■ Forum nº 266

Au plus trois carrés en progression arithmétique

Théorème (Fermat, Euler)**.**
Il est impossible de trouver quatre carrés d'entiers naturels distincts en progression arithmétique.

> *Ce joli résultat, conjecturé par Fermat et démontré par Euler (une preuve confuse, rédigée par les assistants du maître, selon André Weil [1]), a animé la liste* `ups-math` *récemment. Les preuves élémentaires ne sont pas simples. La preuve reprise par Dickson ne semble pas viable. Les autres preuves élémentaires utilisent une descente infinie, elles sont souvent « elliptiques ». Vous trouverez ci-dessous la jolie preuve de Jean Itard (un peu plus détaillée que dans la version originale [2]) et celle, plus courte, de Russell A. Gordon et Sara L. Graham (qui expliquent également dans leur article [4] pourquoi la preuve proposée par Dickson n'aboutit pas). Vous pourrez également trouver d'autres preuves dans [5] ou [6].*

Remarque. Dans ce qui suit, sauf précisions contraires, les nombres rencontrés sont des entiers.

Rappelons d'abord la forme bien connue des triplets pythagoriciens primitifs, c'est-à-dire des triplets (a,b,c) d'entiers naturels non nuls et premiers entre eux dans leur ensemble, vérifiant $a^2+b^2=c^2$. Notons qu'alors, parmi a et b, un et un seul des deux entiers est pair.

Théorème (Triplets pythagoriciens primitifs)**.**
Les triplets pythagoriciens primitifs (a,b,c) avec a impair sont les triplets

$$(p^2-q^2, 2pq, p^2+q^2),$$

avec p,q entiers naturels non nuls, premiers entre eux, de parités opposées, et $p>q$.

La preuve de Jean Itard

► **Trois carrés en progression arithmétique**
Soient trois carrés $x^2<y^2<z^2$ avec $y^2-x^2=z^2-y^2$, soit $2y^2=x^2+z^2$.
Les entiers x et z ayant la même parité, on peut poser $x=p-q$ et $z=p+q$ avec $p>q$, d'où l'on déduit $y^2=p^2+q^2$.
Si x,y,z sont premiers entre eux alors p,q,y aussi et on peut écrire (triplet pythagoricien) :

$$y=a^2+b^2 \quad \text{et } \{p,q\}=\{2ab, b^2-a^2\} \quad (\text{avec } a<b).$$

On en déduit

$$x=\left|(a+b)^2-2b^2\right|, \quad y=a^2+b^2 \quad \text{et} \quad z=(a+b)^2-2a^2.$$

► **Quatre carrés en progression arithmétique**

Supposons qu'il existe quatre carrés en progression arithmétique, $x^2 < y^2 < z^2 < t^2$, et supposons que z soit le plus petit possible. Ils sont alors premiers entre eux dans leur ensemble, donc les trois premiers et les trois derniers aussi. On peut reprendre les formules précédentes pour les trois premiers, et les trois derniers s'expriment de manière analogue aux trois premiers :

$$y = \left|(u+v)^2 - 2v^2\right|, \quad z = u^2 + v^2 \quad \text{et} \quad t = (u+v)^2 - 2u^2, \quad \text{avec } u < v.$$

On en déduit le système $\begin{cases} a^2 + b^2 = \left|(u+v)^2 - 2v^2\right| \\ (a+b)^2 - 2a^2 = u^2 + v^2 \end{cases}$

– Premier cas : $u + v > v\sqrt{2}$.

En ajoutant et en retranchant les deux équations on obtient le système $(\star)$ suivant :

$$\begin{cases} b(a+b) = u(u+v) \\ a(b-a) = v(v-u) \end{cases} \qquad (\star)$$

– Deuxième cas : $u + v < v\sqrt{2}$.

En ajoutant et en retranchant les deux équations on obtient le système

$$\begin{cases} b(a+b) = v(v-u) \\ a(b-a) = u(v+u) \end{cases}$$

On se ramène au premier cas en posant $v = u'$ et $u = -v'$

On peut donc se limiter au premier cas et donc au système $(\star)$ avec v éventuellement négatif.

