et $N(u + iv\sqrt{3})$, c'est-à-dire $N(d)$ divise $4u^2, 12v^2$ et $u^2 + 3v^2$.

Donc $N(d)$ divise $p\gcd(4u^2, 12v^2) = 4p\gcd(u^2, 3v^2) = 4$ puisque on vient de voir que u^2et $3v^2$ sont premiers entre eux.

Ainsi $N(d) = 1$ ou 2 ou 4.

Mais $N(d) = 2$ ou 4, implique que $u^2 + 3v^2$ est pair (puisque c'est un multiple de $N(d)$), donc u et v sont de même parité, ce qui est contraire à l'hypothèse.

Donc $N(d) = 1$, c'est-à-dire d est un inversible de E et $u + iv\sqrt{3}$ et $u - iv\sqrt{3}$ sont premiers entre eux dans E : E étant factoriel, on peut alors dire que $u + iv\sqrt{3}$ est un cube dans E, cela aux unités près : $u + iv\sqrt{3} = \delta(\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3$ avec a et b dans $\mathbb{Z}$ et de même parité et δ une unité.

Montrons que $\delta = \pm j$ ou $\pm j^2$ est impossible.

Par exemple si $\delta = \pm j$, en rentrant le -1 dans le cube si $\delta = -j$, on a $j^2(u + iv\sqrt{3}) = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3$ avec a et b dans $\mathbb{Z}$ et de même parité, et l'égalité des parties imaginaires donne $-u - v = \frac{3b(a^2 - b^2)}{4}$.

Comparons la parité des deux membres :

$-u - v$ est impair, u, v étant de parités contraires (hypothèse)

a et b étant de même parité, il y a deux cas à envisager :

si $a = 2a'$ et $b = 2b'$, $\frac{3b(a^2 - b^2)}{4} = 6b'(a'^2 - a + 3b - b'^2)$ est pair, donc contradiction

si $a = 2a' + 1$ et $b = 2b' + 1$, $\frac{3b(a^2 - b^2)}{4} = 3(2b' + 1)(a'(a' + 1) - b'(b' + 1))$ est pair (pour tout entier relatif n, $n(n + 1)$ est pair), donc contradiction aussi.

Le cas $\delta = \pm j^2$ se traite de la même façon.

Donc, $\delta = \pm 1$, et quitte là encore à rentrer le -1 dans le cube on a $u + iv\sqrt{3} = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3$ avec a et b dans $\mathbb{Z}$ et de même parité.

Comme $j^3 = (j^2)^3 = 1$, on a en fait la triple égalité

$u + iv\sqrt{3} = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3 = ((\frac{-1 + i\sqrt{3}}{2})(\frac{a}{2} + \frac{b}{2}i\sqrt{3}))^3 = ((\frac{-1 - i\sqrt{3}}{2})(\frac{a}{2} + \frac{b}{2}i\sqrt{3}))^3$, soit

$u + iv\sqrt{3} = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3 = (-\frac{a + 3b}{4} + \frac{a - b}{4}i\sqrt{3})^3 = (\frac{-a + 3b}{4} - \frac{a + b}{4}i\sqrt{3})^3$

On est maintenant en mesure de montrer qu'il existe toujours deux entiers relatifs n et m tels que $u + iv\sqrt{3} = (n + mi\sqrt{3})^3$

soit a et b sont pairs et on prend $n = \frac{a}{2}$ et $m = \frac{b}{2}$ et la première égalité permet de conclure

soit a et b sont impairs, cad il existe deux entiers a' et b' tels que $a = 2a' + 1$ et $b = 2b' + 1$, donc $a' - b' = \frac{a - b}{2}$

si $a' - b'$ est pair, $\frac{a - b}{2}$ est pair mais aussi $\frac{a + 3b}{2} = \frac{a - b}{2} + 2b$ est pair donc on peut prendre $n = -\frac{a + 3b}{4}$, $m = \frac{a - b}{4}$ et la deuxième égalité permet de conclure

si $a' - b'$ est impair, $\frac{a + b}{2} = \frac{a - b}{2} + b$ est pair (somme de deux impairs) et $\frac{a - 3b}{2} = \frac{a - b}{2} - b$ est aussi pair, donc on peut prendre $n = \frac{-a + 3b}{4}$, $m = -\frac{a + b}{4}$ et la troisième égalité permet de conclure.

