Séminaire Delange-Pisot-Poitou. Théorie des nombres

Jean Lagrange

Décomposition d'un entier en somme de carrés et fonction multiplicative

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 14, n° 1 (1972-1973), exp. n° 1, p. 1-5

<http://www.numdam.org/item?id=SDPP_1972-1973__14_1_A1_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
14e année, 1972/73, n° 1, 5 p.

9 octobre 1972

DÉCOMPOSITION D'UN ENTIER EN SOMME DE CARRÉS ET FONCTION MULTIPLICATIVE

par Jean LAGRANGE

1. Soient s et n deux entiers positifs, on désigne par $r_s(n)$ le nombre des représentations de n comme somme de s carrés. $r_s(n)$ est donc le nombre de solutions dans $\mathbb{Z}^s$ de l'équation

$$x_1^2 + x_2^2 + \ldots + x_s^2 = n .$$

En particulier, $r_s(1) = 2s$.

Posant $f_s(n) = r_s(n)/2s$, $g_s(n) = f_s(n^2) = r_s(n^2)/2s$, on va démontrer les deux théorèmes suivants :

THÉORÈME 1 (P. BATEMAN [1]). - La fonction f_s est multiplicative pour $s = 1 , 2 , 4 , 8$, et pour ces valeurs seulement.

THÉORÈME 2. - La fonction g_s est multiplicative pour $s = 1 , 2 , 3 , 4 , 5 , 6 , 7 , 8$, et pour ces valeurs seulement.

2. Posant $n = 2^{\alpha_0} m = 2^{\alpha_0} \prod p^{\alpha}$ (m entier impair, le produit est étendu aux diviseurs premiers de m), et $\chi(d) = (-1)^{(d-1)/2}$ (d entier impair), on a :

$$r_2(n) = 4 \textstyle\sum_{d|m} \chi(d) = 4\, \overline{\sigma}_0(m) ,$$

$$r_4(n) = 8(2 + (-1)^n) \textstyle\sum_{d|m} d = 8(2 + (-1)^n)\, \sigma_1(m) ,$$

$$r_6(n) = 4(4\, \chi(m)\, 2^{\alpha_0} - 1) \textstyle\sum_{d|m} \chi(d)\, d^2 = 4(4\, \chi(m)\, 2^{\alpha_0} - 1)\, \overline{\sigma}_2(m) ,$$

$$r_8(n) = \tfrac{16}{7}(8^{\alpha_0+1} - 1) \textstyle\sum_{d|m} d^3 = \tfrac{16}{7}(8^{\alpha_0+1} - 1)\, \sigma_3(m) ,$$

$$r_3(n^2) = 6 \textstyle\prod (\sigma_1(p^{\alpha}) - \chi(p)\, \sigma_1(p^{\alpha-1})) ,$$

$$r_5(n^2) = 10\, \sigma_3(2^{\alpha_0}) \textstyle\prod (\sigma_3(p^{\alpha}) - p\, \sigma_3(p^{\alpha-1})) ,$$

$$r_7(n^2) = 14(\sigma_5(2^{\alpha_0}) + 8\, \sigma_5(2^{\alpha_0-1})) \textstyle\prod (\sigma_5(p^{\alpha}) - p^2\, \chi(p)\, \sigma_5(p^{\alpha-1})) .$$

Les expressions de $r_s(n)$ pour $s = 2 , 4 , 6 , 8$, sont bien connues ; elles sont dues essentiellement à JACOBI ; pour des références, voir DICKSON ([2], chap. VI, VIII, IX).

Les expressions de $r_s(n^2)$ pour $s = 3 , 5 , 7$, sont dues respectivement à HURWITZ [4], HURWITZ [3], SANDHAM [5]. HURWITZ n'ayant pas donné explicitement le calcul de $r_3(n^2)$, on trouvera celui-ci au paragraphe 5.

Une simple vérification donne la partie directe des théorèmes 1 et 2.

3. Pour démontrer la partie réciproque du théorème 1, on remarque que, si f_s

est multiplicative, on doit avoir :

(1) $$f_s(2).f_s(3) = f_s(6) .$$

On obtient facilement

$$f_s(2) = s - 1 ,$$
$$f_s(3) = \frac{2(s-1)(s-2)}{3} ,$$
$$f_s(6) = 2(s-1)(s-2)(1 + \frac{(s-3)(s-4)(s-5)}{45}) .$$

(1) est donc une équation en s de degré 5 , ses racines sont 0 , 1 , 2 , 4 , 8 . D'où la conclusion.

