NOUVELLES ANNALES DE MATHÉMATIQUES

ANGELO GENOCCHI

Note sur une formule de M. Gauss relative à la décomposition d'un nombre en deux carrés et sur quelques formules analogues

Nouvelles annales de mathématiques 1re série, tome 13 (1854), p. 158-170

<http://www.numdam.org/item?id=NAM_1854_1_13__158_1>

NOTE SUR UNE FORMULE DE M. GAUSS RELATIVE A LA DÉCOMPOSITION D'UN NOMBRE EN DEUX CARRÉS ET SUR QUELQUES FORMULES ANALOGUES;

PAR M. ANGELO GENOCCHI (DE TURIN).

Je démontrerai la formule de M. Gauss, qui exprime de combien de manières un nombre entier peut être décomposé en deux carrés (voir *Nouvelles Annales*, t. IX, p. 307).

Je remarque d'abord qu'il y a autant de décompositions pour un nombre n que pour son double. En effet, si l'on a

$$n = u^2 + v^2,$$

il en résulte

$$2n = (u + v)^2 + (u - v)^2;$$

et réciproquement, de

$$2n = u'^2 + v'^2,$$

où u' et v' seront tous les deux pairs ou impairs, on conclut

$$n = \left(\frac{u' + v'}{2}\right)^2 + \left(\frac{u' - v'}{2}\right)^2;$$

donc, à toute décomposition de n, il répond une décomposition de $2n$, et *vice versâ*, et l'on voit d'ailleurs, par ces formules, que les décompositions correspondantes à deux décompositions différentes de l'un des mêmes nombres seront aussi différentes entre elles.

Il suit de là qu'on peut supprimer, dans le nombre proposé, tout facteur puissance de 2, ce qui donnera pour résultat un nombre impair.

En second lieu, si t est le plus grand commun diviseur de u et v, et qu'on fasse

$$u = tu', \quad v = tv',$$

l'équation

$$n = u^2 + v^2$$

deviendra

$$n = t^2 (u'^2 + v'^2),$$

de sorte que $t^2 (u'^2 + v'^2)$ sera divisible par tout diviseur premier p de n. Donc, si p est de la forme $4m + 3$, ne pouvant diviser la somme $u'^2 + v'^2$ de deux carrés premiers entre eux, ce nombre divisera t; et posant

$$n = p^{\pi} n', \quad t = p^{\rho} t',$$

où π et ρ sont des exposants entiers, et n', t' des entiers

premiers à p, on aura

$$p^{\pi} n' = p^{2\rho} t'^2 (u'^2 + v'^2),$$

et, par conséquent,

$$\pi = 2\rho,$$

c'est-à-dire que l'exposant π doit être pair. On voit donc que, si n est décomposable en deux carrés, le produit de tous ses diviseurs premiers de la forme $4m+3$ sera un carré, facteur commun de ces deux mêmes carrés.

On aura en même temps

$$n' = t'^2 (u'^2 + v'^2),$$

et l'on en conclura que, dans cette recherche, on peut aussi faire abstraction des diviseurs premiers de la forme $4m+3$, et, en conséquence, ne considérer que les nombres dont tous les diviseurs premiers ont la forme $4m+1$.

Cela posé, si n est un nombre premier de cette forme, on sait qu'il peut toujours être décomposé en deux carrés, mais d'une seule manière. Si $n = p^{\pi}$, p étant un nombre premier de la même forme, on pourra supposer

$$n = u^2 + v^2 = (u + v\sqrt{-1})(u - v\sqrt{-1}),$$
$$p = q^2 + r^2 = (q + r\sqrt{-1})(q - r\sqrt{-1}),$$

d'où

$$(u + v\sqrt{-1})(u - v\sqrt{-1}) = (q + r\sqrt{-1})^{\pi} (q - r\sqrt{-1})^{\pi};$$

