JOURNAL
DE
MATHÉMATIQUES
PURES ET APPLIQUÉES
FONDÉ EN 1836 ET PUBLIÉ JUSQU'EN 1874
PAR JOSEPH LIOUVILLE

J. LIOUVILLE

Sur un certain genre de décompositions d'un entier en sommes de carrés

Journal de mathématiques pures et appliquées 2^e^ série, tome 6 (1861), p. 233-238.
<http://www.numdam.org/item?id=JMPA_1861_2_6__233_0>

SUR

UN CERTAIN GENRE DE DÉCOMPOSITIONS D'UN ENTIER EN SOMMES DE CARRÉS;

PAR M. J. LIOUVILLE.

Les décompositions d'un entier n en sommes de carrés dont je veux m'occuper ici offrent ce caractère particulier que, lorsqu'il y a dans l'expression de n des carrés impairs, on en prend la racine positivement et on les range avant les autres, dans un ordre du reste quelconque. Le double signe est conservé pour les racines des carrés pairs, à moins qu'elles ne se réduisent à zéro.

J'introduis à ce sujet une notation nouvelle. Je désigne par

$$N(n, p, q)$$

le nombre des décompositions de n en p carrés dont les q premiers sont impairs et à racines positives, tandis que les $(p-q)$ derniers sont pairs et à racines indifféremment positives, nulles ou négatives. En d'autres termes, nous désignons par $N(n, p, q)$ le nombre des solutions de l'équation

$$n = i_1^2 + i_2^2 + \ldots + i_q^2 + \varpi_1^2 + \varpi_2^2 + \ldots + \varpi_{p-q}^2,$$

dont le premier membre est donné, et où la lettre i désigne des entiers positifs impairs, tandis que les entiers ϖ sont indifféremment positifs, nuls ou négatifs. On prendra $q = 0$ si tous les carrés sont pairs.

Soit par exemple $n = 2m$, m étant impair, et $p = 12$, en sorte qu'il s'agisse des décompositions du double d'un entier impair en une somme de douze carrés. Les décompositions spéciales que nous considérons ne pourront être que de trois espèces; car des douze carrés dont la somme exprime $2m$, deux, six ou dix seront impairs et les autres pairs. Les valeurs à donner à q seront donc 2, 6, 10. D'après notre notation $N(2m, 12, 2)$, $N(2m, 12, 6)$, $N(2m, 12, 10)$ répondent respectivement à ces trois cas. Les autres valeurs de $N(2m, 12, q)$ sont nulles. Il est évident que pour $m = 1$, on a

$$N(2, 12, 2) = 1, \quad N(2, 12, 6) = 0, \quad N(2, 12, 6) = 0.$$

Pour $m = 3$, on trouve facilement

$$N(6, 12, 2) = 20, \quad N(2, 12, 6) = 1, \quad N(2, 12, 10) = 0,$$

la valeur de $N(6, 12, 2)$ dépendant de l'équation

$$6 = 1^2 + 1^2 + (\pm 2)^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2 + 0^2,$$

où $(\pm 2)^2$ peut prendre dix places distinctes. On trouve de même pour $m = 5$,

$$N(10, 12, 2) = 182, \quad N(10, 12, 6) = 12, \quad N(10, 12, 10) = 1.$$

Et ainsi de suite.

Le nombre complet des *représentations* de l'entier n par une somme de p carrés, c'est-à-dire le nombre des solutions de l'équation

$$n = x_1^2 + x_2^2 + \ldots + x_p^2,$$

où $x_1, x_2, \ldots, x_p$ sont des entiers indifféremment pairs ou impairs, positifs, nuls ou négatifs, sera désigné convenablement par

$$N(n, p).$$

On le déduirait immédiatement des nombres partiels $N(n, p, 0)$, $N(n, p, 1)$, etc., si ceux-ci étaient connus; car on passe de nos décompositions aux représentations en donnant aux entiers impairs marqués par la lettre i le double signe $\pm$, puis permutant les i et les ϖ et faisant la somme des résultats.

Ainsi dans l'exemple ci-dessus de $p = 12$, $n = 2m$, m impair, la valeur de $N(2m, 12)$ est égale à

$$\frac{11.12}{1.2}\left[2^2 N(2m, 12, 2) + 2^{10} N(2m, 12, 10)\right] \\ + 2^6 . \frac{7.8.9.10.11.12}{1.2.3.4.5.6} N(2m, 12, 6),$$

et peut s'écrire

$$N(2m, 12) = 264\left[N(2m, 12, 2) + 224 N(2m, 12, 6) \\ + 256 N(2m, 12, 10)\right].$$

Nous verrons bientôt qu'on peut tirer parti de ce résultat.

Les décompositions indiquées par la notation

$$N(n, p, q)$$

donnent lieu à une théorie étendue et fort intéressante. Mais je ne veux communiquer ici que deux théorèmes relatifs au cas de $n = 2m$, m impair, et où figureront les fonctions numériques que je désigne par $\zeta_\mu(m)$, $\rho_\mu(m)$, dont je rappelle la définition. Soit d un diviseur de m, δ le diviseur conjugué, de façon que $m = d\delta$: on a

$$\zeta_\mu(m) = \sum d^\mu,$$

et

$$\rho_\mu(m) = \sum (-1)^{\frac{\delta-1}{2}} d^\mu.$$

Quand $\mu = 0$, au lieu de $\zeta_0(n)$ et $\rho_0(n)$, j'écris simplement $\zeta(m)$ et $\rho(m)$.

