Nouvelles annales de mathématiques

E. de Jonquières

Décomposition du carré d'un nombre N et de ce nombre lui-même en sommes quadratiques de la forme $x^2 + t \cdot y^2, t$ étant un nombre rationnel positif ou négatif ; résolution en nombres entiers du système des équations indéterminées $y = x^2 + t(x+\alpha)^2, y^2 = z^2 + t(z+\beta)^2$

Nouvelles annales de mathématiques 2e série, tome 17 (1878), p. 419-424

<http://www.numdam.org/item?id=NAM_1878_2_17__419_0>

Décomposition du carré d'un nombre N *et de ce nombre lui-même en sommes quadratiques de la forme* $x^2 + t.y^2$, *t étant un nombre rationnel positif ou négatif; résolution en nombres entiers du système des équations indéterminées*

$$y = x^2 + t(x+\alpha)^2, \quad y^2 = z^2 + t(z+\beta)^2;$$

Par M. E. de JONQUIÈRES.

1. Les formules que j'ai données dans la livraison du mois de juin dernier (t. XVII, p. 246) permettent de décomposer immédiatement, en une somme de deux carrés, le carré N^2 du produit d'un nombre quelconque de facteurs premiers qui ont cette même forme et, par un changement convenable et bien déterminé dans les signes des différents termes dont elles se composent, font connaître toutes les décompositions de même espèce du carré de ce produit.

J'ajoute que, moyennant une très-légère modification, ces formules servent pour décomposer en une somme quadratique de la forme $x^2 + t.y^2$ le carré N^2 du produit d'un nombre quelconque n de facteurs ayant tous cette même forme. Pour cela, il suffit d'y remplacer par $\sqrt{t}.b_i$ la quantité qui y est généralement désignée par b_i. Chacun des facteurs premiers de N est alors égal à une somme telle que $a_i^2 + tb_i^2$, et d'une seule manière si t est positif (*).

Cette substitution change les formules (1) dont il s'agit

(*) Legendre demontre dans la *Théorie des nombres*, 2e Partie, no 234, que *tout nombre premier qui est de la forme* $x^2 + ty^2$, *t étant un nombre positif, ne peut être qu'une seule fois de cette forme.*

en celles-ci :

$$
(1') \quad \begin{cases} x = \Pi_n(a^2 - t.b^2) - 2^2\Sigma\left[\Pi_2(a\sqrt{t}.b)\Pi_{n-2}(a^2 - t.b^2)\right] \\ \qquad\qquad + 2^4\Sigma\left[\Pi_4(a\sqrt{t}.b)\Pi_{n-4}(a^2 - t.b^2)\right] - \ldots \\ y = 2\Sigma\left[\Pi_1(a\sqrt{t}.b)\Pi_{n-1}(a^2 - t.b^2)\right] \\ \quad - 2^3\Sigma\left[\Pi_3(a\sqrt{t}.b)\Pi_{n-3}(a^2 - t.b^2)\right] + 2^5\Sigma[\ldots] - \ldots, \end{cases}
$$

dont tous les termes recevront successivement les changements de signe indiqués à la page 289 de l'article précité, si l'on veut obtenir toutes les décompositions distinctes, dans chacune desquelles les composants x et y sont premiers entre eux, et qui sont encore ici les seules intéressantes à considérer.

On remarquera que $\sqrt{t}$ ne figure dans la valeur de y que comme facteur commun de tous les termes et par conséquent disparaît, pour devenir t, lorsqu'on élève y au carré en formant la somme $x^2 + t.y^2 = N^2$.

J'ajoute enfin que toutes les décompositions de cette *espèce* dérivent une à une, et par la même loi que dans le cas primitif, de celles de même forme du nombre N lui-même et sont, comme celles-ci, au nombre de 2^{n-1}.