donc $u + v\sqrt{-1}$ sera l'un des diviseurs *complexes* du produit

$$(q + r\sqrt{-1})^{\pi} (q - r\sqrt{-1})^{\pi}.$$

Or, pour les nombres complexes de la forme $A + B\sqrt{-1}$, on démontre le principe, que ces nombres ne peuvent être décomposés en facteurs complexes *premiers* que d'une seule manière (*) ; d'ailleurs, $q + r\sqrt{-1}$ et $q - r\sqrt{-1}$ sont des nombres complexes premiers : donc $u + v\sqrt{-1}$ aura la forme

$$(\sqrt{-1})^i (q + r\sqrt{-1})^h (q - r\sqrt{-1})^k,$$

i étant 0, 1, 2, ou 3, et h, k étant nuls ou entiers positifs. On en tire

$$u - v\sqrt{-1} = (-\sqrt{-1})^i (q - r\sqrt{-1})^h (q + r\sqrt{-1})^k;$$

et, par la multiplication,

$$u^2 + v^2 = (q^2 + r^2)^{h+k},$$

c'est-à-dire

$$n = p^{h+k};$$

d'où il suit

$$h + k = \pi,$$

et

$$u + v\sqrt{-1} = (\sqrt{-1})^i (q + r\sqrt{-1})^h (q - r\sqrt{-1})^{\pi - h}.$$

Cette équation fournira toutes les valeurs possibles de u et v, et, par suite, toutes les décompositions de n en deux

(*) Je renvoie au beau Mémoire de M. Gauss, *Theoria resid. biquadr.*, inséré dans les *Comment Gotting. recent.*, tome VII; on peut voir aussi une démonstration de Wantzel dans les *Comptes rendus* de l'Institut, séance du 15 mars 1847. Le même principe n'est pas vrai pour les nombres complexes de tous les degrés, comme M. Kummer l'a démontré (*voyez* le Journal de M. Liouville, tome XII, page 202). Ainsi c'est, je crois, par inadvertance qu'on a dit (*Nouvelles Annales*, tome VIII, page 364) que la démonstration du dernier théorème de Fermat dépend de ce principe.

carrés, en remplaçant h successivement par $0, 1, 2, 3, \ldots, \pi$. Mais on peut la réduire à

$$u + v\sqrt{-1} = (q + r\sqrt{-1})\ (q - r\sqrt{-1})^{\pi - h},$$

car le facteur $(\sqrt{-1})^t$ ne peut qu'échanger entre elles les valeurs de u et v, ou changer leurs signes, ce qui n'augmente pas le nombre des décompositions. On aura ainsi $\pi + 1$ déterminations de u et v; mais comme

$$u - v\sqrt{-1} = (q - r\sqrt{-1})^h\,(q + r\sqrt{-1})^{\pi - h},$$

et que, par conséquent, la substitution de $\pi - h$ à h change seulement le signe de v, on n'emploiera que la moitié des valeurs de h, et le nombre des déterminations sera réduit à $\frac{\pi + 1}{2}$ si π est impair, à $\frac{\pi}{2} + 1$ si π est pair.

Dans ce dernier cas, on aura, pour $h = \frac{1}{2}\pi$, la détermination

$$u + v\sqrt{-1} = (q + r\sqrt{-1})^h\,(q - r\sqrt{-1})^h = (q^2 + r^2)^h,$$

c'est-à-dire

$$u = (q^2 + r^2)^h, \quad v = 0;$$

alors $n = u^2$ et n'est pas décomposé en deux carrés : donc, en excluant cette détermination, on conclura que le nombre des décompositions de $n = p^\pi$ en deux carrés est $\frac{\pi + 1}{2}$ pour π impair, $\frac{\pi}{2}$ pour π pair.

