NOUVELLES ANNALES DE MATHÉMATIQUES

G. FONTENÉ

Correspondance $(1,1)$ entre les deux décompositions $N = A \times B$ et $N = P^2 + Q^2$

Nouvelles annales de mathématiques 4^e série, tome 3 (1903), p. 108-115

<http://www.numdam.org/item?id=NAM_1903_4_3__108_0>

© Nouvelles annales de mathématiques, 1903, tous droits réservés.

L'accès aux archives de la revue « Nouvelles annales de mathématiques » implique l'accord avec les conditions générales d'utilisation (http://www.numdam.org/conditions). Toute utilisation commerciale ou impression systématique est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

NUMDAM

Article numérisé dans le cadre du programme Numérisation de documents anciens mathématiques
http://www.numdam.org/

[15a]

CORRESPONDANCE (1, 1) ENTRE LES DEUX DÉCOMPOSITIONS $N = A \times B$ ET $N = P^2 + Q^2$;

PAR M. G. FONTENÉ.

§ I. — DÉCOMPOSITION D'UN NOMBRE EN UN PRODUIT DE DEUX FACTEURS.

1. Soit

$$N = a^\alpha b^\beta c^\gamma \dots,$$

les facteurs a, b, c, ... étant premiers. Le nombre des décompositions de N en un produit de deux facteurs est

$$\frac{(\alpha+1)(\beta+1)(\gamma+1)\dots}{2},$$

si N n'est pas carré parfait; lorsque N est un carré, le nombre des décompositions est

$$\frac{(\alpha+1)(\beta+1)(\gamma+1)\dots-1}{2}+1$$

ou

$$\frac{(\alpha+1)(\beta+1)(\gamma+1)\dots+1}{2}.$$

2. Le nombre des décompositions de N en un produit de deux facteurs premiers entre eux est égal au nombre des décompositions de $abc\dots$ en un produit de deux facteurs, soit

$$2^{k-1},$$

en appelant k le nombre des facteurs premiers distincts. Les facteurs en question sont d'ailleurs les

termes du produit

$$(1+a^{\alpha})(1+b^{\beta})(1+c^{\gamma})\ldots,$$

c'est-à-dire les termes du polynome

$$1+(a^{\alpha}+b^{\beta}+\ldots)+(a^{\alpha}b^{\beta}+\ldots)+(a^{\alpha}b^{\beta}c^{\gamma}+\ldots)+\ldots,$$

chaque facteur s'associant avec un autre pour donner le produit N. On suppose N différent de 1.

3. Soit $N = A \times B$, A et B ayant Δ pour plus grand commun diviseur; on a

$$N = \Delta^2 ab,$$

a et b étant premiers entre eux. Les décompositions de N en un produit de deux facteurs ayant Δ comme plus grand commun diviseur, correspondent donc aux décompositions du quotient $N : \Delta^2$ en deux facteurs premiers entre eux.

4. On peut classer les décompositions de N en un produit de deux facteurs d'après le plus grand commun diviseur Δ de ces facteurs : il faudra prendre pour Δ^2 tous les diviseurs carrés de N. Soit

$$N = a^{\alpha}b^{\beta}\ldots r^{\rho}s^{\sigma}\ldots,$$

les exposants α, β, ... étant impairs, les exposants ρ, σ, ... étant pairs; soit k le nombre des facteurs premiers distincts. Les diviseurs carrés Δ^2 sont les termes du produit

$$\begin{aligned}
&(1+a^2+a^4+\ldots+a^{\alpha-1})\\
&\times(1+b^2+b^4+\ldots+b^{\beta-1})\\
&\times\ldots\ldots\ldots\ldots\ldots\ldots\\
&\times(1+r^2+r^4+\ldots+r^{\rho-2}+r^{\rho})\\
&\times(1+s^2+s^4+\ldots+s^{\sigma-2}+s^{\sigma})\\
&\times\ldots\ldots\ldots\ldots\ldots\ldots
\end{aligned}$$