La relation $u + iv\sqrt{3} = (n + im\sqrt{3})^3$ étant équivalente à $u = n(n^2 - 9m^2)$ et $v = 3m(n^2 - m^2)$, n et m sont forcément premiers entre eux (sinon u et v ne le seraient pas).

preuve de la remarque 1 :

on exploite autrement le fait que $u + iv\sqrt{3} = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3$ avec a et b dans $\mathbb{Z}$ de même parité, cad $u + iv\sqrt{3}$ est un cube dans E.

En effet on a vu au début de cette démonstration que $E = \{a + b\frac{1 + i\sqrt{3}}{2}\ ;\ a, b \text{ dans } \mathbb{Z}\}$ et ainsi

$u + iv\sqrt{3} = (a + b\frac{1 + i\sqrt{3}}{2})^3 = (\frac{2a + b}{2} + \frac{b}{2}i\sqrt{3})^3$, avec a et b dans $\mathbb{Z}$ (en fait, cela revient à remplacer le a de $u + iv\sqrt{3} = (\frac{a}{2} + \frac{b}{2}i\sqrt{3})^3$ par $2a + b$, qui a bien même parité que b).

L'égalité des parties réelles et imaginaires donne $2u = (2a + b)(a - b)(a + 2b)$ et $2v = 3ab(a + b)$.

Et $u^2+3v^2 = N(u+iv\sqrt{3}) = N((\frac{2a+b}{2}+\frac{b}{2}i\sqrt{3})^3) = (N(\frac{2a+b}{2}+\frac{b}{2}i\sqrt{3}))^3$,
soit $u^2+3v^2 = ((\frac{2a+b}{2})^2+\frac{3b^2}{4})^3 = (a^2+ab+b^2)^3$ □.

Les seuls triplets $(x,y,z) \in \mathbb{Z}^3$ solutions de $x^3+y^3 = 2z^3$ sont les (x,x,x) et $(x,-x,0)$.

preuve :

Je m'inspire de l'exercice 1.7 du chapitre 1 de la référence 1 : c'est la méthode analogue à celle utilisée par Euler pour traiter le cas $x^3+y^3 = z^3$ (Fermat, cas $n = 3$).

On fait l'hypothèse qu'il existe au moins un triplet $(x,y,z) \in \mathbb{Z}^3$ qui soit solution avec $|x| \neq |y|$ (cela implique $z \neq 0$, car sinon $x = -y$) et on va montrer que cette existence aboutit à l'existence d'un autre triplet solution (x',y',z') avec $|x'| \neq |y'|$ et $|z'| < |z|$, ce qui va permettre de conclure (principe de la "descente").

Le cas où x et y ne sont pas premiers entre eux est immédiat, car alors il existe p premier les divisant, donc p^3 divise $2z^3$ et
soit $p = 2$ et 2^2 divise z^3 donc 2 divise z
soit $p \neq 2$ et p divise z^3, donc divise z
ainsi, p divise x,y,z et $(x',y',z') = (\frac{x}{p},\frac{y}{p},\frac{z}{p})$ est solution avec $|x'| \neq |y'|$ et $|z'| < |z|$.

On se place maintenant dans le cas où x et y sont premiers entre eux.