Je suppose maintenant $n = p^\pi n'$, n' étant premier à p, et j'ai

$$(u + v\sqrt{-1})\ (u - v\sqrt{-1})$$
$$= (q + r\sqrt{-1})^\pi\,(q - r\sqrt{-1})^\pi\,n',$$

qui montre que $u + v\sqrt{-1}$ doit être un diviseur complexe du produit

$$(q + r\sqrt{-1})^{\pi}(q - r\sqrt{-1})^{\pi} n';$$

donc, si $u' + v'\sqrt{-1}$ désigne un diviseur complexe de n', $u + v\sqrt{-1}$ aura la forme

$$(\sqrt{-1})^{i}(q + r\sqrt{-1})^{h}(q - r\sqrt{-1})^{k}(u' + v'\sqrt{-1}),$$

d'où, en changeant le signe de $\sqrt{-1}$, et multipliant les résultats, on tirera

$$u^2 + v^2 = (q^2 + r^2)^{h+k}(u'^2 + v'^2),$$

ou

$$n = p^{h+k}(u'^2 + v'^2),$$

et, par suite,

$$h + k = \pi, \quad u'^2 + v'^2 = n'.$$

On obtiendra donc toutes les valeurs de u et v par l'équation

$$u + v\sqrt{-1}$$

$$= (\sqrt{-1})^{i}(q + r\sqrt{-1})^{h}(q - r\sqrt{-1})^{\pi - h}(u' + v'\sqrt{-1}),$$

où l'on remplacera h successivement par $0, 1, 2, 3, \ldots, \pi$, et u', v' par toutes les solutions de l'équation

$$u'^2 + v'^2 = n'.$$

Mais on peut, pour les mêmes raisons que ci-dessus, omettre le facteur $(\sqrt{-1})^{i}$, et alors l'équation précédente fournira $(\pi + 1)$ N′ déterminations de u et v, N′ étant le

nombre des solutions de l'équation

$$u'^2 + v'^2 = n'.$$

Ces déterminations seront égales deux à deux au signe de v près, si l'on emploie successivement tous les deux diviseurs complexes $u' + v'\sqrt{-1}$ et $u' - v'\sqrt{-1}$ de n', car on aura

$$u - v\sqrt{-1} = (q - r\sqrt{-1})^h (q + r\sqrt{-1})^{\pi - h} (u' - v'\sqrt{-1});$$

si π est pair et n' un carré, on aura ainsi la détermination

$$u + v\sqrt{-1} = (q + r\sqrt{-1})^h (q - r\sqrt{-1})^h u' = (q^2 + r^2)^h u'$$

pour $h = \frac{1}{2}\pi$, et

$$u'^2 = n', \quad v' = 0,$$

laquelle donnant

$$u = (q^2 + r^2)^h u', \quad v = 0,$$

ne devra pas être comptée dans les décompositions de n en deux carrés. Donc le nombre de ces décompositions sera

$$\frac{(\pi + 1)\,\mathrm{N}'}{2}$$

lorsque, n n'étant pas un carré, π est impair, et sera

$$\frac{(\pi + 1)\,\mathrm{N}' - 1}{2}$$

si n est un carré et π pair : N' exprime combien il y a des nombres complexes

$$u' + v'\sqrt{-1}, \quad u' - v'\sqrt{-1},$$

qui satisfont à l'équation

$$u'^2 + v'^2 = n',$$

et se déduit du nombre des décompositions de n' en deux carrés, puisque ce nombre est $\frac{N'}{2}$ si n' est pair, et $\frac{N'-1}{2}$ si N' est impair.

De tout cela il est facile de conclure que si

$$n = a^{\alpha} b^{\beta} c^{\gamma} \ldots,$$

a, b, c, etc., étant des diviseurs premiers différents, tous de la forme $4m+1$, et α, β, γ, etc., des exposants entiers positifs, et si l'on fait

$$N = (\alpha+1)(\beta+1)(\gamma+1)\ldots,$$

le nombre des décompositions de n en deux carrés sera $\frac{N}{2}$ lorsque n n'est pas un carré, et $\frac{N-1}{2}$ lorsque n est un carré. Car ce théorème est démontré dans le cas d'un seul diviseur premier, et l'on peut aussi déduire de ce qui précède que, s'il est vrai pour i diviseurs premiers, il sera vrai également pour un diviseur premier de plus.