Dans les premiers facteurs, le nombre des termes est $\frac{\alpha+1}{2}$, $\frac{\beta+1}{2}$, $\cdots$; dans les derniers facteurs, en comptant à part le dernier terme, le nombre des termes est $\frac{\rho}{2}+1$, $\frac{\sigma}{2}+1$, ... Si, pour former un diviseur carré Δ^2, on n'emploie, comme facteur, aucun des termes r^ρ, s^σ, ..., où l'exposant est celui qui entre dans N, le quotient $\frac{N}{\Delta^2}$ a des facteurs premiers distincts en nombre k, et donne des décompositions en nombre 2^{k-1}; pour chaque facteur r^ρ, s^σ, ... introduit dans Δ^2, le nombre des facteurs premiers distincts du quotient $\frac{N}{\Delta^2}$ diminue d'une unité, et le nombre des décompositions, au lieu d'être 2^{k-1}, est seulement alors $2^{k-1}\times\frac{1}{2}\times\frac{1}{2}\times\ldots$. On trouve ainsi que le nombre total des décompositions de N est

$$n=2^{k-1}\left(\frac{\alpha+1}{2}\right)\left(\frac{\beta+1}{2}\right)\cdots\left(\frac{\rho}{2}+\frac{1}{2}\right)\left(\frac{\sigma}{2}+\frac{1}{2}\right)\cdots;$$

les derniers facteurs, s'il y en a trois, par exemple, ont pour produit

$$\frac{\rho}{2}\frac{\sigma}{2}\frac{\tau}{2}+\frac{1}{2}\sum\frac{\rho}{2}\frac{\sigma}{2}+\frac{1}{4}\sum\frac{\rho}{2}+\frac{1}{8},$$

ce qui rend compte de la formule. On a donc

$$n=\frac{(\alpha+1)(\beta+1)\ldots(\rho+1)(\sigma+1)\ldots}{2}.$$

Toutefois, si le nombre N est un carré, quand on prend $\frac{N}{\Delta^2}=1$, le calcul précédent donne $2^{k-1}\times\frac{1}{2^k}$ ou $\frac{1}{2}$ comme nombre des solutions, au lieu de 1 qui est le nombre exact; le nombre total des décompositions est

donc, pour ce cas exceptionnel,

$$n = \frac{(\rho+1)(\sigma+1)\ldots+1}{2}.$$

On retrouve bien le résultat indiqué au n° 1.

§ II. — Décomposition d'un nombre en une somme de deux carrés.

5. On appelle entiers imaginaires de Gauss les nombres de la forme $x+yi$, x et y étant entiers; ces entiers imaginaires ont les mêmes lois de divisibilité que les entiers ordinaires.

Sont premiers absolus dans le domaine considéré :

1° Les nombres premiers réels de la forme $4h-1$;

2° Le nombre $1+i$ dont la norme est égale à 2;

3° Les nombres $x+yi$, dont les normes sont les nombres premiers ordinaires de la forme $4h+1$.

6. La norme d'un nombre du domaine peut s'écrire

$$N = P^2 \times 2^p \times (a+a'i)^\alpha (a-a'i)^\alpha \times \ldots,$$

P étant un produit de facteurs premiers de la forme $4h-1$, les facteurs $a+a'i$, ... étant premiers, ou encore

$$N = P^2 \times 2^p \times A^\alpha \times B^\beta \times \ldots,$$

les nombres premiers A, B, ... étant de la forme $4h+1$.

Quand on cherche les solutions de l'équation

$$X^2 + Y^2 = N,$$

si l'on fait

$$p = 2p' + \pi \qquad (\pi = 0 \text{ ou } 1),$$

il faudra prendre

$$X = P \times 2^{p'} \times x, \qquad Y = P \times 2^{p'} \times y,$$

de sorte que l'on est ramené à résoudre

$$x^2+y^2=\mathrm{N}'=\mathrm{A}^{\alpha}\mathrm{B}^{\beta}\ldots\times 1 \quad \text{ou} \quad 2.$$

En ce qui concerne la présence du facteur 2, si l'on pose

$$\mathrm{N}''=\mathrm{A}^{\alpha}\mathrm{B}^{\beta}\ldots,$$

et si l'on a

$$\mathrm{N}''=x^2+y^2=(x+yi)(x-yi),$$

on aura

$$\begin{aligned}2\mathrm{N}''&=(x+yi)(1+i)\times(x-yi)(1-i)\\&=(x-y)^2+(x+y)^2;\end{aligned}$$

