Sommes de trois carrés

Alexandre Junod, Lycée Denis-de-Rougemont (Neuchâtel), alexandre.junod@rpn.ch

Problématique

Un nombre entier $m > 0$ étant donné, on veut savoir s'il existe trois autres entiers x, y et z tels que $m = x^2 + y^2 + z^2$. On peut déjà remarquer que, modulo 4, le carré d'un nombre pair est congru à 0 et celui d'un nombre impair est congru à 1. Il s'ensuit que si $m = x^2 + y^2 + z^2$ est divisible par 4, alors x, y et z sont pairs et $\frac{m}{4}$ est également une somme de trois carrés. La réciproque est trivialement vraie (si m est somme de trois carrés, alors $4m$ en est aussi une) et en réitérant au besoin le raisonnement, on est amené à n'étudier que les nombres m qui ne sont pas divisibles par 4. D'autre part, modulo 8, un carré d'entier ne peut être congru qu'à 0, 1 ou 4, donc si le nombre m est une somme de trois carrés, il ne peut pas être congru à 7 modulo 8. Il ne reste à étudier que les nombres m congrus à 1, 2, 3, 5 ou 6 (modulo 8) et nous allons montrer qu'une décomposition en somme de trois carrés est toujours possible dans ces cas. On peut supposer que m n'est divisible par aucun carré parfait.

1 Résultat préliminaire

Inspiré par [2] (lemmes des pages 37-42), nous allons montrer qu'il existe un nombre r, somme de deux carrés, qui est congru à -1 modulo m et tel que m est un carré modulo r. En d'autres termes, il existe trois nombres entiers a, b et c tels que m divise $a^2 + b^2 + 1$ et $a^2 + b^2$ divise $c^2 - m$.

• Cas $m \equiv 2 \pmod 4$, c'est-à-dire $m \equiv 2$ ou $m \equiv 6 \pmod 8$

Les nombres $8m$ et $m - 1$ sont premiers entre eux car tout diviseur commun divise $8m - 8(m - 1) = 8$ alors que $m - 1$ est impair. Par le théorème de Dirichlet (que nous admettons), il existe un nombre premier de la forme $p = (m - 1) + k \cdot 8m$. Il est congru à 1 modulo 4 et un théorème de Fermat nous assure qu'il s'agit d'une somme de deux carrés (voir [3]). De plus, ce nombre premier est congru à -1 modulo m, donc modulo tout nombre premier q qui divise m. Ainsi, si on écrit $m = 2m'$, la loi de réciprocité quadratique (voir [4]) permet d'écrire

$$\left(\frac{m}{p}\right) = \left(\frac{2m'}{p}\right) = \left(\frac{2}{p}\right) \prod_{q|m'} \left(\frac{q}{p}\right) = \left(\frac{2}{p}\right) \prod_{q|m'} \left(\frac{p}{q}\right) = \left(\frac{2}{p}\right) \prod_{q|m'} \left(\frac{-1}{q}\right) = \left(\frac{2}{p}\right) \prod_{q \equiv 3} (-1)$$

où la congruence sur les diviseurs premiers (impairs) de m' est à considérer modulo 4.

- Si m' a un nombre pair de diviseurs premiers congrus à 3 modulo 4, alors $m' \equiv 1 \pmod 4$, $m \equiv 2 \pmod 8$, $p \equiv 1 \pmod 8$ et donc $\left(\frac{2}{p}\right) = 1$ (voir [4]).
- Sinon, $m' \equiv 3 \pmod 4$, $m \equiv 6 \pmod 8$, $p \equiv 5 \pmod 8$ et donc $\left(\frac{2}{p}\right) = -1$ (voir [4]).

Dans tous les cas, on a $\left(\frac{m}{p}\right) = 1$, autrement dit m est un carré modulo p.

• Cas $m \equiv 1 \pmod 4$, c'est-à-dire $m \equiv 1$ ou $m \equiv 5 \pmod 8$

Alors $2m \equiv 2 \pmod 8$ et, par le cas précédent, il existe un nombre premier $p = (2m-1) + k \cdot 16m$ qui est une somme de deux carrés, congru à -1 modulo $2m$ donc modulo m, et tel que $2m$ est un carré modulo p. Comme $p \equiv 1 \pmod 8$, alors 2 est un carré modulo p (voir [4]) et il en est de même pour m car les congruences $2 \equiv x^2$ et $2m \equiv y^2$ impliquent $m \equiv 2^{-1}y^2 \equiv (x^2)^{-1}y^2 = (x^{-1}y)^2 \pmod p$.

