NOUVELLES ANNALES DE MATHÉMATIQUES

E. DE JONQUIÈRES

Étude sur les décompositions en sommes de deux carrés, du carré d'un nombre entier composé de facteurs premiers de la forme $4n+1$, et de ce nombre lui-même. Formules et application à la résolution complète, en nombres entiers, des équations indéterminées, simultanées, $y = x^2 + (x+1)$ et $y^2 = z^2 + (z+1)^2$

Nouvelles annales de mathématiques 2e série, tome 17 (1878), p. 241-247

<http://www.numdam.org/item?id=NAM_1878_2_17__241_0>

ÉTUDE SUR LES DÉCOMPOSITIONS EN SOMMES DE DEUX CARRÉS, DU CARRÉ D'UN NOMBRE ENTIER COMPOSÉ DE FACTEURS PREMIERS DE LA FORME $4n+1$, ET DE CE NOMBRE LUI-MÊME.

FORMULES ET APPLICATION A LA RÉSOLUTION COMPLÈTE, EN NOMBRES ENTIERS, DES ÉQUATIONS INDÉTERMINÉES, SIMULTANÉES, $y=x^2+(x+1)^2$ ET $y^2=z^2+(z+1)^2$;

PAR M. E. DE JONQUIÈRES.

I. Soient $f_1, f_2, f_3, \ldots, f_n$ les n facteurs du nombre N, que nous supposerons d'abord à la première puissance et, par suite, tous différents entre eux.

Chacun d'eux étant un nombre premier, de la forme $4k+1$, se décompose d'une seule manière en une somme de deux carrés premiers entre eux. On a donc

$$f_1 = a_1^2 + b_1^2,\quad f^2 = a_2^2 + b_2^2,\quad \ldots,\quad f_n = a_n^2 + b_n^2,$$

et nous supposerons $a_i > b_i$; car les deux nombres a_i, b_i sont inégaux, l'un pair et l'autre impair.

Le nombre I de toutes les décompositions possibles du nombre N en une somme de deux carrés est, dans le cas actuel, donné par la formule $\mathrm{I} = \frac{1}{2}2^n = 2^{n-1}$, et le nombre I' des décompositions de N^2 par la formule

$$\mathrm{I}' = \tfrac{1}{2}(3^n - 1).$$

(*Voir* GAUSS, *Recherches arithmétiques*, p. 157. — LEGENDRE, *Théorie des nombres*, 2e édition, p. 268, et GENOCCHI, *Nouvelles Annales de Mathématiques*, t. XIII, 1re série, p. 165.)

Ces $\dfrac{3^n-1}{2}$ décompositions de N^2 se subdivisent en n

espèces distinctes, que nous désignerons par les signes $(E_1), (E_2), \ldots, (E_n)$.

Celles de la première espèce (E_1) sont au nombre de n, et dans chacune d'elles les deux nombres composants admettent $n - 1$ facteurs communs avec N.

Celles de la deuxième espèce (E_2) sont au nombre de $2\dfrac{n(n-1)}{1.2}$, et dans chacune d'elles les deux nombres composants admettent $n - 2$ facteurs communs avec N.

Celles de la troisième espèce (E_3) sont au nombre de $2^2\dfrac{n(n-1)(n-2)}{1.2.3}$, et chacun des deux nombres composants y admet $n - 3$ facteurs communs avec N.

Et ainsi de suite, jusqu'à la dernière espèce (E_n), qui comprend 2^{n-1} solutions (nombre précisément égal à celui des décompositions de N), dans aucune desquelles l'un ou l'autre des nombres composants n'a de facteur commun avec N.

Le nombre total de ces décompositions, dans les n espèces réunies, est donc

$$\begin{aligned}I' = n + 2\frac{n(n-1)}{1.2} + 2^2\frac{n(n-1)(n-2)}{1.2.3} + \ldots \\ + 2^{n-2}n + 2^{n-1} = \frac{3^n - 1}{2}\end{aligned}$$

Les propositions précédentes, que M. Volpicelli a simplement énoncées, à peu près dans les mêmes termes, dans le tome IX (1^{re} série) des *Nouvelles Annales*, année 1850, sont intuitives. Il est évident, en effet, que parmi les I' décompositions de N^2 doivent se trouver celles de $f_1^2\left(\dfrac{N}{f_1}\right)^2$ et de ses analogues, formant une première espèce, dans laquelle f_1 est facteur commun des deux nombres x et y dont la somme des carrés est égale à N^2. On doit y trouver pareillement celles de $f_1^2 f_2^2\left(\frac{N}{f_1 f_2}\right)^2$, et de ses analogues, dans chacune desquelles le second facteur $\frac{N}{f_1 f_2}$ est le seul décomposé, et ainsi de suite.