► **Utilisation d'une méthode diophantienne**

Posons $b = ru$,avec r nombre rationnel, dans le système $(\star)$:

$$\begin{cases} r(a + ru) = u + v \\ ra(r^2u - ra) = r^2v(v-u) \end{cases}$$

En reportant $ra = u\left(1 - r^2\right) + v$ dans la seconde équation, on obtient

$$\left(u\left(1-r^2\right) + v\right)\left(\left(2r^2 - 1\right)u - v\right) = r^2v(v-u),$$

qui s'écrit encore

$$u^2\left(1-r^2\right)\left(2r^2-1\right) + 2uv\left(2r^2-1\right) - v^2\left(1+r^2\right) = 0.$$

Pour que cette équation du second degré en u/v ait des solutions rationnelles, il faut que son discriminant réduit $\Delta = (2r^2-1)^2 + (1-r^4)(2r^2-1) = (2r^2-1)(2r^2-r^4)$ soit un carré de nombre rationnel, ou encore que $(2r^2-1)(2-r^2)$ soit un carré.

Posons $r = \dfrac{c}{d}$, avec c et d premiers entre eux. Il faut donc que $(2c^2-d^2)(2d^2-c^2)$ soit le carré d'un entier.

Les entiers $2c^2 - d^2$ et $2d^2 - c^2$ sont premiers entre eux car, si un nombre premier p divise $2c^2 - d^2$ et $2d^2 - c^2$, alors il divise $3c^2$ et $3d^2$, donc $p = 3$ divise $2c^2 - d^2$. Par réduction modulo 3, on prouve que 3 divise c et d : contradiction.

Les entiers $2c^2 - d^2$ et $2d^2 - c^2$ sont de même signe et donc positifs (leur somme est positive), on peut donc écrire $2c^2 - d^2 = \alpha^2$ et $2d^2 - c^2 = \beta^2$, avec α et β entiers. Par suite, α^2, c^2, d^2 et β^2 sont des carrés en progression arithmétique.

Comme $r = \dfrac{c}{d} = \dfrac{b}{u}$ avec la première fraction réduite, on a $c \leqslant b$ et $d \leqslant u$.

Par suite, $c^2 < a^2 + b^2 = y < y^2 < z^2$ et $d^2 < u^2 + v^2 = z < z^2$, on a donc un quadruplet avec c et d strictement plus petits que z : contradiction.

La preuve de Russell A. Gordon et Sara L. Graham

Théorème 1.
Il n'existe pas de paire de triplets pythagoriciens de la forme (a, b, c) et $(a, 2b, d)$.

Démonstration. Supposons qu'il en existe une.

On peut supposer ces triplets primitifs. En effet, si $g = \text{pgcd}(a, b) > 1$, on obtient une paire de triplets pythagoriciens (a', b', c') et $(a', 2b', d')$ dont le premier est primitif en divisant les deux triplets par g. De plus, si a' est impair, alors les deux triplets sont primitifs ; et, si a' est pair, b' est alors impair, on peut diviser le second triplet par 2, et $(b', a'/2, d'/2)$ et (b', a', c') sont deux triplets primitifs de la même forme.

On peut aussi supposer que b est le plus petit possible. Un (seul) des entiers a ou b est pair, c'est nécessairement b, et les autres entiers en jeu sont impairs.

On en déduit l'écriture

$$a = v^2 - u^2, \quad b = 2uv, \quad c = u^2 + v^2, \quad \text{avec } \text{pgcd}(u, v) = 1, v > u \text{ et } u + v \text{ impair.}$$

De même,

$$a = y^2 - x^2, \quad 2b = 2xy, \quad d = x^2 + y^2, \quad \text{avec } \text{pgcd}(x, y) = 1, y > x \text{ et } x + y \text{ impair.}$$

Les entiers u et v sont de parités opposées. Modulo 4, a est congru à 1 si v est impair, -1 sinon. On en déduit que u et x ont la même parité. On suppose par exemple qu'ils sont impairs, et donc v et y pairs. Le cas où u et x sont pairs revient à échanger dans la suite x et y, u et v.