• Cas $m \equiv 3 \pmod 8$

Les nombres $4m$ et $\frac{m-1}{2}$ sont premiers entre eux car tout diviseur commun divise $4m - 8\frac{m-1}{2} = 4$ alors que $\frac{m-1}{2}$ est impair. Par le théorème de Dirichlet, il existe un nombre premier de la forme $p = \frac{m-1}{2} + k \cdot 4m$. Comme il est congru à 1 modulo 4, il s'agit d'une somme de deux carrés. Le nombre $2p = (m-1) + k \cdot 8m$ est également une somme de deux carrés car $2(x^2+y^2) = (x+y)^2 + (x-y)^2$. Il est congru à -1 modulo m et la loi de réciprocité quadratique (voir [4]) implique

$$\left(\frac{m}{p}\right) = \prod_{q|m}\left(\frac{q}{p}\right) = \prod_{q|m}\left(\frac{p}{q}\right) = \prod_{q|m}\left(\frac{4p}{q}\right) = \prod_{q|m}\left(\frac{-2}{q}\right) = \prod_{\substack{q\equiv 5\\ q\equiv 7}}(-1),$$

où les congruences sur les diviseurs premiers de m sont à considérer modulo 8. On peut donc écrire

$$m = \left(\prod_{q\equiv 1} q\right)\left(\prod_{q\equiv 3} q\right)\left(\prod_{q\equiv 5} q\right)\left(\prod_{q\equiv 7} q\right) \equiv \left(\prod_{q\equiv 3} 3\right)\left(\prod_{q\equiv 5}(-3)\right)\left(\prod_{q\equiv 7}(-1)\right) = \underbrace{\left(\prod_{q\equiv \pm 3} 3\right)}_{A}\left(\frac{m}{p}\right).$$

On a $A \equiv 1$ ou $A \equiv 3$ alors que $\left(\frac{m}{p}\right) = \pm 1$. Comme $m \equiv 3$, la seule possibilité est $A \equiv 3$ et $\left(\frac{m}{p}\right) = 1$. Ainsi, il existe un entier x tel que p divise $x^2 - m$. Quitte à remplacer x par $x + p$, on peut supposer que x est impair, tout comme m. Ainsi $x^2 - m$ est pair et m est un carré modulo $2p$.

2 Décomposition en somme de trois carrés rationnels

Par construction, r est une somme de deux carrés congrue à -1 modulo m et il existe un nombre ρ tel que $m \equiv \rho^2 \pmod r$. L'ensemble $E = \{0, 1, \ldots, \lfloor\sqrt{mr}\rfloor\} \times \{0, 1, \ldots, \lfloor\sqrt{m}\rfloor\} \times \{0, 1, \ldots, \lfloor\sqrt{r}\rfloor\}$ est de cardinalité $(1 + \lfloor\sqrt{mr}\rfloor)(1 + \lfloor\sqrt{m}\rfloor)(1 + \lfloor\sqrt{r}\rfloor) > \sqrt{mr}\sqrt{m}\sqrt{r} = mr$. Par le principe des tiroirs, il contient au moins deux éléments distincts $(x_1; y_1; z_1)$ et $(x_2; y_2; z_2)$ tels que $x_1 - ry_1 + (r+1)\rho z_1$ et $x_2 - ry_2 + (r+1)\rho z_2$ aient le même reste lors de la division euclidienne par mr. Si on pose $x = x_1 - x_2$, $y = y_1 - y_2$ et $z = z_1 - z_2$, on a alors la congruence $x - ry + (r+1)\rho z \equiv 0 \pmod{mr}$. En la multipliant par $x + ry - (r+1)\rho z$, on obtient

$$x^2 - (ry - (r+1)\rho z)^2 \equiv 0 \pmod{mr}.$$

Le membre de gauche est congru à $x^2 + ry^2 - mz^2$ modulo m (car $r \equiv -1 \pmod m$) et modulo r. Comme m et r sont premiers entre eux, la congruence a lieu modulo mr, autrement dit $x^2 + ry^2 - mz^2$ est un multiple de mr. De plus, comme $|x| < \sqrt{mr}$, $|y| < \sqrt{m}$ et $|z| < \sqrt{r}$, on a

$$-mr < -mz^2 \leqslant x^2 + ry^2 - mz^2 \leqslant x^2 + ry^2 < mr + mr = 2mr.$$

On en déduit que $x^2 + ry^2 - mz^2 = 0$ ou $x^2 + ry^2 - mz^2 = mr$. Dans ce dernier cas, on peut écrire $x^2 + ry^2 - m(z^2 + r) = 0$ et en multipliant par $z^2 + r$, on trouve

$$0 = (x^2 + ry^2)(z^2 + r) - m(z^2 + r)^2 = (xz + ry)^2 + r(yz - x)^2 - m(z^2 + r)^2.$$

Quitte à renommer les choses, on peut supposer $x^2+ry^2-mz^2=0$ et comme r est une somme de deux carrés, disons $r=r_1^2+r_2^2$, on a $x^2+(r_1y)^2+(r_2y)^2=z^2m$. Ceci signifie que m est une somme de trois carrés de nombres rationnels dont z est un dénominateur commun.

