DÉVELOPPEMENT 17

ÉQUATION DE FERMAT POUR $n = 2$ ET $n = 4$

Proposition. — *Pour que $(x, y, z) \in \mathbb{N}^3$ soit solution de l'équation $x^2 + y^2 = z^2$ il faut et il suffit qu'il existe $d \in \mathbb{N}$ et $u, v \in \mathbb{N}^*$ premiers entre eux tels que*

$$(x, y, z) = \left(d(u^2 - v^2), 2duv, d(u^2 + v^2)\right) \quad ou \quad \left(2duv, d(u^2 - v^2), d(u^2 + v^2)\right).$$

Démonstration. — Il est clair qu'un tel triplet est solution. Réciproquement, les solutions où l'une des variables est nulle sont de cette forme et si on a une solution x, y, z, on en obtient une autre en divisant par leur pgcd. On peut donc supposer que x, y et z sont premiers dans leur ensemble (on dira que (x, y, z) est une solution *première*) alors

- x, y et z sont premiers entre eux deux à deux,
- au plus un des entiers x, y ou z est pair (sinon 2 diviserait x,y et z),
- x et y ne sont pas impairs tous les deux (sinon on aurait $x^2 \equiv 1[4]$ et $y^2 \equiv 1[4]$ d'où $z^2 \equiv 2[4]$ ce qui est impossible).

Quitte à inverser les rôles de x et y, on suppose donc que (x, y, z) est une solution vérifiant x pair, y impair et z impair.

On a $\left(\frac{x}{2}\right)^2 = \left(\frac{z-y}{2}\right)\left(\frac{z+y}{2}\right)$ donc $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont des carrés d'entiers. En effet, tous les diviseurs premiers de $\left(\frac{x}{2}\right)^2$ apparaissent au carré et $\frac{z-y}{2}$ et $\frac{z+y}{2}$ sont premiers entre eux puisque z et y sont premiers entre eux. On a donc $\frac{z-y}{2} = m^2$ et $\frac{z+y}{2} = n^2$ avec $m, n \in \mathbb{N}*$ d'où $x = 2mn$, $y = n^2 - m^2$ et $z = m^2 + n^2$. On vérifie alors qu'un tel triplet est bien solution. □

Proposition. — *Les équations $x^4 + y^4 = z^2$ et $x^4 + y^4 = z^4$ n'ont pas de solution dans $(\mathbb{N}^*)^3$.*

Démonstration. — Il suffit de montrer que la première n'a pas de solution $(x, y, z) \in (\mathbb{N}^*)^3$. Supposons par l'absurde qu'il existe une telle solution, on peut de plus choisir z minimal. Alors x, y et z sont premiers dans leur ensemble (sinon, en notant d le pgcd, $(\frac{x}{d}, \frac{y}{d}, \frac{z}{d^2})$ serait solution mais $\frac{z}{d^2} < z$). D'après la première proposition, il existe des entiers u et v premiers entre eux avec $0 < v < u$ tels que $x^2 = 2uv$, $y^2 = u^2 - v^2$ et $z = u^2 + v^2$ (quitte à échanger les rôles de x et y).

Si $u \equiv 0[2]$ alors $v \equiv 1[2]$ (puisque $u \wedge v = 1$) d'où $y^2 \equiv -1[4]$ ce qui est impossible puisqu'un carré est congru à 0 ou 1 modulo 4 donc u est impair et v est pair. On a $v^2 + y^2 = u^2$ avec u, v et y premiers dans leur ensemble (puisque $u \wedge v = 1$) donc il existe des entiers r et s premiers entre eux tels que $v = 2rs$, $y = r^2 - s^2$ et $u = r^2 + s^2$. Il s'ensuit que $x = 2uv = 4rs(r^2 + s^2)$ mais r, s et $r^2 + s^2$ sont premiers entre eux deux à deux donc ce sont tous des carrés *i.e.* $r = \alpha^2$, $s = \beta^2$ et $r^2 + s^2 = \gamma^2$ d'où $\alpha^4 + \beta^4 = \gamma^2$. Or $x \neq 0$ et $y \neq 0$ donc $\alpha \neq 0$ et $\beta \neq 0$ et on a $\gamma^2 = s^2 + r^2 = u < u^2 + v^2 = z$ ce qui contredit la minimalité de z. □

Leçons concernées

09 Congruences dans $\mathbb{Z}$, anneau $\mathbb{Z}/n\mathbb{Z}$. Applications

10 Nombres premiers. Applications

18 Équations diophantiennes du premier degré $ax + by = c$. Exemples d'équations diophantiennes de degré supérieur

Références

F. Combes, *Algèbre et géométrie*, Bréal, 1998.

X. Gourdon, *Algèbre*, Ellipses, 1994.

Sébastien Pellerin