Equation de Fermat pour $n = 3$

P. CALDERO M1-Lyon1

Dans cette section, nous voulons montrer que l'équation

$$X^3 + Y^3 = Z^3$$

ne possède pas de solution entières. Il s'agit là d'un exemple historique de l'utilisation des anneaux factoriels en théorie des nombres.

Dans la suite, on désignera par α le complexe $\alpha = \frac{1+i\sqrt{3}}{2}$ qui est une racine primitive sixième de l'unité. Nous nous servirons des propriétés classique de l'anneau $\mathbb{Z}[\alpha]$, ces propriétés seront montrées en appendice.

On suppose tout le long par l'absurde que l'équation de Fermat possède une solution non triviale (X, Y, Z).

La méthode de descente.

Par une méthode classique qui remonte à Fermat, on se ramène au cas où X et Y sont premiers entre eux. Effectivement, si p est un nombre premier qui divise X, Y. Alors, p divise $X^3 + Y^3$ donc divise Z^3 et comme p est premier, il divise Z. On a donc $(\frac{X}{p})^3 + (\frac{Y}{p})^3 = (\frac{Z}{p})^3$ et nous obtenons ainsi un triplet solution $(\frac{X}{p}, \frac{Y}{p}, \frac{Z}{p})$. De proche en proche, on obtient un triplet tel que X et Y sont premiers entre eux. Et dans ce cas X, Y et Z sont deux à deux premiers entre eux.

Le changement de variable

Il est dû à Euler. On pose $X = U + V$ et $Y = U - V$.

Là, il faut toutefois faire attention. On veut tout de même que U et V soient des entiers, ce qui n'est pas encore garanti ! Puisque

$$U = \frac{X+Y}{2},\ V = \frac{X-Y}{2}$$

Mais, Euler a trouvé la parade : l'équation de Fermat assure qu'au moins un des entiers X, Y, Z est pair et forcément un seul, puisqu'ils sont deux à deux premiers entre eux. Donc, si Z est pair, X et Y sont tous deux impairs et U et V sont entiers. Mais si Z est impair, et si, disons, X est pair, alors on n'a qu'à changer l'équation en

$$Y^3 + (-Z)^3 = (-X)^3$$

et le tour est joué. On peut donc toujours se ramener au cas où U et V sont entiers.

L'équation de Fermat devient, après calcul

$$2U(U^2 + 3V^2) = Z^3$$

Avec les propriétés suivantes

1. U et V sont de parités différentes
2. U et V sont premiers entre eux

3. $2U$ et U^2+3V^2 sont premiers entre eux
4. $2U$ et U^2+3V^2 sont des cubes de $\mathbb{Z}$.

Le premier point est clair puisque $U+V$ (ou $U-V$) est impair. Pour le second point, il suffit de remarquer que si p premier divise U et V, alors p divise X et Y. Ce qui est impossible par hypothèse. Le troisième point découle du deuxième et du fait que 2 ne peut diviser U^2+3V^2 d'après le premier point. Par le troisième point et le fait que $\mathbb{Z}$ est factoriel, on a que $2U$ et U^2+3V^2 sont des cubes de $\mathbb{Z}$ modulo les inversibles. Mais les inversibles, 1 et -1 sont des cubes également. Donc, $2U$ et U^2+3V^2 sont des cubes de $\mathbb{Z}$.

Le lemme ad hoc.

Nous montrons que si

1. U et V sont de parités différentes
2. U et V sont premiers entre eux
3. $U^2+3V^2=W^3$,

alors il existe a, b, c entiers tels que

$$2U=(2a+b)(a-b)(a+2b),\ 2V=3ab(a+b),\ W=a^2+ab+b^2$$

On va travailler dans l'anneau factoriel $A=\mathbb{Z}[\alpha]$, l'anneau des entiers d'Eisenstein.

On écrit l'équation

$$(U+i\sqrt{3}V)(U-i\sqrt{3}V)=W^3$$

Montrons que $(U+i\sqrt{3}V)$ et $(U-i\sqrt{3}V)$ sont premiers entre eux dans A. Pour cela, on considère un élément premier d de A qui des divise tous deux. Donc d divise la somme $2U$ et la différence $2i\sqrt{3}V$. On utilise donc la norme N pour dire que $N(d)$ divise $N(U)=4U^2$ et $N(2i\sqrt{3}V)=12V^2$ dans $\mathbb{Z}$.

