NOUVELLES ANNALES DE MATHÉMATIQUES

S. RÉALIS

Développements sur quelques théorèmes d'arithmétique

Nouvelles annales de mathématiques 2^e série, tome 18 (1879), p. 500-509

<http://www.numdam.org/item?id=NAM_1879_2_18__500_0>

DÉVELOPPEMENTS SUR QUELQUES THÉORÈMES D'ARITHMÉTIQUE;

PAR M. S. REALIS.

THÉORÈME I. — *Tout nombre* N, *premier et de la forme* $4p+1$, *est la somme de deux carrés entiers.*

Scolie I. — Faisant

$$x=\alpha^2+\beta^2-\gamma^2,$$
$$y=(\gamma-\alpha)^2+(\gamma-\beta)^2-\gamma^2,$$

et assignant à α, β, γ des valeurs entières convenables, le nombre N peut toujours être représenté par l'expression x^2+y^2, préalablement débarrassée de tout facteur carré commun à x^2 et y^2.

Ce complément remarquable du théorème énoncé est une conséquence de la résolution générale, en nombres entiers, de l'équation indéterminée

$$x^2+y^2=u^2+v^2,$$

dont il est question dans le scolie II.

Exemples :

$$\alpha=3,\quad \beta=4,\quad \gamma=1;\quad N=5;$$
$$(9+16-1)^2+(4+9-1)^2=12^2(2^2+1^2)=12^2.5;$$

$$\alpha=5,\quad \beta=6,\quad \gamma=1;\quad N=13;$$
$$(25+36-1)^2+(16+25-1)^2=20^2(3^2+2^2)=20^2.13;$$

$$\alpha=2,\quad \beta=5,\quad \gamma=-3;\quad N=17;$$
$$(4+25-9)^2+(25+64-9)^2=20^2(1^2+4^2)=20^2.17;$$

$$\alpha = 10, \quad \beta = 7, \quad \gamma = 3; \quad N = 29;$$
$$(100 + 49 - 9)^2 + (49 + 16 - 9)^2 = 28^2(5^2 + 2^2) = 28^2 . 29;$$

$$\alpha = 12, \quad \beta = 7, \quad \gamma = 5; \quad N = 37;$$
$$(144 + 49 - 25)^2 + (49 + 4 - 25)^2 = 28^2(6^2 + 1^2) = 28^2 . 37;$$

. . . . . .

Remarques. — 1° Mettant les valeurs de x et y sous la forme

$$x = \alpha^2 + \beta^2 - (-\gamma)^2,$$
$$y = (\gamma - \alpha)^2 + (\gamma - \beta)^2 - (-\gamma)^2,$$

et prenant la somme algébrique des racines des six carrés qui figurent dans ces expressions, on reconnaît que cette somme est égale à zéro. Cette particularité curieuse, et digne d'être signalée, peut être rapprochée de certaines propriétés analogues, relatives aux quatre carrés qui concourent à la formation d'un nombre entier quelconque, et pour lesquelles nous renvoyons à un article inséré aux *Nouvelles Annales,* 2e série, t. XII, p. 212.

2° La décomposition qui vient d'être indiquée n'est pas une propriété exclusive des nombres premiers; d'après le scolie II qui va suivre, elle a lieu, d'une manière générale, pour tout nombre N qui est la somme de deux carrés premiers entre eux; c'est-à-dire qu'elle a lieu pour tout nombre impair dont aucun diviseur n'est de la forme $4p - 1$, et pour son double. Mais, le cas des nombres premiers étant le plus intéressant à considérer, il nous a paru opportun de l'énoncer d'abord à part, en le rattachant à l'un des plus importants théorèmes de Fermat.