1) x et y sont impairs :

car $x^3+y^3 = 2z^3$ est pair donc x et y ont même parité, mais étant premiers entre eux ils sont impairs

2) il existe u et v dans Z tels que $x = u+v$ $y = u-v$ et
u,v premiers entre eux et de parités différentes et $uv \neq 0$.

en effet $x = 2k+1, y = 2k'+1$ et on prend $u = k+k'+1, v = k-k'$: u et v sont premiers entre eux sinon x et y ne le seraient pas et u et v sont de parité différente sinon x et y seraient pairs, donc non premiers entre eux.
$uv = 0$ est impossible car $u = 0$ ou $v = 0$ implique $|x| = |y|$.

3) $u(u^2+3v^2) = z^3$

Conséquence immédiate de $(u+v)^3+(u-v)^3 = 2z^3$.

4) Par utilisation du lemme ci-dessus on va maintenant montrer qu'il existe un triplet solution (x',y',z') avec $|x'| \neq |y'|$ et $|z'| < |z|$.
Deux cas sont à envisager.

cas 1 : 3 ne divise pas z.

u et u^2+3v^2 sont premiers entre eux, car sinon il existe p premier les divisant donc p divise z^3 donc z, mais z n'est pas divisible par 3, donc $p \neq 3$, et comme p divise u et $3v^2$, p divise u et v, donc divise x et y ce qui contredit le fait que x et y sont premiers entre eux.
Donc u et u^2+3v^2 sont premiers entre eux et comme $u(u^2+3v^2) = z^3$, ce sont des cubes.
Donc u et v vérifient les hypothèses du lemme et ainsi il existe deux entiers relatifs n et m premiers entre eux tels que

$u+iv\sqrt{3}=(n+im\sqrt{3})^3$, soit $u=n(n-3m)(n+3m)$ et $v=3m(n^2-m^2)$.

n et $n-3m$ sont premiers entre eux, sinon il existe $d>1$ divisant n et $n-3m$, donc divisant n et $3m$, donc u et v ce qui est impossible, u et v étant premiers entre eux

n et $n+3m$ sont premiers entre eux : même raison

$n-3m$ et $n+3m$ sont premiers entre eux : soit $d>0$ les divisant, alors d divise $2n$ et $6m$, donc divise $2u$ et $2v$, donc divise $2p\gcd(u,v)=2$, donc $d=1$ ou 2 ; mais si $d=2$, comme d divise $n-3m$, 2 divise u, mais $d=2$ divise aussi $n-3m+2m=n-m$ et 2 divise v, ce qui est impossible, u et v étant premiers entre eux.

Or u est un cube, donc $n, n-3m, n+3m$ sont des cubes :

$n-3m=x'^3, n+3m=y'^3, n=z'^3$ avec x', y', z' dans $\mathbb{Z}$.

Et évidemment $x'^3+y'^3=2z'^3$:

$|x'|\neq|y'|$ car $m\neq 0$ sinon $v=0$, de même $n\neq 0$ sinon $u=0$, et cf le 2), $uv\neq 0$.

de $u=n(n^2-9m^2)$ et $n^2-9m^2\neq 0$ (sinon $u=0$), on tire $|n|\leq|u|$ et de $u(u^2+3v^2)=z^3$ on tire $|u|(u^2+3v^2)=|z|^3$, d'où $(uv\neq 0)$ $|u|^3<|z|^3$ et finalement $|z'|^3=|n|\leq|u|<|u|^3<|z|^3$ et $|z'|<|z|$.

Donc on a trouvé un autre triplet solution (x', y', z') avec $|x'|\neq|y'|$ et $|z'|<|z|$.

cas 2 : 3 divise z.

Comme $u(u^2+3v^2)=z^3$, c'est que 3 divise u ou 3 divise u^2+3v^2 ; mais si 3 divise u^2+3v^2, 3 divise u^2 donc divise u : on a toujours 3 qui divise u.

En fait 3^2 divise u : en effet, si ce n'était pas le cas on aurait $u=3q$ avec q non divisible par 3 et comme la valuation de 3 dans z^3 est ≥ 3, c'est que 3^2 divise $u^2+3v^2=3^2q^2+3v^2$ et donc 3 divise v^2, donc 3 divise v, ce qui contredit que u et v sont premiers entre eux.

