NOUVELLES ANNALES DE MATHÉMATIQUES

S. REALIS

Scolies pour un théorème d'arithmétique

Nouvelles annales de mathématiques 2e série, tome 12 (1873), p. 212-223

<http://www.numdam.org/item?id=NAM_1873_2_12__212_1>

SCOLIES POUR UN THÉORÈME D'ARITHMÉTIQUE;

PAR M. S. REALIS,
Ingénieur à Turin.

LEMME I. — *Tout nombre entier de l'une des formes*

$$8n+3,\quad 4n+1,\quad 4n+2$$

est la somme de trois carrés.

Pour la démonstration de ce lemme, qui contient trois propositions distinctes, nous renvoyons à la *Théorie des nombres* de Legendre (3[e] édition, t. I, p. 393 et suiv.).

Les propositions énoncées, ainsi que les conséquences que nous allons en déduire, peuvent être considérées comme autant de scolies au théorème général énoncé par Bachet de Méziriac et par Fermat, et démontré par Lagrange, que *tout nombre entier est la somme de quatre carrés.*

Nous n'avons pas besoin d'ajouter que, dans les énoncés, on regarde zéro comme un carré dont la racine est nulle.

THÉORÈME I. — *Tout nombre impair est la somme de quatre carrés dont les racines, prises avec des signes convenables, ont une somme algébrique égale à l'unité.*

D'après le lemme ci-dessus, et en observant que les trois carrés dans lesquels se décompose un nombre de la forme $8n+3$ ne peuvent être qu'impairs, nous pouvons poser

$$(1) \qquad 8n+3=(2a-1)^2+(2b-1)^2+(2c-1)^2,$$

et nous serons assurés que, pour toute valeur entière et positive de n, on peut assigner des valeurs entières de a, b, c satisfaisant à la formule (1).

Cela posé, nous observerons que la relation (1) entre n, a, b, c est équivalente à l'une quelconque des suivantes :

$$(2) \qquad 2n+1=\alpha^2+\beta^2+\gamma^2+\delta^2,$$

$$(3) \qquad 2n+1=\alpha'^2+\beta'^2+\gamma'^2+\delta'^2,$$

où l'on a fait, pour abréger,

$$\alpha = \frac{-a+b-c+1}{2},$$

$$\beta = \frac{-a-b+c+1}{2},$$

$$\gamma = \frac{a-b-c+1}{2},$$

$$\delta = \frac{a+b+c-1}{2},$$

et

$$\alpha' = \frac{-a+b+c}{2},$$

$$\beta' = \frac{a-b+c}{2},$$

$$\gamma' = \frac{a+b-c}{2},$$

$$\delta' = \frac{-a-b-c+2}{2};$$

ce qui se trouve vérifié par l'identité des valeurs de n tirées des formules considérées.

Maintenant, dans la formule (1), il peut arriver deux cas, selon que la somme $a+b+c$ est un nombre impair ou un nombre pair. Dans le premier cas, les nombres α, β, γ, δ sont entiers; dans l'autre cas, les nombres α', β', γ', δ' sont entiers; on a d'ailleurs

$$\alpha+\beta+\gamma+\delta=1$$

pour la formule (2), et

$$\alpha'+\beta'+\gamma'+\delta'=1$$

pour la formule (3). Dans les deux cas, le nombre $2n+1$ est décomposé en quatre carrés, dont les racines sont des entiers donnant une somme algébrique égale à l'unité; ainsi le théorème énoncé se trouve démontré.

Et comme de l'une quelconque des formules (2), (3) on remonte de suite à la formule (1), on voit que, si l'on avait une démonstration directe du théorème I, celle du lemme I, en ce qui concerne la décomposition du nombre $8n+3$ en trois carrés, s'ensuivrait immédiatement.

Ajoutons, en passant, que la valeur de n tirée de l'une quelconque des équations (1), (2), (3) étant

$$n = \frac{a^2-a}{2} + \frac{b^2-b}{2} + \frac{c^2-c}{2},$$

il en résulte le théorème de Fermat sur la décomposition d'un entier en trois nombres triangulaires.