Montrons que 3 ne divise pas U. Effectivement, s'il le divisait, on aurait par l'équation $U^2+3V^2=W^3$, que 3 divise W donc 9 divise $U^2-W^3=-3V^2$ et donc 3 diviserait V. Ce qui est impossible car U et V sont premiers entre eux. Conclusion 3 ne divise par U, le pgcd de $4U^2$ et $12V^2$ est donc 4. Ainsi, $N(d)$ divise 4. Comme d n'est pas une unité, cela donne $N(d)=2$ ou 4. Ce qui est impossible car par hypothèses, $N(d)$ divise $N((U+i\sqrt{3}V))=U^2+3V^2$ et U^2+3V^2 est impair par hypothèses.

Conclusion, $(U+i\sqrt{3}V)$ et $(U-i\sqrt{3}V)$ sont premiers entre eux dans A, qui est factoriel. Donc, $(U+i\sqrt{3}V)$ est un cube modulo les entiers de A. C'est à dire

$$(U+i\sqrt{3}V)=\delta(a+b\alpha)^3=\delta((a+\frac{b}{2})+i\sqrt{3}\frac{b}{2})^3,$$

avec $\delta=\alpha^k$, $0\leq k\leq 5$.

1. Si $\delta=\pm 1$

   Dans ce cas, un rapide calcul donne par identification

   $$2U=(2a+b)(a-b)(a+2b),\ 2V=3ab(a+b)$$

   Pour W, le calcul est plus astucieux :

   $$W^3=U^2+3V^2=N(U+i\sqrt{3}V)=N(\delta(a+b\alpha)^3)=N(a+b\alpha)^3=(a^2+ab+b^2)^3$$

   Ce qui donne dans $\mathbb{Z}$

   $$W=(a^2+ab+b^2)$$

2. Si $\delta = \pm\alpha$

   Dans ce cas, on obtient

   $$(\frac{U}{2} + \frac{3V}{2}) + i\sqrt{3}(\frac{V}{2} - \frac{U}{2}) = (U + i\sqrt{3}V)\bar{\alpha} = \pm(a + b\alpha)^3$$

   Par le cas précédent, ceci implique que $V - U = 3ab(a+b)$. Mais ceci est impossible puisque 2 divise le membre de droite (travailler modulo 2) et 2 ne peut diviser le membre de gauche par hypothèses (U et V de parités différentes).
3. Si $\delta = \pm\alpha^2$ Ce cas est analogue. On obtient une impossibilité.

   Ceci conclut notre affaire.

On achève la preuve sans pitié.

On choisit donc une solution de l'équation de Fermat telle que $|XYZ|$ soit minimale. On trouve alors en utilisant ce qui précède que $2U = (2a + b)(a - b)(a + 2b)$ est un cube.

Montrons alors que $(2a+b)$, $(a-b)$, $(a+2b)$ sont premiers entre eux. Supposons que p premier divise $(2a + b)$ et $(a - b)$. Donc, par une habile combinaison linéaire, p divise $3a$ et $3b$. Mais si p valait 3, 3 diviserait $2U$, donc U, et l'on a vu que cela était impossible. Donc p divise a et b. Si p valait 2, alors, a et b seraient pairs et on obtiendrait que 2 divise U et V, impossible. Donc p impair divise $(2a + b)(a - b)(a + 2b) = 2U$ et $3ab(a + b) = 2V$ et donc il divise U et V, absurde. De même, on montre que les autres couples sont premier entre eux.

Comme ces trois nombres sont premiers entre eux, et que leur produit est un cube, ce sont aussi des cubes. Mézalor, $(a - b) + (a + 2b) = 2a + b$ est encore une solution de l'équation de Fermat (une somme de deux cubes qui donne un cube). Cette solution (x, y, z) vérifie

$$|xyz|^3 = |2U| = |X + Y| \leq |X^3 + Y^3|$$

La dernière inégalité vient du fait que $X + Y$ divise $|X^3 + Y^3|$. Donc $|xyz|^3 \leq |Z|^3 < |XYZ|^3$ (car les cas $X, Y = \pm 1$ sont facilement exclus). Résultat des courses, $|xyz| < |XYZ|$, absurde par minimalité.