Exemples :

$$\alpha = 3, \quad \beta = 1, \quad \gamma = 1; \quad N = 10;$$
$$(9 + 1 - 1)^2 + (4 + 0 - 1)^2 = 3^2(3^2 + 1^2) = 3^2 . 10;$$

$$\alpha = 8, \quad \beta = 7, \quad \gamma = 1; \quad N = 25;$$
$$(64 + 49 - 1)^2 + (49 + 36 - 1)^2 = 28^2(4^2 + 3^2) = 28^2 . 25;$$

$$\alpha = 5, \quad \beta = 3, \quad \gamma = 2; \quad N = 26;$$
$$(25 + 9 - 4)^2 + (9 + 1 - 4)^2 = 6^2(5^2 + 1^2) = 6^2 . 26;$$

$$\alpha = 4, \quad \beta = 3, \quad \gamma = -1; \quad N = 34;$$
$$(16 + 9 - 1)^2 + (25 + 16 - 1)^2 = 8^2(3^2 + 5^2) = 8^2 . 34;$$

$$\alpha = 4, \quad \beta = 1, \quad \gamma = -3; \quad N = 50;$$
$$(16 + 1 - 9)^2 + (49 + 16 - 9)^2 = 8^2(1^2 + 7^2) = 8^2 . 50;$$

$$\alpha = 0, \quad \beta = 9, \quad \gamma = 7; \quad N = 65;$$
$$(0 + 81 - 49)^2 + (49 + 4 - 49)^2 = 4^2(8^2 + 1^2) = 4^2 . 65;$$

. . . . . .

Ajoutons, comme renseignement sur lequel nous n'insisterons pas ici, que, une fois la décomposition en deux carrés effectuée pour un nombre donné, la détermination des entiers α, β, γ et, par suite, du facteur commun à x^2 et y^2, s'en déduit par un procédé direct.

Scolie II. — On a, par identité,

$$(\alpha^2 + \beta^2 - \gamma^2)^2 + [(\gamma - \alpha)^2 + (\gamma - \beta)^2 - \gamma^2]^2$$
$$= [\alpha^2 + (\alpha - \gamma)^2 - (\alpha - \beta)^2]^2 + [\beta^2 + (\beta - \gamma)^2 - (\beta - \alpha)^2]^2.$$

Cette formule est susceptible d'applications importantes. D'abord, elle peut être souvent utile, lorsqu'il s'agit de constater qu'un nombre impair, qui se présente sous la forme indiquée au premier membre (dégagée de ses facteurs carrés), admet des diviseurs. On

sait, en effet, qu'un tel nombre ne saurait être premier, s'il est décomposable de plus d'une manière en deux carrés.

Par exemple, pour $\alpha = 35$, $\beta = 24$, $\gamma = -25$, les deux membres de la formule sont, respectivement,

$$(1225 + 576 - 625)^2 + (3600 + 2401 - 625)^2 = 168^2(7^2 + 32^2) = 168^2 . 1073,$$

$$(1225 + 3600 - 121)^2 + (576 + 2401 - 121)^2 = 168^2(28^2 + 17^2) = 168^2 . 1073,$$

et, comme ils présentent deux décompositions différentes, on en conclut que le nombre 1073 n'est pas premier. Cependant, si l'on avait pris $\alpha = 14$, $\beta = 39$, $\gamma = -25$, la même formule n'aurait donné que le résultat

$$156^2(7^2 + 32^2) = 156^2 . 1073,$$

ce qui ne nous apprend rien sur la nature du nombre 1073, en tant que premier ou composé.

Pour

$$\alpha = 1, \quad \beta = 2^{2m+1} + 2^{m+1}, \quad \gamma = 2^{2m+1} - 1,$$

il vient, après suppression des facteurs communs, l'égalité

$$(2^{2m+1})^2 + 1^2 = (2^{2m+1} - 1)^2 + (2^{m+1})^2,$$

et l'on en déduit que le nombre $2^{4m+2} + 1$, où m est un entier plus grand que zéro, n'est jamais premier. En effet, ce nombre (à part qu'il est évidemment divisible par 5) est égal au produit

$$(2^{2m+1} + 2^{m+1} + 1)(2^{2m+1} - 2^{m+1} + 1),$$

ainsi que la remarque en a été faite dans la *Nouvelle Correspondance mathématique* (t. IV, p. 86 et 98). Complétons ce résultat, en inscrivant l'égalité évidente

$$2^{2m+1} = 2^{m+1} + 1 = (2^m)^2 + (2^m \pm 1)^2,$$

par laquelle chaque facteur du produit considéré se réduit à une somme de deux carrés, ainsi que cela doit être.