THÉORÈME II. — *Tout nombre double d'un impair est la somme de quatre carrés dont les racines ont une somme algébrique égale à zéro.*

Un corollaire immédiat de la troisième partie du lemme I établit que *tout nombre impair est la somme de quatre carrés dont deux sont égaux.*

On peut donc poser

$$2n+1 = a^2+b^2+c^2,$$

a, b, c étant des entiers.

On déduit de là

$$4n+2 = (a+c)^2 + (-a+c)^2 + (-b-c)^2 + (b-c)^2,$$

où

$$(a+c) + (-a+c) + (-b-c) + (b-c) = 0;$$

ce qui démontre la proposition.

Réciproquement, de ce qu'un nombre double d'un impair se décompose en quatre carrés dont les racines fournissent une somme algébrique nulle, il s'ensuit que l'impair considéré est la somme de quatre carrés dont deux sont égaux.

THÉORÈME III. — *Tout nombre double d'un impair est la somme de quatre carrés dont les racines ont une somme algébrique égale à* 2.

Quel que soit l'entier positif n, on peut satisfaire à l'équation

$$(4) \qquad 4n + 1 = (2a - 1)^2 + 4b^2 + 4c^2$$

par des valeurs entières de a, b, c; c'est ce que nous apprend le lemme I, où il est à observer que, des trois carrés dans lesquels se décompose le nombre $4n + 1$, un seul peut et doit être impair.

Mais on s'assure à l'instant que la relation (4) est équivalente à la suivante :

$$4n + 2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2,$$

où

$$\alpha = a + b + c,$$
$$\beta = a - b - c,$$
$$\gamma = -a + b - c + 1,$$
$$\delta = -a - b + c + 1,$$

et

$$\alpha + \beta + \gamma + \delta = 2.$$

De là le théorème énoncé.

Réciproquement, de ce théorème, supposé établi *a priori*, découle la conséquence que le nombre $4n + 1$ est la somme de trois carrés.

Remarque. — On déduit aussi de (4)

$$2n + 1 = 2(a^2 + b^2 + c^2) - 2a + 1,$$

ou

$$2n + 1 = (a - 1)^2 + a^2 + (b + c)^2 + (b - c)^2.$$

On voit par là que *tout nombre impair est la somme de quatre carrés dont deux sont consécutifs*, conformément à l'énoncé de la question 1061 des *Nouvelles Annales*, proposée par M. Lionnet (2e série, t. XI, p. 96).

En outre, la valeur de n fournie par les relations posées étant

$$n = (a^2 - a) + b^2 + c^2,$$

il en résulte d'abord que *tout nombre entier est la somme de deux carrés et du double d'un nombre triangulaire*. Puis, si n est un nombre pair $2n'$, on obtient

$$n' = \frac{a^2 - a}{2} + \left(\frac{b + c}{2}\right)^2 + \left(\frac{b - c}{2}\right)^2,$$

$\frac{b + c}{2}$ et $\frac{b - c}{2}$ étant entiers (puisque, en ce cas, b et c sont nécessairement tous les deux pairs ou tous les deux impairs). Ce résultat fait reconnaître que *tout nombre entier est la somme de deux carrés et d'un nombre triangulaire*, et fournit ainsi la solution de la question 1060 proposée par M. Lionnet.

Corollaires. — 1° *Tout nombre entier de la forme* $(2n + 1)2^{2m}$ *est la somme de quatre carrés dont les racines ont une somme algébrique égale à* 2^m;

2° *Tout nombre pair de la forme* $(2n + 1)2^{2m+1}$ *est la somme de quatre carrés dont les racines ont une somme algébrique égale à zéro;*

3° *Tout nombre pair de la forme* $(2n + 1)2^{2m+1}$ *est la somme de quatre carrés dont les racines ont une somme algébrique égale à* 2^{m+1}.

Faisant $m = 0$, on a les trois théorèmes qui viennent d'être démontrés.

Lemme II. — *Tout nombre double d'un impair est la somme de quatre carrés dont l'un peut être choisi arbitrairement parmi les carrés inférieurs à ce nombre.*

C'est une conséquence du lemme I.