Théorème I. « Si m désigne un entier impair à volonté et ν un » entier donné, on pourra poser, pour toutes les valeurs de m,

$$\zeta_{2\nu-1}(m) = N(2m, 4\nu, 2) + A_1 N(2m, 4\nu, 6) + \ldots \\ + A_{\nu-1} N(2m, 4\nu, 4\nu - 2),$$

» $A_1, A_2, \ldots, A_{\nu-1}$ étant des constantes, c'est-à-dire ayant des valeurs » indépendantes de m, mais qui changent quand ν change. »

Notre équation peut s'écrire

$$\zeta_{2\nu-1}(m) = \sum A_s \mathrm{N}(2m, 4\nu, 4s+2),$$

la sommation portant sur s dont les valeurs successives sont $0, 1, 2, \ldots, \nu-1$.

On a

$$A_0 = 1, \quad A_{\nu-1} = 16^{\nu-1},$$

et en général

$$A_{\nu-s-1} = 16^{\nu-2s-1} A_s.$$

Les coefficients A_s se déterminent d'ailleurs aisément au moyen des plus petites valeurs de m.

En passant aux cas particuliers, on trouve, pour $\nu = 1$,

$$\zeta_1(m) = \mathrm{N}(2m, 4, 2),$$

puis, pour $\nu = 2$,

$$\zeta_3(m) = \mathrm{N}(2m, 8, 2) + 16\mathrm{N}(2m, 8, 6),$$

puis, pour $\nu = 3$,

$$\zeta_5(m) = \mathrm{N}(2m, 12, 2) + 224\mathrm{N}(2m, 12, 6) + 256\mathrm{N}(2m, 12, 10).$$

Et ainsi de suite.

Laissant de côté les deux premières équations qui répondent à des théorèmes démontrés par Jacobi, j'observe que la troisième fournit $\mathrm{N}(2m, 12)$; car, d'après la valeur de $\mathrm{N}(2m, 12)$ indiquée plus haut et comparée à celle de $\zeta_5(m)$, il vient

$$\mathrm{N}(2m, 12) = 264\zeta_5(m),$$

ce qui s'accorde avec le théorème que j'ai donné dans le cahier de mai 1860 et qu'on peut établir aussi par d'autres procédés.

J'observerai en passant que la valeur de $\mathrm{N}(m, 12)$ semble moins simple. Elle dépend non-seulement de $\zeta_5(m)$ et $\zeta_1(m)$, mais encore de la somme

$$\sum s^4$$

des carrés des premiers termes dans l'ensemble des représentations de m par une somme de quatre carrés $s^2 + s'^2 + s''^2 + s'''^2$. Je trouve

$$\mathrm{N}(m, 12) = 8\zeta_5(m) - 16m^2\zeta_1(m) + 16\sum s^4.$$

Si m était pair, on aurait aisément $\sum s^4$, mais pour m impair la difficulté paraît grande. On pourrait encore faire dépendre $\mathrm{N}(m, 12)$ de $\mathrm{N}(4m, 12, 12)$, en vertu de l'équation

$$\mathrm{N}(m, 12) = 24\zeta_5(m) - 2^{12}\mathrm{N}(4m, 12, 12).$$

Mais ce n'est pas le lieu d'approfondir ces questions délicates.

Théorème II. « Si m désigne un entier impair à volonté et ν un en-
» tier donné, on pourra trouver des constantes

$$\mathrm{B}_0, \mathrm{B}_1, \ldots, \mathrm{B}_\nu$$

» telles, qu'on ait, pour toutes les valeurs de m,

$$\rho_{2\nu}(m) = \sum \mathrm{B}_s \mathrm{N}(2m, 4\nu + 2, 4s + 2),$$

» le signe sommatoire portant sur s dont les valeurs sont $0, 1, 2, \ldots, \nu - 1, \nu$. »

Les coefficients B_s sont constants en ce sens qu'ils ne dépendent pas de m. Ils changent avec ν; mais on a toujours $\mathrm{B}_0 = 1$, et dès que ν est > 0, on a $\mathrm{B}_\nu = 0$. Au surplus les coefficients B_s se calculent pour chaque valeur de ν au moyen des plus petites valeurs de m.

Pour $\nu = 0$, notre équation donne

$$\rho(m) = \mathrm{N}(2m, 2, 2),$$

ce qui répond au théorème si connu sur la décomposition de $2m$ en deux carrés impairs. Pour $\nu = 1$, elle donne

$$\rho_2(m) = \mathrm{N}(2m, 6, 2);$$

puis, pour $\nu = 2$,

$$\rho_4(m) = \mathrm{N}(2m, 10, 2) + 64\mathrm{N}(2m, 10, 6);$$

et ainsi de suite.

Je me contenterai de faire observer que la dernière des équations que je viens d'écrire conduit assez facilement à la valeur de $N(2m, 10)$ quand m est de la forme $4g+3$, auquel cas on peut prouver que

$$N(2m, 10, 2) = 16N(2m, 10, 6), \quad N(2m, 10, 10) = 0,$$

ce qui permet d'exprimer $N(2m, 10, 2)$ et $N(2m, 10, 6)$ au moyen de $\rho_4(m)$, et puisque les autres valeurs de $N(2m, 10, q)$ sont nulles, d'en conclure $N(2m, 10)$. J'ai trouvé ainsi :

$$N(2m, 10) = 12.17.\rho_4(m).$$

Dans la même supposition sur m, Eisenstein a obtenu

$$N(m, 10) = 12\rho_4(m).$$

Il faut donc que, pour $m = 4g+3$, on ait généralement

$$N(2m, 10) = 17N(m, 10);$$

et c'est en effet ce qu'on peut démontrer à priori par un raisonnement arithmétique très-simple.

Il y aurait, nous le répétons, bien des choses à dire au sujet des fonctions $N(n, p, q)$ et d'autres fonctions analogues. Mais tout cela viendra à son temps.