On obtient ainsi la formule de M. Gauss.

Si l'on cherche le nombre des solutions de l'équation

$$x^2 + y^2 = n,$$

on peut compter comme telle $x = \sqrt{n}$, $y = 0$, dans le cas de n carré, et alors ce nombre serait $\frac{N+1}{2}$ au lieu de $\frac{N-1}{2}$ (*).

On sait que N est le nombre des diviseurs entiers de n.

(*) Ceci montre l'inutilité de la correction indiquée tome IX, page 308. Tm.

La formule de M. Gauss est aussi une conséquence de l'équation (*)

$$(1 + 2t + 2t^4 + 2t^9 + \ldots)^2 = 1 + 4\left(\frac{t}{1-t} - \frac{t^3}{1-t^3} + \frac{t^5}{1-t^5} - \ldots\right),$$

à laquelle on est conduit dans la théorie des fonctions elliptiques ou des *factorielles réciproques*. En effet, si l'on représente par $M t^n$ le terme général du premier membre développé, l'exposant n sera de la forme $x^2 + y^2$, et le coefficient M sera

$$M = 2N_1 + 4N_2,$$

où N_1 indique le nombre (0 ou 2) des solutions de l'équation

$$x^2 + y^2 = n,$$

l'une des inconnues x, y étant nulle, et N_2 indique le nombre des autres solutions de la même équation, pourvu qu'on compte comme deux solutions les deux déterminations

$$x = u \quad \text{et} \quad y = v, \quad x = v \quad \text{et} \quad y = u,$$

si u et v sont différents, et comme une seule si $u = 0$, mais sans avoir égard au signe de x et de y. D'autre part, un terme quelconque du second membre est

$$4(-1)^i \frac{t^{2i+1}}{1 - t^{2i+1}},$$

qui se développe en termes de la forme

$$4(-1)^i . t^{2i+1} . t^{(2i+1)h} = 4(-1)^i t^{(2i+1)(h+1)},$$

de sorte que l'exposant de t sera n si l'on a

$$(2i + 1)(h + 1) = n,$$

(*) Cauchy, *Comptes rendus*, 1843, 2e semestre, pages 523 et 567.

et, par suite, si $2i+1$ est un diviseur de n; on voit, de plus, que ce terme sera positif si i est pair, négatif si i est impair, et que, dans le premier cas, $2i+1$ est de la forme $4m+1$; dans le second, $2i+1$ est de la forme $4m+3$; donc, en appelant d_1 le nombre total des diviseurs de n de la première forme, d_3 celui des diviseurs de la seconde, l'agrégat de tous les coefficients de t^n dans le développement du second membre sera

$$4d_1 - 4d_3,$$

qui devra être égal à M, et, par conséquent,

$$N_1 + 2N^2 = 2(d_1 - d_3).$$

Donc, si n est réduit à n'avoir aucun diviseur premier de la forme $4m+3$, d_3 étant nul, on aura

$$N_1 + 2N_2 = 2d_1,$$

résultat qui coincide, comme on voit facilement, avec la formule de M. Gauss.

La même théorie, que nous venons de rappeler, donne l'équation

$$(1+2t+2t^4+2t^9+\ldots)(1+2t^3+2t^{2\cdot4}+2t^{2\cdot9}+\ldots)$$
$$= 1+2\left(\frac{t}{1-t}+\frac{t^3}{1-t^3}-\frac{t^5}{1-t^5}-\frac{t^7}{1-t^7}+\ldots\right),$$

de laquelle on tire d'une manière semblable le nombre des solutions de l'équation