Soit $4n + 2$ le nombre considéré, et désignons par k^2 un carré moindre que ce nombre. Si k est pair, le nombre $4n + 2 - k^2$ est de la forme $4p + 2$, et se décompose en trois carrés. On satisfait donc à l'équation

$$4n + 2 - k^2 = a^2 + b^2 + c^2$$

en nombres entiers a, b, c, et l'on a ainsi

$$(5) \qquad 4n + 2 = a^2 + b^2 + c^2 + k^2,$$

où k^2 peut être l'un quelconque des carrés pairs qui précèdent le nombre $4n + 2$, et où il est bon d'observer que a, b, c représentent nécessairement deux nombres impairs et un pair.

Si k est impair, le nombre $4n + 2 - k^2$ est de la forme $4p + 1$, et se décompose en trois carrés. Une équation telle que (5) est donc possible en nombres entiers a, b, c, quel que soit le carré impair $k^2 < 4n + 2$. En ce cas, a, b, c ne peuvent être que deux pairs et un impair.

Théorème IV. — *Tout nombre double d'un impair est la somme de quatre carrés qui peuvent être déterminés de manière que la somme algébrique de leurs racines égale tel nombre que l'on voudra de la suite*

$$0, \ 2, \ 4, \ 6, \ldots, \quad 2\mu - 2, \quad 2\mu,$$

μ^2 étant le plus grand carré inférieur au nombre proposé.

Cette proposition, dont les théorèmes II et III sont des cas particuliers, se démontre comme il suit :

Soient $4n + 2$ le nombre proposé, et k^2 un carré inférieur à ce nombre.

D'après le lemme II, une équation telle que (5), où n et k sont fixés d'avance, admet toujours une solution en nombres entiers a, b, c.

Nous pouvons remplacer cette équation par la suivante :

(6) $$4n + 2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2;$$

en donnant à α, β, γ, δ les valeurs

$$\alpha = \frac{a + b + c + k}{2},$$

$$\beta = \frac{-a + b - c + k}{2},$$

$$\gamma = \frac{-a - b + c + k}{2},$$

$$\delta = \frac{a - b - c + k}{2};$$

car on aura, par identité,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = a^2 + b^2 + c^2 + k^2.$$

Si k est pair, a, b, c représentent deux nombres impairs et un pair, ainsi qu'on l'a observé plus haut, et les nombres α, β, γ, δ sont entiers.

Si k est impair, a, b, c sont deux nombres pairs et un impair, et α, β, γ, δ sont encore entiers.

On a d'ailleurs

(7) $$\alpha + \beta + \gamma + \delta = 2k.$$

Ces résultats (6) et (7), où k est la racine de l'un quelconque des carrés qui se trouvent au-dessous du nombre proposé $4n + 2$, établissent le théorème énoncé.

Corollaire. — *Tout nombre impair est la somme de quatre carrés qui peuvent être déterminés de manière que les racines de deux d'entre eux aient pour différence tel nombre que l'on voudra de la suite*

$$0,\ 1,\ 2,\ 3,\ 4,\ldots,\ \mu - 1,\ \mu,$$

μ^2 étant le plus grand carré inférieur au double du nombre proposé.

Par le théorème IV, l'équation

$$(6) \qquad 4n + 2 = \alpha^2 + \beta^2 + \gamma^2 + \delta^2$$

est résoluble en nombres entiers α, β, γ, δ (deux pairs, α, γ; deux impairs, β, δ), qui satisfont à la condition

$$\alpha + \beta + \gamma + \delta = 2k,$$

k étant la racine d'un carré arbitraire, inférieur à $4n + 2$.

En posant

$$A = \frac{\alpha - \gamma}{2}, \quad B = \frac{\beta - \delta}{2}, \quad C = \frac{-\beta - \delta}{2}, \quad D = \frac{\alpha + \gamma}{2},$$

d'où

$$D - C = \frac{\alpha + \beta + \gamma + \delta}{2} = k,$$

l'équation (6) donne

$$2n + 1 = A^2 + B^2 + C^2 + D^2,$$

c'est-à-dire

$$2n + 1 = A^2 + B^2 + C^2 + (C + K)^2;$$

ce qui prouve la proposition.

Dans le cas de $k = 0$, l'impair $2n + 1$ se trouve décomposé en quatre carrés dont deux sont égaux. Pour $k = 1$, on a la décomposition considérée dans la question 1061 déjà citée.