Mais ce qui rend l'identité ci-dessus surtout importante, c'est qu'elle résout complètement, et en employant trois seules variables, l'équation indéterminée

$$x^2 + y^2 = u^2 + v^2,$$

traitée jadis par Le Besgue à l'aide de principes entièrement différents (voir les *Nouvelles Annales*, 1re série, t. VII, p. 37 ; *voir* aussi, pour la solution usuelle, le *Bulletin de Bibliographie*, etc., de Terquem, t. III, p. 86). Nous nous bornons ici à énoncer cette propriété, que l'on peut démontrer en toute rigueur, et dont la proposition qui fait l'objet du scolie I est une conséquence directe. On verra plus bas, dans les observations qui suivent le théorème III, que l'identité considérée, et l'équation qu'elle sert à résoudre, sont des cas particuliers de relations plus générales.

THÉORÈME II. — *Tout nombre* N *appartenant à l'une des formes*

$$4p + 1,\ 4p + 2,\ 8p + 3,$$

et n'ayant pas de facteurs carrés, est la somme de trois carrés premiers entre eux.

Scolie. — Faisant

$$x = \alpha^2 + \beta^2 + \gamma^2 - \delta^2 - \varepsilon^2,$$
$$y = (\delta - \alpha)^2 + (\delta - \beta)^2 + (\delta - \gamma)^2 - (\delta - \varepsilon)^2 - \delta^2,$$
$$z = (\varepsilon - \alpha)^2 + (\varepsilon - \beta)^2 + (\varepsilon - \gamma)^2 - (\varepsilon - \delta)^2 - \varepsilon^2,$$

et déterminant convenablement les entiers α, β, γ, δ, ε, le nombre N peut toujours être représenté par l'expression $x^2 + y^2 + z^2$, préalablement débarrassée des facteurs communs à x^2, y^2, z^2.

Ce complément du théorème cité résulte de la résolution générale, que nous allons exposer, d'une équation indéterminée à six inconnues.

Il est bien entendu que l'un des trois carrés considérés peut être nécessairement nul, ainsi que cela a lieu, par exemple, pour les nombres 5, 10, 13, 37.

Exemples :

$$\alpha = 3,\quad \beta = 1,\quad \gamma = 4,\quad \delta = 1,\quad \varepsilon = 1;\quad N = 6;$$
$$(9 + 1 + 16 - 1 - 1)^2 + (4 + 0 + 9 - 0 - 1)^2 + (4 + 0 + 9 - 0 - 1)^2 = 12^2(2^2 + 1^2 + 1^2) = 12^2.6;$$

$$\alpha = 3,\quad \beta = 4,\quad \gamma = 6,\quad \delta = 2,\quad \varepsilon = 3;\quad N = 10;$$
$$(9 + 16 + 36 - 4 - 9)^2 + (1 + 4 + 16 - 1 - 4)^2 + (0 + 1 + 9 - 1 - 9)^2 = 16^2(3^2 + 1^2 + 0) = 16^2.10;$$

$$\alpha = 0,\quad \beta = 2,\quad \gamma = 1,\quad \delta = 1,\quad \varepsilon = 1;\quad N = 11;$$
$$(0 + 4 + 1 - 1 - 1)^2 + (1 + 1 + 0 - 0 - 1)^2 + (1 + 1 + 0 - 0 - 1)^2 = 3^2 + 1^2 + 1^2 = 11;$$

$$\alpha = 0,\quad \beta = 5,\quad \gamma = 3,\quad \delta = 1,\quad \varepsilon = 3;\quad N = 13;$$
$$(0 + 25 + 9 - 1 - 9)^2 + (1 + 16 + 4 - 4 - 1)^2 + (9 + 4 + 0 - 4 - 9)^2 = 8^2(3^2 + 2^2 + 0) = 8^2.13;$$

$$\alpha = 6,\quad \beta = 1,\quad \gamma = 2,\quad \delta = 1,\quad \varepsilon = 2;\quad N = 14;$$
$$(36 + 1 + 4 - 1 - 4)^2 + (25 + 0 + 1 - 1 - 1)^2 + (16 + 1 + 0 - 1 - 4)^2 = 12^2(3^2 + 2^2 + 1^2) = 12^2.14;$$

.....