De $uv = x(y/2)$, on peut déduire $u = \alpha\beta$, $v = \gamma\delta$, $x = \alpha\gamma$ et $y = 2\beta\delta$, les entiers $\alpha, \beta, \gamma, \delta$ étant premiers deux à deux. De plus, α est impair (car u est impair), δ est pair (car v est pair et γ, qui divise x, est impair).

De $a = v^2 - u^2 = y^2 - x^2$ on déduit $u^2 + y^2 = x^2 + v^2$, d'où $\beta^2(\alpha^2 + 4\delta^2) = \gamma^2(\alpha^2 + \delta^2)$.

Puisque $\text{pgcd}(\beta, \gamma) = 1$ et $\text{pgcd}(\alpha^2 + \delta^2, \alpha^2 + 4\delta^2) = 1$, on a $\alpha^2 + \delta^2 = \beta^2$ et $\alpha^2 + 4\delta^2 = \gamma^2$, d'où une paire de triplets pythagoriciens primitifs de la forme (α, δ, β) et $(\alpha, 2\delta, \gamma)$ avec δ pair et $\delta \leqslant y/2 < y \leqslant b$, ce qui est en contradiction avec b minimal. □

Théorème 2. Il n'existe pas quatre carrés distincts en progression arithmétique.

Démonstration. Supposons $x^2 < y^2 < z^2 < t^2$ en progression arithmétique : $x^2 + z^2 = 2y^2$ et $y^2 + t^2 = 2z^2$. On peut les supposer premiers entre eux deux à deux et, par suite, x et z, qui ont la même parité, sont impairs, et y et t aussi. En posant $a = x^2$ et $r = y^2 - x^2$, r est pair, strictement positif, et $a(a+r)(a+2r)(a+3r)$ est un carré.

Nous allons démontrer qu'une égalité $a(a+r)(a+2r)(a+3r) = b^2$ avec $r > 0$ pair n'est pas possible.

On peut supposer a et r premiers entre eux.

$$b^2 = a(a+3r)(a+r)(a+2r) = (a^2+3ar)(a^2+3ar+2r^2) = (a^2+3ar+r^2)^2 - r^4,$$

donc $(b, r^2, a^2+3ar+r^2)$ est un triplet pythagoricien. Il est primitif car un nombre premier divisant b et r^2, donc r, diviserait a et r.

On peut donc écrire $r^2 = 2uv$ et $a^2+3ar+r^2 = u^2+v^2$, avec u et v premiers entre eux, de parités opposées. Par symétrie, on peut supposer u pair. Comme $(u/2)v$ est un carré avec u et v premiers entre eux, on peut écrire $u = 2c^2$ et $v = d^2$, avec c et d premiers entre eux. Alors $\left(a + \dfrac{3}{2}r\right)^2 = a^2+3ar+r^2+\dfrac{5}{4}r^2 = 4c^4+d^4+5c^2d^2 = (c^2+d^2)(4c^2+d^2)$.

Comme c et d sont premiers entre eux, c^2+d^2 et $4c^2+d^2$ sont premiers entre eux, chacun de ces nombres est donc un carré, ce qui contredit le théorème 1. □

Bibliographie

[1] André WEIL. *Number Theory. An approach through history from Hammurapi to Legendre*. Birkhäuser, Berlin, 1984.

[2] Jean ITARD. *Arithmétique et Théorie des Nombres*. P.U.F., Paris, 1973.

[3] Leonard E. DICKSON. *History of the Theory of Numbers*, Vol. 2. Chelsea Publishing Co., New York, 1934.

[4] Russell A. GORDON, Sara L. GRAHAM. Comments on proofs that there are no four squares in arithmetic progression. *The Fibonacci Quarterly*, 53 (2015), 1, 68–73.
`https://doi.org/10.1080/00150517.2015.12428290`

[5] Kevin BROWN. No Four Squares In Arithmetic Progression.
`https://www.mathpages.com/home/kmath044/kmath044.htm`

[6] Alf VAN DER POORTEN. Fermat's four squares theorem.
`https://arxiv.org/pdf/0712.3850`, 2007.