Théorème V. — *Tout nombre impair est la somme de quatre carrés qui peuvent être déterminés de manière que la somme algébrique de leurs racines égale tel nombre que l'on voudra de la suite*

$$1, 3, 5, 7, \ldots, 2\mu - 1, \quad 2\mu + 1,$$

$(2\mu + 1)^2$ étant le plus grand carré impair au-dessous du quadruple du nombre proposé.

Le mode de démonstration employé pour le théorème I s'applique comme il suit à la proposition généralisée qu'on vient d'énoncer :

Soient $2n+1$ le nombre proposé, et k^2 un carré impair compris entre zéro et $4(2n+1)$.

Le nombre $8n+4-k^2$, étant de la forme $8p+3$, se décompose en trois carrés impairs que nous représenterons par $(2a-k)^2$, $(2b-k)^2$, $(2c-k)^2$; en sorte que l'équation

$$(8)\quad 8n+4-k^2=(2a-k)^2+(2b-k)^2+(2c-k)^2,$$

dans laquelle n et k sont fixés d'avance, subsistera pour des valeurs entières de a, b, c.

Cette équation donne

$$2n+1=\left(\frac{2a-k}{2}\right)^2+\left(\frac{2b-k}{2}\right)^2+\left(\frac{2c-k}{2}\right)^2+\left(\frac{k}{2}\right)^2,$$

et nous fournit ainsi une décomposition du nombre proposé en quatre carrés fractionnaires.

Mais cette relation est identiquement équivalente à l'une quelconque des suivantes :

$$(9)\qquad 2n+1=\alpha^2+\beta^2+\gamma^2+\delta^2,$$

$$(10)\qquad 2n+1=\alpha'^2+\beta'^2+\gamma'^2+\delta'^2,$$

où l'on a posé, pour abréger,

$$\alpha=\frac{a+b+c-k}{2},$$

$$\beta=\frac{-a+b-c+k}{2},$$

$$\gamma=\frac{-a-b+c+k}{2},$$

$$\delta=\frac{a-b-c+k}{2},$$

et

$$\alpha' = \frac{a - b + c}{2},$$

$$\beta' = \frac{a + b - c}{2},$$

$$\gamma' = \frac{-a + b + c}{2},$$

$$\delta' = \frac{-a - b - c + 2k}{2},$$

et où l'on a

$$\alpha + \beta + \gamma + \delta = k,$$

$$\alpha' + \beta' + \gamma' + \delta' = k.$$

Maintenant, si $a + b + c$ est un nombre impair, α, β, γ, δ sont entiers, et la décomposition (9) vérifie le théorème. Si $a + b + c$ est un nombre pair, α', β', γ', δ' sont entiers, et le théorème est vérifié par la décomposition (10).

Note. — La formule (8) montre que *tout nombre quadruple d'un impair est la somme de quatre carrés impairs, dont l'un peut être choisi arbitrairement parmi ceux qui sont au-dessous du nombre proposé.*

On a vu plus haut (lemme II) une proposition analogue, touchant les nombres doubles d'un impair.

A ces propositions, il est bon d'ajouter les deux suivantes, qui se rapportent à la décomposition des nombres impairs :

Tout nombre impair de la forme $4n + 1$ est la somme de quatre carrés dont l'un peut être choisi arbitrairement parmi les carrés pairs inférieurs à ce nombre.

Tout nombre impair de la forme $4n + 3$ est la somme de quatre carrés dont l'un peut être choisi arbitrairement parmi les carrés impairs inférieurs à ce nombre.

En effet, l'entier positif $4n + 1 - 4h^2$ est de la forme $4p + 1$, et se décompose en trois carrés (dont deux pairs et un impair), et l'entier positif $4n + 3 - (2h' + 1)^2$ est de la forme $4p + 2$, et se décompose de même en trois carrés (dont deux impairs et un pair). De là résultent deux équations, telles que

$$4n + 1 = 4a^2 + 4b^2 + (2c + 1)^2 + 4h^2,$$
$$4n + 3 = 4a'^2 + (2b' + 1)^2 + (2c' + 1)^2 + (2h' + 1)^2,$$

résolubles en nombres entiers a, b, c et a', b', c' respectivement, n, h et h' étant fixés d'avance.