Remarque. — Plus généralement : tout nombre N, qui est la somme de trois carrés entiers, peut être représenté, en fonction des entiers α, β, γ, δ, ε, par l'expression ci-dessus, dont les termes ont été préalablement dégagés de tout facteur commun, étranger à la composition de N.

Cette proposition remarquable est une conséquence de l'identité

$$x^2 + y^2 + z^2 = t^2 + u^2 + v^2,$$

dans laquelle x, y, z sont tels qu'il a été dit, et t, u, v sont exprimés par

$$t = \alpha^2 + (\alpha - \delta)^2 + (\alpha - \varepsilon)^2 - (\alpha - \beta)^2 - (\alpha - \gamma)^2,$$
$$u = \beta^2 + (\beta - \delta)^2 + (\beta - \varepsilon)^2 - (\beta - \alpha)^2 - (\beta - \gamma)^2,$$
$$v = \gamma^2 + (\gamma - \delta)^2 + (\gamma - \varepsilon)^2 - (\gamma - \alpha)^2 - (\gamma - \beta)^2.$$

On peut démontrer rigoureusement, en effet, que cette identité renferme toutes les solutions entières de l'équation indéterminée qu'elle établit entre les variables t, u, v, x, y, z.

THÉORÈME III. — *Tout nombre entier est la somme de quatre carrés entiers* (ou d'un moindre nombre).

Scolie. — Toutes les solutions entières, distinctes, de l'équation indéterminée à huit inconnues

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = u_1^2 + u_2^2 + u_3^2 + u_4^2,$$

s'obtiennent au moyen des formules

$$x_1 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 - \beta_1^2 - \beta_2^2 - \beta_3^2,$$
$$x_2 = (\beta_1 - \alpha_1)^2 + (\beta_1 - \alpha_2)^2 + (\beta_1 - \alpha_3)^2 + (\beta_1 - \alpha_4)^2 - (\beta_1 - \beta_2)^2 - (\beta_1 - \beta_3)^2 - \beta_1^2,$$
$$x_3 = (\beta_2 - \alpha_1)^2 + (\beta_2 - \alpha_2)^2 + (\beta_2 - \alpha_3)^2 + (\beta_2 - \alpha_4)^2 - (\beta_2 - \beta_1)^2 - (\beta_2 - \beta_3)^2 - \beta_2^2,$$
$$x_4 = (\beta_3 - \alpha_1)^2 + (\beta_3 - \alpha_2)^2 + (\beta_3 - \alpha_3)^2 + (\beta_3 - \alpha_4)^2 - (\beta_3 - \beta_1)^2 - (\beta_3 - \beta_2)^2 - \beta_3^2,$$
$$u_1 = \alpha_1^2 + (\alpha_1 - \beta_1)^2 + (\alpha_1 - \beta_2)^2 + (\alpha_1 - \beta_3)^2 - (\alpha_1 - \alpha_2)^2 - (\alpha_1 - \alpha_3)^2 - (\alpha_1 - \alpha_4)^2,$$
$$u_2 = \alpha_2^2 + (\alpha_2 - \beta_1)^2 + (\alpha_2 - \beta_2)^2 + (\alpha_2 - \beta_3)^2 - (\alpha_2 - \alpha_1)^2 - (\alpha_2 - \alpha_3)^2 - (\alpha_2 - \alpha_4)^2,$$
$$u_3 = \alpha_3^2 + (\alpha_3 - \beta_1)^2 + (\alpha_3 - \beta_2)^2 + (\alpha_3 - \beta_3)^2 - (\alpha_3 - \alpha_1)^2 - (\alpha_3 - \alpha_2)^2 - (\alpha_3 - \alpha_4)^2,$$
$$u_4 = \alpha_4^2 + (\alpha_4 - \beta_1)^2 + (\alpha_4 - \beta_2)^2 + (\alpha_4 - \beta_3)^2 - (\alpha_4 - \alpha_1)^2 - (\alpha_4 - \alpha_2)^2 - (\alpha_4 - \alpha_3)^2,$$

en y attribuant aux variables α_k, β_k des valeurs convenables, et en supprimant les facteurs communs aux valeurs des x et des u.