II. Lorsque, parmi les facteurs premiers de N, il en est qui ne sont pas décomposables en une somme quadratique de la forme donnée $x^2 + t.y^2$, il n'en faut pas conclure immédiatement, comme dans le cas de $t = 1$, que chacun de ceux-ci doive entrer avec un exposant pair dans la composition de N, pour que le nombre N soit décomposable de la façon requise. Cette condition ne subsiste que pour ceux d'entre eux qui ne sont pas des *divisions linéaires* de la formule $x^2 + t.y^2$, en conservant à cette expression le sens que lui ont donné Lagrange et Legendre dans sa *Théorie des nombres* (2^e Partie, § X à XIII, 2^e édition). Il faut donc s'assurer préalablement quels sont ceux qui sont des diviseurs linéaires, soit par un calcul direct, soit en se servant des Tables dressées dans ce but par Legendre (Tables IV, V, VI et VII), lorsque le nombre t s'y trouve compris.

On aura ainsi réduit le nombre N à la forme PQR; P étant le produit des p facteurs premiers qui ne sont ni diviseurs quadratiques, ni diviseurs linéaires de x^2+ty^2; Q exprimant le produit des q facteurs premiers de N qui sont diviseurs linéaires, mais non quadratiques; enfin R représentant le produit des r diviseurs quadratiques du nombre N.

Le carré N^2 étant égal à $P^2.Q^2.R^2$, on sait déjà que P^2 n'est pas décomposable et que les formules (1') donnent les 2^{r-1} décompositions de R^2, dans chacune desquelles les composants x et y sont premiers entre eux. Il reste à savoir décomposer Q^2.

III. Or, d'après un théorème démontré par Legendre, *loco citato*, lorsqu'un nombre est diviseur linéaire d'une forme quadratique donnée $x^2+t.y^2$, sans être en même temps diviseur quadratique de cette forme, il existe toujours un nombre entier, moindre que $2\sqrt{\frac{t}{3}}$, tel qu'il suffit de multiplier par ce nombre auxiliaire le diviseur linéaire pour rendre ce dernier diviseur quadratique. En conséquence, on multipliera chacun des q facteurs de Q par le nombre α convenable, et l'on transformera ainsi Q en un produit de la forme $(\alpha_1 q_1)(\alpha_2 q_2)(\alpha_3 q_3)\ldots = A.Q$. Comme tous les facteurs $\alpha_i q_i$ de AQ sont actuellement de la forme requise $a^2+t.b^2$, les formules (1') donneront immédiatement les 2^{q-1} décompositions, de dernière espèce à un facteur près, dont A^2Q^2 est susceptible. Parmi elles, il y en aura dont les deux nombres composants seront de la forme $A.x$, $A\sqrt{t}.1$, c'est-à-dire qui auront en commun le facteur A, produit de tous les nombres auxiliaires α_1, α_2, α_3, ...

En effet, s'il n'y en avait aucune dans ce cas, le nombre Q ne serait donc décomposable d'aucune manière en une somme quadratique de la forme $x^2 + ty^2$, ce qui ne peut être, puisqu'il a, par hypothèse, pour facteurs premiers des diviseurs linéaires de cette forme et que, d'après un théorème connu (*Théorie des nombres*, § XIII, n° 231), tout produit de deux tels diviseurs est un diviseur quadratique de la même forme. En divisant par A les deux composants de chacun de ces systèmes, on connaîtra les composants eux-mêmes de tous les systèmes de dernière espèce que comporte la décomposition de Q^2, systèmes qui sont d'ailleurs en même nombre que ceux de Q et qui en dérivent directement un à un.

IV. La décomposition de $N^2 = P^2 Q^2 R^2$ sera ainsi rendue facile, soit par de simples multiplications des nombres obtenus, si l'on ne veut pas obtenir les décompositions de la dernière espèce, soit, si l'on ne recherche que ces dernières, en appliquant directement les formules (1') à la décomposition du nombre

$$(AQR)^2 = (\alpha_1 q_1)(\alpha_2 q_2) \ldots r_1 r_2 r_3 \ldots,$$

dont tous les facteurs ont la forme quadratique $a^2 + t.b^2$, mais en ne prenant, bien entendu, parmi elles, que celles appartenant à des systèmes dont les deux composants auront A pour facteur commun, ainsi qu'on l'avait fait pour obtenir les décompositions de Q^2; soit enfin (ce qui est plus simple encore) en décomposant par les mêmes formules le carré du nombre N', obtenu en posant

$$N' = (\alpha_1 \alpha_2 q_1 q_2)(\alpha_3 \alpha_4 q_3 q_4) \ldots (\alpha_{2q+1} - q_{1q+1}) R,$$

et en opérant de même sur les résultats obtenus.