$$x^2+2y^2=n.$$

Si N_1 est le nombre des solutions de cette équation lorsque l'une des inconnues est nulle, et N_2 celui des autres solutions; si, d'autre part, on exprime respectivement par

d_1, d_3, d_5, d_7 combien le nombre n a de diviseurs des formes

$$8m+1, \quad 8m+3, \quad 8m+5, \quad 8m+7,$$

on trouvera

$$N_1 + 2N_2 = d_1 + d_3 - d_5 - d_7.$$

On a aussi

$$(1+2t+2t^4+2t^9+\ldots)(1+2t^3+2t^{3\cdot 4}+2t^{3\cdot 9}+\ldots)$$
$$= 1 + 2\left(\frac{1-t}{1-t^3}t + \frac{1+t^2}{1+t^6}t^2 + \frac{1-t^3}{1-t^9}t^3 + \ldots\right),$$

et en appelant N_1 le nombre des solutions de l'équation

$$x^2 + 3y^2 = n,$$

qui correspondent à l'une des inconnues nulle, N_2 celui des autres solutions, on trouvera

$$N_1 + 2N_2 = (-1)^n (d_1 - d_2 - d_3 - d_4) :$$

ici, d_1 est le nombre de ces diviseurs i de n, dont les réciproques $\frac{n}{i}$ sont de la forme $3m+1$, et diffèrent d'eux d'un nombre impair; d_2 est le nombre des diviseurs dont les réciproques sont aussi de la forme $3m+1$, mais diffèrent d'eux d'un nombre pair; d_3 est le nombre des diviseurs dont les réciproques sont de la forme $3m+2$, et diffèrent d'eux d'un nombre impair; et enfin, d_4 est le nombre des autres diviseurs, dont les réciproques sont de la forme $3m+2$ (*).

(*) La formule qu'a donnée M. Cauchy (*Comptes rendus*, tome XIX, page 1383) revient à celle-ci; mais il faut y mettre $\frac{1}{2}$N à la place de N, et entendre par N le nombre de toutes les solutions entières positives, entières négatives et nulles de l'équation

$$x^2 + 3y^2 = n.$$

Ces deux formules peuvent aussi être démontrées par la première méthode que j'ai exposée pour celle de M. Gauss.

Je rappellerai enfin les deux équations :

$$(t+t^3+t^{25}+t^{49}+\ldots)^4$$
$$=\frac{t^4}{1-t^8}+\frac{3t^{12}}{1-t^{24}}+\frac{5t^{20}}{1-t^{40}}+\frac{7t^{28}}{1-t^{56}}+\ldots,$$

$$(1+2t+2t^4+2t^9+\ldots)^4$$
$$=1+8\left(\frac{t}{1-t}+\frac{2t^2}{1+t^2}+\frac{3t^3}{1-t^3}+\ldots\right).$$

De la première on déduira que, si n est un nombre impair, et si l'on désigne par D la somme de ses diviseurs, et par N le nombre des solutions de l'équation

$$x^2+y^2+z^2+u^2=4n$$

en nombres impairs, on a

$$N=D.$$

Quant à la deuxième, soient n un entier quelconque, D_1 la somme de ses diviseurs impairs, D_2 la somme de ses diviseurs pairs dont les réciproques sont impairs, et D_4 la somme de ses diviseurs pairs dont les réciproques sont aussi pairs; de plus, que le nombre des solutions de l'équation

$$x^2+y^2+z^2+u^2=n$$

soit N_1 si trois des inconnues sont nulles, N_2 si deux sont nulles, N_3 si une seule inconnue est nulle, N_4 si aucune n'est nulle : on aura

$$N_1+2N_2+4N_3+8N_4=4(D_1+D_2-D_4).$$

On doit remarquer que les deux déterminations

$$x=a,\quad y=b,\quad z=c,\quad u=d.$$

et

$$x = b, \quad y = a, \quad z = c, \quad u = d$$

sont comptées pour deux solutions si a et b sont différents, et ainsi des autres.