3 Algorithme final

Nous donnons ici une démonstration adaptée du théorème d'Aubry qui affirme qu'une somme entière de trois carrés de nombres rationnels est une somme de trois carrés d'entiers. On suppose donc que $m=(x/d)^2+(y/d)^2+(z/d)^2$ où les entiers x, y et z ne sont pas tous divisibles par $d>0$ (sinon, le théorème serait trivialement démontré). D'un point de vue géométrique, le point $P(x/d;y/d;z/d)$ se trouve sur la sphère $\mathcal{S}$ centrée en l'origine et de rayon $\sqrt{m}$. En arrondissant chacune de ses coordonnées à l'entier le plus proche, on obtient un point différent $Q([x/d];[y/d];[z/d])$. La droite (QP) est dirigée par le vecteur non nul $d\cdot\overrightarrow{QP}$ dont les composantes sont des nombres entiers et tout point P' situé sur cette droite vérifie une relation vectorielle $\overrightarrow{OP'}=\overrightarrow{OQ}+\lambda d\overrightarrow{QP}$ avec $\lambda\in\mathbb{R}$. On peut écrire

$$\|\overrightarrow{OP'}\|^2-m=\lambda^2\underbrace{d^2\|\overrightarrow{QP}\|^2}_{a>0}+\underbrace{2d(\overrightarrow{OQ}\cdot\overrightarrow{QP})}_{b}\lambda+\underbrace{\|\overrightarrow{OQ}\|^2-m}_{c}.$$

Cette expression est quadratique en λ avec des coefficients a, b et c entiers. Elle s'annule lorsque $\lambda=\frac{1}{d}$ (car alors $P'=P$) et pour $\lambda=\frac{d\cdot c}{a}$ par la relation de Viète. Le nombre a est un entier strictement positif et, modulo d, on a $a=\|d\cdot\overrightarrow{QP}\|^2=\|d\cdot\overrightarrow{OP}-d\cdot\overrightarrow{OQ}\|^2\equiv\|d\cdot\overrightarrow{OP}\|^2=x^2+y^2+z^2=md^2\equiv 0$. Il s'ensuit que $d'=\frac{a}{d}=d\|\overrightarrow{QP}\|^2$ est un entier positif. On a la majoration

$$d'=d\left(\left(\frac{x}{d}-\left[\frac{x}{d}\right]\right)^2+\left(\frac{y}{d}-\left[\frac{y}{d}\right]\right)^2+\left(\frac{z}{d}-\left[\frac{z}{d}\right]\right)^2\right)\leqslant d\left(\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2+\left(\frac{1}{2}\right)^2\right)<d.$$

Pour résumer, l'égalité $\|\overrightarrow{OP'}\|^2=m$ a lieu lorsque $\lambda=\dfrac{d\cdot c}{a}=\dfrac{c}{d'}$. Les coordonnées du point P' associé (deuxième point d'intersection de (QP) avec $\mathcal{S}$) sont des nombres rationnels ayant le dénominateur commun $d'<d$ et des numérateurs $\widetilde{x}=d'[x/d]+c\,(x-d[x/d])$, $\widetilde{y}$ et $\widetilde{z}$ (définis de manière analogue). On peut itérer l'algorithme $(x;y;z;d)\longmapsto(\widetilde{x};\widetilde{y};\widetilde{z};d')$ jusqu'à ce que d' divise $\widetilde{x}$, $\widetilde{y}$ et $\widetilde{z}$, quitte à avoir $d'=1$. On obtient alors la décomposition $m=(\widetilde{x}/d')^2+(\widetilde{y}/d')^2+(\widetilde{z}/d')^2$ avec trois carrés d'entiers.

4 Conclusion et références

Nous avons démontré le théorème de Legendre $(1752-1833)$ qui stipule que tout nombre entier peut s'écrire comme une somme de trois carrés, sauf s'il est de la forme $m=4^k(8n+7)$ avec k et n entiers. Comme toutes les preuves que nous avons rencontrées, notre version mobilise le théorème de Dirichlet, la loi de réciprocité quadratique et le théorème de Fermat concernant les sommes de deux carrés mais elle évite d'autres résultats tels la théorie des formes quadratiques ou le théorème de Minkowski sur les espaces convexes symétriques (voir [1] ou [2]).

[1] V. CHISTOLINI, T. MACDONALD, M. ZHANG
Representing numbers as sums of three squares : history and proofs,
`www.maths.dk/teaching/courses/math357-spring2016/projects/three_squares.pdf`

[2] J. CRETAL, A. SALVARY, *Sommes de carrés*, Travail de Master, 2009-2010
`http://math.univ-lille1.fr/~bhowmik/enseignement/Mem_master/mem_sommescarres.pdf`

[3] A. JUNOD, *Sommes de deux et quatre carrés*, Bulletin de la SSPMP n° 144, septembre 2020

[4] A. JUNOD, *La loi de réciprocité quadratique*, Bulletin de la SSPMP n° 146, mai 2021