Quant aux *formes* de ces décompositions, M. Volpicelli se borne à faire connaître la plus simple de toutes, celle de l'espèce (E_1), qu'il écrit ainsi :

$$x = (a_i^2 - b_i^2)\frac{N}{f_i}, \quad y = 2a_i b_i \frac{N}{f_i} \quad \text{et} \quad x^2 + y^2 = N^2,$$

l'indice i devant recevoir successivement toutes les valeurs comprises depuis 1 jusqu'à n. Cette forme bien connue est celle qui se présente pour la décomposition du carré d'un nombre premier de la forme $4n+1$ en une somme de deux carrés.

J'ignore si M. Volpicelli a fait connaître plus tard, dans quelque autre recueil mathématique, les formules relatives aux $n-1$ autres espèces; j'ajoute même que je ne le crois pas. Quoi qu'il en soit, ayant été conduit tout dernièrement à les découvrir, à l'occasion du problème d'Analyse indéterminée cité dans le titre de cette Étude, je vais les donner ici, dans la pensée que cette communication ne fera double emploi avec aucune autre publiée antérieurement et à mon insu sur le même sujet.

II. Les valeurs des nombres composants x, y dans les décompositions de la deuxième espèce (E_2) sont

$$x = \frac{N}{f_i f_{i'}}[(a_i^2 - b_i^2)(a_{i'}^2 - b_{i'}^2) \pm 4a_i b_i . a_{i'} b_{i'}],$$

$$y = \frac{N}{f_i f_{i'}}[2a_i b_i (a_{i'}^2 - b_{i'}^2) \mp 2a_{i'} b_{i'} (a_i^2 - b_i^2)],$$

les signes supérieurs devant être pris ensemble et les signes inférieurs ensemble, et i, i' prenant toutes les valeurs possibles, mais différentes entre elles, depuis 1 jusqu'à n.

On peut donner à ce résultat un autre énoncé qui, dans sa généralité, convient, comme je vais le dire, aux décompositions des autres espèces, et permet d'en abréger uniformément la définition. Nous dirons donc que x et y ont, respectivement, pour valeurs les produits du facteur $\frac{N}{f_i f_{i'}}$ multiplié successivement par toutes les décompositions de la *dernière* (ici la seconde) espèce, dont est susceptible le carré d'un nombre composé des deux facteurs simples et premiers f_i, $f_{i'}$, qui ne font point partie du facteur $\frac{N}{f_i f_{i'}}$ commun à x et à y.

D'après cela, le nombre des décompositions de l'espèce (E_2) est égal à $2^{\frac{n(n-1)}{2}}$, car le carré d'un nombre composé de deux tels facteurs ne comporte que quatre décompositions, dont deux appartiennent à la première espèce déjà considérée et ne figurent pas parmi celles de la seconde, qui est alors la dernière espèce.

III. Les valeurs de x et de y dans la troisième espèce (E_3) ont pareillement pour valeurs respectives les produits du facteur $\frac{N}{f_i f_{i'} f_{i''}}$ multiplié successivement par toutes les décompositions de troisième ou dernière espèce des carrés des nombres composés des trois facteurs f_i, $f_{i'}$, $f_{i''}$, qui ne figurent pas dans $\frac{N}{f_i f_{i'} f_{i''}}$, de sorte que l'espèce (E_3) contient $2^2 \frac{n(n-1)(n-2)}{1.2.3}$ décompositions distinctes, ou systèmes de valeurs différentes et conjuguées de x et de y.

Et ainsi de suite, jusqu'au groupe (E_n), de telle sorte qu'un groupe (E_p), d'espèce p, contient

$$2^{p-1}\,\frac{n(n-1)(n-2)\ \ldots\ (n-p+1)}{1.2.3\ldots p},$$

décompositions ou systèmes de valeurs de x et y, c'est-à-dire autant de fois 2^{p-1} qu'il y a de combinaisons possibles des diviseurs premiers de N, pris p à p.