4. Pour démontrer la partie réciproque du théorème 2 ([1]), on applique la méthode précédente. Si g_s est multiplicative, on doit avoir

$$g_s(2).g_s(3) = g_s(6) ,$$

soit :

(2) $$f_s(4).f_s(9) = f_s(36) .$$

Pour calculer $f_s(n)$, n fixé, en fonction de s , on utilise la fonction θ :

$$\theta(z) = \sum_{n=-\infty}^{\infty} z^{n^2} = 1 + 2 \sum_{n=1}^{\infty} z^{n^2} .$$

D'où :

$$\theta^s(z) = (1 + 2 \sum_{n=1}^{\infty} z^{n^2})^s = 1 + \sum_{n=1}^{\infty} r_s(n)\, z^n .$$

Les $a_j(n)$ étant définis par

$$(\sum_{n=1}^{\infty} z^{n^2})^j = \sum_{n=j}^{\infty} a_j(n)\, z^n ,$$

on a

$$r_s(n) = \sum_{j=1}^{n} 2^j\, a_j(n) \binom{s}{j}$$

et

$$f_s(n) = \sum_{j=1}^{n} (2^{j-1}/j)\, a_j(n) \binom{s-1}{j-1} .$$

$f_s(n)$ pour n fixé est un polynôme en s de degré $n-1$. L'équation (2) est donc de degré 35 . Il faut vérifier que ses seules racines positives entières sont 1 , 2 , ... , 8 .

$f_s(4).f_s(9)$ est un polynôme de degré 12 ; on écrit

$$f_s(4).f_s(9) = \sum_{j=1}^{12} b_j \binom{s-1}{j-1} ,$$

les calculs se faisant à l'aide de la formule de Newton.

On a ainsi

$$f_s(36) - f_s(4).f_s(9) = \sum_{j=1}^{36} c_j \binom{s-1}{j-1} ,$$

([1]) Cette démonstration m'a été communiquée par P. BATEMAN.

avec

$$c_j = a_j(36) - b_j \quad \text{pour} \quad 1 \leqslant j \leqslant 12 ,$$

$$c_j = a_j(36) \qquad \text{pour} \quad 13 \leqslant j \leqslant 36 ,$$

$j = 1 , 2 , \ldots , 8$ étant racine de l'équation (2), on a $c_j = 0$, pour $1 \leqslant j \leqslant 8$.

Par définition des $a_j(n)$, on a $c_j \geqslant 0$ pour $13 \leqslant j \leqslant 36$.

Un calcul montre de plus que $c_j > 0$ pour $9 \leqslant j \leqslant 12$.

On a donc, pour s entier supérieur ou égal à 9 ,

$$f_s(36) - f_s(4).f_s(9) \geqslant c_9 \left(8^{s-1}\right) > 0 ,$$

ce qui termine la démonstration.

En fait les calculs donnent

$$c_9 = \frac{247808}{9} , \quad c_{10} = 65536 , \quad c_{11} = 409600 , \quad c_{12} = 452608 .$$

5. Pour terminer, démontrons la formule d'Hurwitz

$$r_3(n^2) = 6 \prod \left(\sigma_1(p^\alpha) - \chi(p)\, \sigma_1(p^{\alpha-1})\right) ,$$

où on a posé $n = 2^{\alpha_0} m = 2^{\alpha_0} \prod p^\alpha$ (m impair).

Nous éviterons l'utilisation des formules elliptiques, supposant connues seulement les expressions de $r_2(n)$ et $r_4(n)$.

Rappelons que

$$r_2(n) = 4 \sum_{d|m} \chi(d) = 4\, \overline{\sigma}_1(m)$$

$$r_4(n) = 8(2 + (-1)^n) \sum_{d|m} d = 8(2 + (-1)^n)\, \sigma_1(m) .$$

Pour une démonstration élémentaire de ces formules, on pourra consulter VENKOV ([6], chap. 5).

Nous utiliserons le lemme suivant :

LEMME. - Si f est une fonction arithmétique complètement multiplicative, et si $F(n) = \sum_{d|n} f(d)$, on a :

$$F(n_1 n_2) = F(n_1).F(n_2) - \sum_p f(p)\, F\left(\frac{n_1}{p}\right).F\left(\frac{n_2}{p}\right) + \sum_{p,q} f(pq)\, F\left(\frac{n_1}{pq}\right).\, F\left(\frac{n_2}{pq}\right)$$

$$- \sum_{p,q,r} f(pqr)\, F\left(\frac{n_1}{pqr}\right).\, F\left(\frac{n_2}{pqr}\right) + \ldots$$

$p , q , r , \ldots$ étant les nombres premiers distincts qui divisent à la fois n_1 et n_2 .