V. Voici quelques exemples de ces différents cas :

1° Soient $t = 2$, $N = 10659 = 3.11.17.19$. On a

$$3 = (1^2 + 2.1^2),\quad 11 = (3^2 + 2.1^2),$$
$$17 = (3^2 + 2.2^2),\quad 19 = (1^2 + 2.3^2),$$

et les formules $(1')$ donnent, pour la première des huit solutions de la dernière espèce,

$$\overline{10659}^2 = \overline{8159}^2 + 2.\overline{4850}^2.$$

2° Si $t = 3$, $N = 53599 = 7.13.19.31$, on a

$$7 = (2^2 + 3.1^2),\quad 13 = (1^2 + 3.2^2),$$
$$19 = (4^2 + 3.1^2),\quad 31 = (2^2 + 3.3^2),$$

et les formules $(1')$ donnent, pour la première des huit solutions de la dernière espèce,

$$\overline{53599}^2 = \overline{31273}^2 + 3.\overline{25132}^2.$$

Dans les deux exemples qui précèdent, tous les facteurs de N étaient des diviseurs quadratiques de la forme requise $x^2 + ty^2$. En voici d'autres où cette condition n'est remplie qu'en partie, ou même pas du tout, les facteurs étant alors simplement des diviseurs linéaires de la formule.

3° $t = 5$, $N = 189 = 3.7.9 = 3.7(2^2 + 5.1^2)$.

Les multiplicateurs propres à rendre quadratiques les facteurs 3 et 7, diviseurs linéaires de la forme $x^2 + 5y^2$, sont ici respectivement 2 et 2; on a ainsi

$$4N = 6.14.9 = 189 = (1^2 + 5.1^2)(3^2 + 5.1^2)(2^2 + 5.1^2),$$

et les formules $(1')$ donnent les quatre solutions de dernière espèce

$$x_1 = 4.99,\quad y_1 = 4.72;\quad x_2 = 4.149,\quad y_2 = 4.52;$$
$$x_3 = 4.171,\quad y_3 = 4.36;\quad x_4 = 4.61,\quad y_4 = 4.80.$$

qui, étant divisées par 4, produit des deux multiplicateurs auxiliaires, donnent les quatre systèmes de décomposition de dernière espèce de $\overline{189}^2$.

4° $t = 15$, $N = 17.23.19 = 7429$. Les facteurs 17 et 23 sont diviseurs linéaires, tandis que 19 est diviseur quadratique. En écrivant

$$N = (17.23).19 = (16^2 + 15.3^2)(2^2 + 15.1^2),$$

et appliquant les formules (1′) à ce produit de *deux* facteurs quadratiques, on trouve les deux solutions de dernière espèce

$$\overline{7429}^2 = \overline{7091}^2 + 15.\overline{572}^2 \quad \text{et} \quad \overline{7429}^2 = \overline{4429}^2 + 15.\overline{1540}^2.$$

5° $t = 19$, $N = 5.7.11 = 385$. Le multiplicateur quadratique est ici 4 pour les trois facteurs, d'où

$$64.N = (1^2 + 19.1^2)(3^2 + 19.1^2)(5^2 + 19.1^2)$$

et les formules (1′) donnent l'unique solution

$$N^2 = \overline{223}^2 + 19.\overline{72}^2,$$

correspondante à celle de $N = 385 = 9^2 + 19.4^2$, qui est aussi unique. Quant aux trois autres décompositions fournies par les formules (1′), savoir :

$$x_2 = 32.751, \quad x_3 = 32.769, \quad x_4 = 32.599,$$
$$y_2 = 32.39, \quad y_3 = 32.9, \quad y_4 = 32.111,$$

elles sont étrangères à la question, puisque les composants ont 32 pour facteur commun, au lieu de 64.

6° t, négatif, $= -3$,

$$N = 481 = 13.37 = (5^2 - 3.2^2)(7^2 - 3.2^2).$$

La formule générale (1′) donne les deux solutions

$$\overline{481}^2 = \overline{577}^2 - 3.\overline{184}^2 = \overline{3937}^2 - 3.\overline{2256}^2.$$

Le cas de t fractionnaire sera examiné plus loin.

La suite prochainement.