On a donc $u=3^2u'$ et $z=3z'$, d'où $3^2u'(3^4u'^2+3v^2)=3^3z'^3$, soit $u'(27u'^2+v^2)=z'^3$.

Comme u' et $27u'^2+v^2$ sont premiers entre eux (sinon il existe p premier les divisant, donc p divise u' et v^2, donc p divise u et v, ce qui est impossible) :

u' et $27u'^2+v^2$ sont des cubes : $u'=r'^3$ et $27u'^2+v^2=s'^3$.

Donc $v^2+3(3u')^2$ est un cube, avec v et $3u'$ premiers entre eux (car u et v sont premiers entre eux et $u=3(3u')$) et v et $3u'$ sont de parités différentes (car u et v sont de parités différentes et u et $3u'$ ont même parité).

On peut appliquer à nouveau le lemme :

il existe deux entiers relatifs n et m premiers entre eux tels que

$v=n(n-3m)(n+3m)$ et $3u'=3m(n^2-m^2)$.

Donc $r'^3=m(n-m)(n+m)$.

m et $n-m$ sont premiers entre eux, sinon il existe $d>1$ divisant m et $n-m$, donc divisant m et n, donc ce qui est impossible, n et m étant premiers entre eux

m et $n+m$ sont premiers entre eux : même raison

$n-m$ et $n+m$ sont premiers entre eux : soit $d>0$ les divisant, alors d divise $2n$ et $2m$, donc divise $2p\gcd(n,m)=2$, donc $d=1$ ou 2 ; mais si $d=2$, comme d divise $n-m$, $n-m$, donc $3u'$ est pair, et $n+3m=n-m+4m$ est aussi pair, donc v est pair et ainsi v et $3u'$ ont même parité ce qui est faux (voir ci-dessus).

Le produit de ces trois nombres étant un cube, ce sont des cubes :

$m-n=x'^3, n+m=y'^3, m=z'^3$ avec x', y', z' dans $\mathbb{Z}$ et donc $x'^3+y'^3=2z'^3$.

$|x'|\neq|y'|$ car $n\neq 0$ sinon $v=0$, de même $m\neq 0$ sinon $u=0$, et cf le 3), $uv\neq 0$.

de $3u'=m(n^2-m^2)$ et $n^2-m^2\neq 0$ (sinon $u=0$), on tire $|m|\leq|3u'|<3^2|u'|=|u|$ et comme (voir cas 1) $|u|^3<|z|^3$ on a $|z'|^3=|m|<|u|<|u|^3<|z|^3$ et $|z'|<|z|$.

Donc, là aussi, on a trouvé un triplet solution (x', y', z') avec $|x'|\neq|y'|$ et $|z'|<|z|$.

Conclusion : supposer que l'équation $x^3 + y^3 = 2z^3$ admette un triplet solution (x,y,z) avec $|x| \neq |y|$ implique l'existence d'un autre triplet solution (x',y',z') avec $|x'| \neq |y'|$ et $|z'| < |z|$;
rien n'empêche de continuer le processus : il existe un triplet solution (x'',y'',z'') avec $|x''| \neq |y''|$ et $|z''| < |z'| < |z|$.
En poursuivant, on va obtenir une infinité d'entiers $(|z'|, |z''|, \ldots.)$ situés dans l'intervalle $[0;|z|]$: c'est impossible!
Donc les éventuels triplets solutions $(x,y,z) \in \mathbb{Z}^3$ sont à chercher uniquement parmi ceux tels que $|x| = |y|$:

soit $x = y$ et alors $z = x$ et le triplet est (x,x,x) effectivement solution, pour tout x dans $\mathbb{Z}$

soit $x = -y$ et alors $z = 0$ et le triplet est $(x,-x,0)$ effectivement solution, pour tout x dans $\mathbb{Z}$.□

Référence 1 : Invitation aux mathématiques de Fermat-Wiles de Yves Hellegouarch, chez Masson