La démonstration se fait par récurrence sur le nombre des facteurs premiers communs à n_1 et n_2 .

Nous utiliserons également l'identité

$$(3) \qquad \overline{\sigma}_0(1)\, \overline{\sigma}_0(2m-1) + \overline{\sigma}_0(3)\, \overline{\sigma}_0(2m-3) + \ldots + \overline{\sigma}_0(2m-1)\, \overline{\sigma}_0(1) = \sigma_1(m) ,$$

m entier impair.

Cette identité est équivalente à

$$3(r_2(1).r_2(2m-1) + r_2(3).r_2(2m-3) + \ldots + r_2(2m-1).r_2(1)) = 2r_4(2m) = 6r_4(m) ,$$

la vérification de cette dernière identité se fait en écrivant

$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2m$, et en prenant $x_1^2 + x_2^2 = 1 , 3 , 5 , \ldots 2m-1$.

On remarque d'abord que $r_3(r^{2\alpha_0} m^2) = r_3(m^2)$.

Pour $m \equiv 1 \pmod 4$, on a

$$2r_3(m) = 3(r_2(m) + 2r_2(m-4) + 2r_2(m-16) + \ldots)$$

(si $m = x_1^2 + x_2^2 + x_3^2$, on prend $x_1 = 0 , 2 , 4 , \ldots$, puis $x_2 = 0 , 2 , 4 , \ldots$, et $x_3 = 0 , 2 , 4 , \ldots$).

Donc, pour m impair quelconque,

$$2r_3(m^2) = 3(r_2(m^2) + 2r_2(m^2-4) + 2r_2(m^2-16) + \ldots)$$

soit

$$r_3(m^2) = 6 \sum_{j \in \underset{\sim}{Z}} \overline{\sigma}_0(m^2 - 4j^2)$$

On utilise ensuite le lemme,

$$\sum_{j \in \underset{\sim}{Z}} \overline{\sigma}_0(m^2-4j^2) = \sum_{j \in \underset{\sim}{Z}} \overline{\sigma}_0(m-2j)\,\overline{\sigma}_0(m+2j) - \sum_p \chi(p) \sum_{(p)} \overline{\sigma}_0(m'_p)\,\overline{\sigma}_0(m''_p)$$

$$+ \sum_{p,q} \chi(pq) \sum_{(pq)} \overline{\sigma}_0(m'_{pq})\,\overline{\sigma}_0(m''_{pq}) \ldots ,$$

$\sum_{(d)}$ étant étendue à toutes les solutions en entiers impairs positifs de

$$m'_d + m''_d = m/d .$$

L'identité (3) donne

$$r_3(m^2) = 6(\sigma_1(m) - \sum_p \chi(p)\,\sigma_1(\tfrac{m}{p}) + \sum_{p,q} \chi(pq)\,\sigma_1(\tfrac{m}{pq}) \ldots)$$

C'est bien l'identité d'Hurwitz.

BIBLIOGRAPHIE

[1] BATEMAN (P. T.). - A multiplicative function, Problem E-2051, Amer. math. Monthly, t. 76, 1969, p. 190-191.

[2] DIKSON (L. E.). - History of the theory of numbers, vol. 2. - New York, Chelsea Publ., 1952 (reprinted).

[3] HURWITZ (A.). - Sur la décomposition des nombres en cinq carrés, C. R. Acad. Sc. Paris, t. 98, 1884, p. 504-507.

[4] HURWITZ (A.). - Somme de trois carrés, Intermédiaire des Recherches mathématiques, t. 14, 1907, p. 106-107.

[5] SANDHAM (H. F.). - A square as the sum of 7 squares, Quart. J. Math., Oxford, Series 2, t. 4, 1953, p. 230-236.

[6] VENKOV (B. A.). - Elementary number theory. - Groningen, Wolters-Noordhoff publishing, 1970 (Wolters-Noordhoff Series of Monographs and Textbooks in pure and applied Mathematics).

(Texte reçu le 23 octobre 1972)

Jean LAGRANGE
Faculté des Sciences, Mathématiques
Moulin de la House
Boîte postale 347
51062 REIMS CEDEX