1.7 DÉMONSTRATION « À LA EULER » DU THÉORÈME DE FERMAT POUR n = 3

Cette démonstration, qui pourraît être celle de Fermat, a été trouvée par Euler[10] en 1753 : elle n'utilise que la théorie de la forme quadratique X^2+3Y^2 qui, en ce qui nous concerne, suit de près celle de $X^2 + Y^2$.

Plus tard, en 1770, il en donne une forme voisine dans le langage de l'arithmétique de $\mathbb{Z}[\sqrt{-3}]$.

Considérons l'équation :

$$x^3 + y^3 = z^3 \tag{1}$$

On peut supposer que x, y, z sont premiers entre eux deux à deux et que z est pair. En posant :

$$x = p + q, \quad y = p - q$$

on obtient :

$$\frac{p}{4}(p^2 + 3q^2) = \left(\frac{z}{2}\right)^3, \quad pq \neq 0 \tag{2}$$

et x et y étant impairs, $p^2 + 3q^2$ doit être impair, ce qui entraîne que $\frac{p}{4} \in \mathbb{Z}$.

Nous allons distinguer deux cas selon que z n'est pas, ou est, un multiple de 3.

1) Si 3 ne divise pas z.

Alors les deux facteurs du premier membre de (2) sont premiers entre eux et sont donc des cubes :

$$p = 4r^3 \qquad p^2 + 3q^2 = s^3.$$

D'après le corollaire du paragraphe précédent (adapté à $\mathbb{Z}[\sqrt{-3}]$) il existe u et $v \in \mathbb{Z}$ tels que :

$$\begin{cases} p = P_3(u, v) = u(u + 3v)(u - 3v) \\ q = Q_3(u, v) = 3v(u^2 - v^2) \end{cases}$$

avec $(u, v) = 1$.

Puisque q est impair, v est impair et u est pair.

Puisque $\frac{p}{4} \in \mathbb{Z}$, on voit que $\frac{u}{4} \in \mathbb{Z}$ et puisque $\frac{p}{4} = r^3$ et 3 ne divise pas p, on voit que $u/4$, $u + 3v$ et $u - 3v$ sont des cubes :

$$u = 4a^3, \quad u + 3v = b^3, \quad u - 3v = c^3.$$

Alors on obtient :

$$(-2a)^3 + b^3 + c^3 = 0 \tag{3}$$

qui est une seconde solution de (1), mais en entiers plus petits (exercice).

10.L. Euler 1707-1783.

2) Si z est un multiple de 3.

Alors p est divisible par 3 et, comme p et q sont premiers entre eux, on voit que q n'est pas divisible par 3. On peut écrire :

$$\frac{p}{4}\left[q^2+3\left(\frac{p}{3}\right)^2\right]=9\left(\frac{z}{6}\right)^3$$

donc $\frac{p}{4}$ est un multiple de 9, ainsi :

$$\frac{p}{36}\left[q^2+3\left(\frac{p}{3}\right)^2\right]=\left(\frac{z}{6}\right)^3$$

et les deux facteurs du membre de gauche sont des cubes premiers entre eux.

Le corollaire du paragraphe précédent entraîne l'existence de u et v, premiers entre eux, tels que :

$$p=36r^3,\quad q=P_3(u,v),\quad \frac{p}{3}=Q_3(u,v)$$

d'où :

$$-4r^3=v(v+u)(v-u) \tag{4}$$

On trouve encore que u doit être impair et v pair puisque q est impair et :

$$q=P_3(u,v)=u(u+3v)(u-3v).$$

En multipliant la relation (4) par 2, on voit que $2v$, $v+u$, $v-u$ doivent être des cubes d'où, encore, une solution non triviale de (3) en entiers plus petits (exercice).

Remarque. On verra dans l'exercice 7 que l'équation :

$$x^3+y^3=2z^3 \tag{G_3}$$

peut se traiter de la même manière et que ses seules solutions primitives non triviales sont $\pm(1,1,1)$.

1.8 KUMMER 1847

On a vu plus haut qu'Euler avait aussi introduit l'anneau $\mathbb{Z}[j]$ pour étudier l'équation de Fermat du troisième degré et en admettant que le théorème fondamental de l'arithmétique s'étendait tel quel à $\mathbb{Z}[j]$ (ce qui est bien exact contrairement à ce qui se passe pour $\mathbb{Z}[\sqrt{-3}]$).

Après lui, d'autres mathématiciens (Lagrange, Gauss, Cauchy, Jacobi, Liouville) ont envisagé de généraliser cette étude aux anneaux $\mathbb{Z}[\zeta]$, où ζ désigne une racine de l'unité d'ordre premier impair, et d'étendre à ceux-ci le théorème fondamental de l'arithmétique.

En 1847, l'académie des sciences de Paris était déjà en ébullition au sujet de cette question (voir [Ed.] p. 76-80) lorsque Liouville lui annonça que Kummer avait prouvé trois ans plus tôt que le théorème fondamental de l'arithmétique ne s'étendait pas à $\mathbb{Z}[\zeta]$ mais que la théorie de la factorisation pouvait être sauvée par l'introduction de « nombres idéaux ».

© Dunod. La photocopie non autorisée est un délit.