Cette proposition comprend les énoncés relatifs aux équations mentionnées dans les scolies précédents, et n'est elle-même qu'un cas particulier d'une proposition plus générale. Combinée avec le théorème III, elle entraîne ce corollaire que, les x étant de la forme indiquée, tout nombre entier N peut être représenté par l'expression $x_1^2 + x_2^2 + x_3^2 + x_4^2$, préalablement débarrassée des facteurs carrés communs à ses quatre termes, et étrangers à la composition de N.

Les formules proposées vérifient l'équation ci-dessus par identité : sur cela il ne peut y avoir de doute ; elles donnent donc une infinité de solutions entières. Ce que nous n'avons pas encore démontré, c'est que tous les cas particuliers sont compris dans l'identité en question. Mais les preuves à l'appui de la généralité absolue de notre solution, et les moyens de résoudre la question inverse, c'est-à-dire de déterminer les α et les β d'après les valeurs des x et des u supposées connues, ne seront pas développés ici. Ces explications, rattachées à des questions plus générales, feront partie d'un travail spécial, où nous nous réservons d'exposer quelques considérations nouvelles sur la résolution des équations indéterminées.

Note. — On voit assez, par ce qui précède, quelles sont les formules qui vérifient par identité l'équation indéterminée à $2m$ inconnues

$$x_1^2 + x_2^2 + \ldots + x_m^2 = u_1^2 + u_2^2 + \ldots + u_m^2,$$

et comment elles se prêtent à préciser la forme des m carrés dans lesquels un nombre donné peut être décom-

posé. Mais les décompositions des entiers en deux, trois et quatre carrés, étant celles dont on a le plus souvent à s'occuper, et les nouvelles formules offrant surtout de l'intérêt par leur association avec les théorèmes concernant la transformation des formes linéaires en formes quadratiques, nous ne nous arrêterons pas ici sur la généralisation facile dont nous parlons.

Il y a cependant un cas particulier qui a une importance propre, et que nous ne devons pas omettre de signaler : c'est celui qui se rapporte aux nombres de la forme $X^2 + nY^2$.

L'identité

$$x^2 + ny^2 = u^2 + nv^2,$$

où l'on a fait, pour abréger,

$$\begin{aligned} x &= \alpha^2 + n\beta^2 - n\gamma^2, \\ y &= (\gamma - \alpha)^2 + n(\gamma - \beta)^2 - \gamma^2, \\ u &= \alpha^2 + n(\alpha - \gamma)^2 - n(\alpha - \beta)^2, \\ v &= \beta^2 + n(\beta - \gamma)^2 - (\alpha - \beta)^2, \end{aligned}$$

est un cas particulier de la relation générale dont on a fait mention. Elle renferme la totalité des solutions entières de l'équation indéterminée qu'elle établit entre les variables u, v, x, y, et l'on en peut déduire des conséquences importantes pour l'analyse numérique.

Cette identité s'emploie avec avantage, entre autres applications, pour mettre en évidence que certains nombres, qui se présentent sous la forme de son premier membre, sont susceptibles d'être mis d'une manière différente sous la même forme, et par conséquent ne sont pas premiers. Aucun nombre premier, en effet, ne saurait être compris plus d'une fois dans la forme $X^2 + nY^2$, si n est positif.

Prenant, par exemple, dans le cas de $n = 3$,

$$\alpha = 3.2^{2m-1}, \quad \beta = 3.2^{2m-1} - 1, \quad \gamma = 2^{2m} - 2^m - 1,$$

on arrive, après suppression des facteurs communs, au résultat

$$(2^{2m} - 1)^2 + 3(2^m)^2 = (2^{2m-1} + 1)^2 + 3(2^{2m-1})^2,$$

et il s'ensuit que le nombre $2^{4m} + 2^{2m} + 1$, où m est un entier positif, n'est jamais premier. On a effectivement

$$\begin{aligned} 2^{4m} + 2^{2m} + 1 &= (2^{2m} + 2^m + 1)(2^{2m} - 2^m + 1) \\ &= [(2^{m-1} + 1)^2 + 3(2^{m-1})^2][(2^{m-1} - 1)^2 + 3(2^{m-1})^2], \end{aligned}$$

à quoi l'on peut ajouter que ce nombre est toujours divisible par 3.