Appendice sur l'anneau des entiers d'Eisenstein.

L'anneau des entiers d'Eisenstein est $A := \mathbb{Z}[\alpha]$, c'est aussi $\mathbb{Z}[j]$. En voici quelques propriétés.

1. Tout élément de A s'écrit de manière unique sous la forme $a + \alpha b$ avec a, b entiers.

   En fait par définition, il s'agit du plus petit anneau contenant Z et α. Il est constitué des polynômes entiers en α. Or, α vérifie

   $$\alpha^2 - \alpha + 1 = 0$$

   Et donc, par une division euclidienne de P dans $\mathbb{Z}[X]$ par $(X^2 - X + 1)$, de reste R, on peut se ramener à $P(\alpha) = R(\alpha)$ avec R de degré 1 à coefficients entiers. L'unicité est claire.
2. La norme $N(a + \alpha b)$ vaut $a^2 + ab + b^2$. Entre autres, elle est entière sur A.
3. Les éléments inversibles de A sont les racines 6-ièmes de l'unité.

   On sait que ce sont les éléments de norme 1 de A. Effectivement, A est envoyé par la norme sur $\mathbb{N}$ et de plus A est stable par l'involution bar puisque $\bar{\alpha} = \alpha - 1 \in A$. Maintenant, les éléments de norme 1 de la forme $a + \alpha b$ vérifient $1 = a^2 + ab + b^2 = (a + b/2)^2 + 3b^2/4$. ce qui donne $b = 0$ ou 1. Et on a, via un cas par cas, les solutions $(a, b) = (\pm 1, 0)$, $(0, \pm 1)$, $\pm(1, -1)$. Ce sont les racines sixièmes de l'unité.

4. A est euclidien donc factoriel.

   Soit $z = x + \alpha y$ dans $\mathbb{C}$ avec x, y réels. On choisit a, b dans $\mathbb{Z}$ tels que $|x - a| \leq 1/2$, $|y - b| \leq 1/2$. Alors,

   $$N(z - (a + \alpha b)) = (x - a)^2 + |(x - a)(y - b)| + (y - b)^2 \leq 3/4 < 1$$

   Donc, pour tout couple Z, Z' d'élements de A, avec Z' non nul, on peut en posant $z = Z/Z'$, trouver $Q = a + \alpha b$ dans A tel que $N(Z/Z' - Q) < 1$. Ce qui donne, en multipliant par $Z' : N(Z - Z'Q) < N(Z')$.

   Il suffit de poser $R = Z - Z'Q$ pour obtenir $Z = Z'Q + R$ avec $N(R) < N(Z')$.

L'anneau $\mathbb{Z}[i\sqrt{3}]$ n'est pas factoriel.

On peut ne pas comprendre pour travailler dans l'anneau A plutôt que dans l'anneau apparamment plus simple $B = \mathbb{Z}[i\sqrt{3}]$. Soit $\beta = i\sqrt{3}$.

Montrons que B n'est pas factoriel.

On a $2.2 = (1 + \beta)(1 - \beta)$. Or, 2, et $(1 \pm \beta)$ sont irréductibles.

Effectivement, supposons que 2 se décompose en $2 = (a + b\beta)(a' + b'\beta)$. Alors, $4 = N(2) = N(a + b\beta)N(a' + b'\beta)$. Et comme $N(a + b\beta)$, $N(a' + b'\beta) \neq 1$ puisque l'on a pris la norme d'éléments non inversibles, on a $N(a + b\beta) = 2$. Donc, $a^2 + 3b^2 = 2$, qui n'a pas de solution entière. Même chose pour $(1 \pm \beta)$.

Conclusion, 2, et $(1 \pm \beta)$ sont bien irréductibles, mais pour l'instant il n'y a pas de contradiction ! Il faut montrer que 2 et $(1 \pm \beta)$ ne sont pas associés. Ce qui est vrai, car si $2u = (1 \pm \beta)$, pour un élément inversible u ede B, on aurait $u = (1 \pm \beta)/2$ qui n'appartient pas à B. Mais à A.

Notons que dans A, 2 et $(1 \pm \beta)$ sont toujours irréductibles, mais ils sont associés.