IV. Quant au dernier groupe (E_n), dont la forme et la composition précises sont particulièrement intéressantes, on peut dire les seules essentielles à connaître, puisqu'elles concourent exclusivement, sauf un facteur connu d'avance, à la composition des valeurs de x et de y dans les autres espèces, le facteur $\frac{N}{f_1 f_2 \ldots f_n}$ est égal à l'unité; le groupe contient en totalité 2^{n-1} décompositions distinctes, et x ni y n'ont en commun aucun des facteurs de N. Le système *type* ou *fondamental* des valeurs de x et de y dans ce groupe, c'est-à-dire celui qu'on peut écrire immédiatement, et duquel les $2^{n-1}-1$ autres systèmes de ce groupe se déduisent par de simples changements dans les signes des termes dont il se compose, est le suivant, qui dérive de la théorie des combinaisons et de la décomposition fondamentale

$$N^2 = \overline{(a^2-b^2)}^2 + \overline{2ab}^2$$

appliquée au cas $N = a^2 + b^2$.

Désignons, pour abréger, par $\Pi_k(ab)$ et $\Pi_k(a^2-b^2)$ le produit de k facteurs, tels que ab et (a^2-b^2), et par Σ la somme de tous les produits de ce genre qu'on obtient en combinant entre eux, k à k, et de toutes les manières possibles, les produits $a_i b_i$, ou les termes $(a_i^2-b_i^2)$, de telle sorte, par exemple, que le terme symbolique

$$\Sigma\,[\Pi_2(ab)\,\Pi_2(a^2-b^2)]$$

représente la somme

$$\begin{aligned}
& a_1b_1.a_2b_2(a_3^2-b_3^2)(a_4^2-b_4^2)\\
+\; & a_1b_1\,a_3b_3(a_2^2-b_2^2)(a_4^2-b_4^2)\\
+\; & a_1b_1\,a_4b_4(a_2^2-b_2^2)(a_3^2-b_3^2)\\
+\; & a_2b_2\,a_3b_3(a_1^2-b_1^2)(a_4^2-b_4^2)\\
+\; & a_2b_2\,a_4b_4(a_1^2-b_1^2)(a_3^2-b_3^2)\\
+\; & a_3b_3\,a_4b_4(a_1^2-b_1^2)(a_2^2-b_2^2).
\end{aligned}$$

D'après ces notations, les formules fondamentales qui expriment les valeurs *types* ou initiales de x et de y dans le groupe (E_n) sont

$$(1)\quad \left\{\begin{aligned}
x &= \Pi_n(a^2-b^2)\\
&\quad - 2^2\Sigma[\Pi_2(ab)\,\Pi_{n-2}(a^2-b^2)]\\
&\quad + 2^4\Sigma[\Pi_4(ab)\,.\,\Pi_{n-4}(a^2-b^2)] - \text{etc.}\;\ldots,\\
y &= 2\,\Sigma[\Pi_1(ab)\,.\,\Pi_{n-1}(a^2-b^2)]\\
&\quad - 2^3\Sigma[\Pi_3(ab)\,\Pi_{n-3}(a^2-b^2)]\\
&\quad + 2^5\Sigma[\Pi_5(ab)\,\Pi_{n-5}(a^2-b^2)] - \text{etc.}\;\ldots
\end{aligned}\right.$$

Dans ces valeurs de x et de y, les termes réunis sous un même signe sommatoire Σ ont tous le même signe, ces groupes de termes prenant alternativement le signe $+$ et le signe $-$, en commençant dans l'une et dans l'autre formule par le signe $+$.

Avant d'indiquer de quelle manière, c'est-à-dire par quelles permutations de signes, les $2^{n-1}-1$ autres systèmes de valeurs de x et de y dont se compose le groupe (E_n) se déduisent des formules types (1), faisons quelques remarques essentielles sur ces formules.

Le premier terme de la valeur de x, savoir $\Pi_n(a^2-b^2)$, est, d'après la convention établie que $a_i > b_i$, toujours positif.

Le groupe de termes qui suit, compris avec le signe — sous le premier signe Σ, se compose de $\frac{n(n-1)}{2}$ termes. Le suivant en contient sous le signe +

$$\frac{n(n-1)(n-2)(n-3)}{1.2.3.4},$$

et ainsi de suite.

Le premier groupe de la valeur de y se compose de n termes. Le suivant en contient $\frac{n(n-1)(n-2)}{1.2.3}$, et ainsi de suite d'après la même loi, de telle sorte que x contient, en totalité, 2^{n-1} termes et que y en contient le même nombre, comme cela doit être, puisque ces valeurs sont conjuguées deux à deux.

(*La suite prochainement.*)