à cause de

$$1-i=(1+i)\times -i, \qquad 1+i=(1-i)i,$$

on aura le même résultat en écrivant

$$2\mathrm{N}''=(x+yi)(1-i)\times(x-yi)(1+i);$$

il y a donc autant de décomposition du nombre $2\mathrm{N}''$ que du nombre N'', et il suffit de considérer l'équation

$$x^2+y^2=\mathrm{N}''=\mathrm{A}^{\alpha}\mathrm{B}^{\beta}\ldots.$$

7. Chacun des nombres premiers A, B, ... est d'une seule façon, somme de deux carrés; soit

$$\mathrm{N}''=(a^2+a'^2)^{\alpha}(b^2+b'^2)^{\beta}(c^2+c'^2)^{\gamma};$$

on suppose a, a', ... positifs. Il sera entendu que l'on a fixé, *arbitrairement d'ailleurs,* l'ordre des deux carrés qui composent chaque facteur, et l'on s'interdira de modifier cet ordre; on doit, en effet, dans ce qui suit, remplacer $a^2+a'^2$ par $(a+a'i)(a-a'i)$, et faire jouer des rôles différents aux deux facteurs de ce produit; or, si l'on prenait a'^2+a^2, on aurait

$$(a'+ai)(a'+ai),$$

ce qui équivaudrait à échanger les rôles des deux facteurs.

Soit une décomposition du nombre N'' en un produit de deux facteurs; en désignant par Δ le plus grand commun diviseur des deux facteurs, on peut écrire, par exemple,

$$N'' = \Delta(a^2 + a'^2)^\lambda (b^2 + b'^2)^\mu \times \Delta(c^2 + c'^2)^\nu.$$

Écrivons alors, d'après une loi facile à saisir :

$$\begin{aligned} N'' = \quad & \Delta(a + a'i)^\lambda (b + b'i)^\mu (c - c'i)^\nu \\ & \times \Delta(a - a'i)^\lambda (b - b'i)^\mu (c + c'i)^\nu; \end{aligned}$$

nous aurons

$$N'' = \Delta(p + qi) \times \Delta(p - qi) = (\Delta p)^2 + (\Delta q)^2 = P^2 + Q^2,$$

les deux nombres P et Q ayant Δ pour plus grand commun diviseur.

On a ainsi établi, entre les décompositions du nombre N'' *en produit de deux facteurs et les décompositions de ce nombre en somme de deux carrés, une correspondance* (1, 1), dépendant à la vérité de la façon dont on a fixé l'ordre des deux carrés, dans chacun des facteurs premiers $a^2 + a'^2$, ..., mais bien déterminée dès que cet ordre est fixé. Et cette correspondance est telle que *le plus grand commun diviseur des deux facteurs qui forment le produit* N'' *est aussi celui des deux nombres* P *et* Q, *dont les carrés ont pour somme* N''.

8. Pour $\Delta = 1$, on a les décompositions propres de N''. Si l'on se donne Δ, Δ^2 étant un diviseur de N'' (1^2 compris, N'' compris s'il y a lieu), on veut avoir

$$p^2 + q^2 = \frac{N''}{\Delta^2},$$

p et q premiers entre eux, c'est-à-dire que l'on a à chercher les décompositions du nombre $\frac{N''}{\Delta^2}$. Ce classement des solutions d'après Δ correspond au classement analogue des solutions du problème considéré tout d'abord.

9. Le nombre total des décompositions du nombre N'' en somme de deux carrés est égal, d'après ce qui précède, au nombre des décompositions du même nombre en un produit de deux facteurs, soit

$$\frac{(\alpha+1)(\beta+1)(\gamma+1)\ldots}{2},$$

si N'' n'est pas un carré, et

$$\frac{(\alpha+1)(\beta+1)(\gamma+1)\ldots+1}{2},$$

si N'' est un carré, en acceptant la décomposition

$$N''=(\sqrt{N''})^2+0^2.$$

Ces formules ont été données par Gauss. Lejeune-Dirichlet a donné, je crois, une autre forme au résultat, en considérant directement le nombre N. J'ignore si la correspondance établie ici a déjà été observée.

En supposant N'' différent de 1, le nombre des décompositions propres est 2^{k-1}, k étant le nombre des facteurs premiers distincts A, B, ...; par $N=1$, on a la décomposition $1=1^2+0^2$. Le nombre des décompositions impropres, avec une valeur donnée de Δ, s'obtient d'une manière analogue, en considérant $\frac{N''}{\Delta^2}$, etc.

10. Voici un exemple de calcul numérique. Soit trouvé

$$5^n=p^2+q^2;$$

on a

$$\begin{aligned} 5^{n+1} &= (p+qi)(p-qi)(2+i)(2-i) \\ &= [(2p-q)+(p+2q)i]\times\dots \\ &= (2p-q)^2+(p+2q)^2. \end{aligned}$$

En partant de $5 = 2^2+1^2$, on obtient les décompositions propres des puissances successives de 5, soit

$$2^2+1^2,\quad 3^2+4^2,\quad 2^2+11^2,\quad (-7)^2+24^2,\quad \dots;$$

en ayant soin de garder le signe —, on aura ensuite

$$(-38)^2+(41)^2.$$