Séminaire Delange-Pisot-Poitou.
Théorie des nombres

Pierre Barrucand

Le problème de Waring et la méthode de Hardy (dissection de Farey)

Séminaire Delange-Pisot-Poitou. Théorie des nombres, tome 3 (1961-1962), exp. n^o 15, p. 1-34

<http://www.numdam.org/item?id=SDPP_1961-1962__3__A9_0>

Séminaire DELANGE-PISOT
(Théorie des nombres)
3e année, 1961/62, n° 15

21 mai 1962

LE PROBLÈME DE WARING ET LA MÉTHODE DE HARDY
[DISSECTION DE FAREY]

par Pierre BARRUCAND

1. - En 1625, GIRARD constatait que tout nombre est somme de quatre carrés parfaits (y compris, bien entendu, 1 et 0), et cette remarque fut reprise par BACHET en 1636. FERMAT s'intéressa au problème et prétendit avoir démontré cette propriété, mais, comme à son habitude, il ne publia pas sa preuve.

C'est seulement en 1770 que LAGRANGE, utilisant certains résultats partiels d'EULER, donna une démonstration de ce célèbre théorème. La même année, WARING, dans son ouvrage Meditationes algebraicae, avait affirmé que tout nombre est la somme de quatre carrés, neuf cubes, dix-neuf bicarrés et ainsi de suite (et sic deinceps). Il ne donna aucune preuve, et il est peu probable qu'il en ait trouvé une. La loi de formation n'est pas évidente, mais s'éclaire quand on sait qu'Euler montra que, de toute façon, si K est la partie entière de $\left(\frac{3}{2}\right)^k$ le nombre $2^k K - 1$ exige $2^k + K - 2$ puissances k-ièmes.

L'hypothèse de Waring s'énoncerait alors :

Tout nombre est somme de $g^*(k) = 2^k + K - 2$ puissances k-ièmes.

Sous cette forme elle n'est pas totalement démontrée, tout ce qu'on peut dire c'est qu'elle est possible et même très probable. En fait, on peut énoncer :

1° Tout nombre est somme d'un nombre $g(k)$ de puissances k-ièmes et $g(k) \geqslant g^*(k)$.

2° $g(k) = g^*(k)$ si $k = 2$, 3 ou est supérieur ou égal à 6 à la condition que $3^k - 2^k K \leqslant 2^k - K - 2$ et on ne connaît pas d'exemple pour lequel cette relation ne serait pas vérifiée.

3° Si $k = 4$ ou 5, $g(k)$ peut être égal à $g^*(k)$, en tous cas, $g(5) \leqslant 40$ et $g(4) \leqslant 35$.

Ce fut seulement en 1859 que LIOUVILLE démontra que tout nombre divisible par 6 est somme de 48 bicarrés, par suite tout nombre est somme de 53 bicarrés. La preuve est excessivement simple. Il suffit de vérifier que :

$$6(a^2 + b^2 + c^2 + d^2)^2 = (a + b)^4 + (a + c)^4 + (b + c)^4 + \dots$$
$$+ (a - b)^4 + (a - c)^4 + (b - c)^4 + \dots$$

Or, tout nombre est somme de quatre carrés.

On parvient facilement à améliorer ce résultat jusqu'à 41 bicarrés, plus difficilement jusqu'à 37 et il ne semble pas que l'on connaisse rien de mieux que 35. Pourtant, le calcul direct montre qu'on n'a jamais besoin de plus de 19 bicarrés, et il n'y a que six ou sept nombres dont le plus petit est 79 qui exigent réellement ce nombre de 19.

Que tout nombre soit somme de 9 cubes fut seulement prouvé au XXe siècle ; la première démonstration, due à WIEFERICH, était partiellement erronée et l'on ne connaît pas de preuve réellement simple.

On peut généraliser ainsi le théorème des quatre carrés : il existe des quadruplets (a, b, c, d) de nombres, tels que tout nombre n puisse être mis sous la forme (F) telle que $n = am_1^2 + bm_2^2 + cm_3^2 + dm_4^2$. Sous cette forme, il existe seulement 55 quadruplets vérifiant ce théorème, comme le prouve, en 1917, RAMANUJAN. Par exemple : $(1, 3, 3, 1)$, $(1, 2, 3, 5)$. Mais il existe aussi des quadruplets tels que tout nombre suffisamment grand, c'est-à-dire supérieur à une limite qui dépend du quadruplet, puisse être mis sous la forme (F). Prenons par exemple $(1, 1, 5, 5)$, seul le nombre 3 ne peut pas être représenté.

Pareillement, on connaît des groupes de 9 nombres tels que l'on ait toujours

$$n = \sum_{\nu=1}^{q} a_\nu n_\nu^3 .$$

Mais surtout, on peut montrer que tout nombre <u>suffisamment grand</u> est susceptible d'être mis sous la forme d'une somme de 7 cubes (LINNIK, 1942). En fait, seuls 23 et 239 exigent 9 cubes, et l'on ne connaît que 15 nombres dont le plus grand est 454, qui en demandent 8. Il est presque certain qu'à partir d'une certaine limite, 6 cubes suffisent. Le plus grand nombre exigeant 7 cubes est 8042, et sans doute le plus grand nombre exigeant 6 cubes est inférieur à 2 millions. Il y a plus que des présomptions qui font croire qu'en fait cinq et même quatre cubes suffisent. Dans ce dernier cas le dernier nombre exigeant cinq cubes pourrait être de l'ordre de 10^{14} ou moins.

On sait de même que tout nombre suffisamment grand est somme de 16 bicarrés ; et ce résultat, dans un sens ne peut être amélioré, car on connaît une suite infinie de nombres, soit $16^{\alpha}.31$ qui exigent 16 bicarrés. De même tout nombre suffisamment grand est somme de 23 puissances 5-ièmes et en général de $G(k)$ puissances k-ièmes.

Dans le sens contraire on sait que, de toutes façons, il y a un nombre infini de nombres qui ne peuvent être somme de k puissances k-ièmes ; cette proposition est due à MAILLET, donc $G(k) \geqslant k + 1$. Donc : tout nombre suffisamment grand est somme de $G(k)$ puissances k-ièmes, et $k + 1 \leqslant G(k) \leqslant g(k)$. En fait $G(k)$ est beaucoup plus petit que $g(k)$ car on sait que $G(k) = O(k \log k)$ (estimation due à VINOGRADOV). Dans quelques cas particuliers on peut montrer que $G(k)$ est supérieur à $k + 1$. Par exemple $G(6) \geqslant 9$, $G(2^n) \geqslant 2^{n+2}$.

On peut aussi chercher à déterminer la limite telle que presque tous les nombres soient sommes de $G_1(k)$ puissances k-ièmes, c'est-à-dire telle que la proportion des exceptions $< n$ décroisse quand n croît. Exemples : presque tous les nombres sont somme de 15 bicarrés et $G_1(4) = 15$ (en effet tout nombre $\equiv 15 (\mathrm{mod}\ 16)$ exige 15 bicarrés). Presque tous les nombres sont somme de quatre cubes et $G_1(3) = 4$, si $n \equiv \pm 4 (g)$, il faut quatre cubes, mais on admet que sans doute $G(3) = G_1(3) = 4$. Ces théorèmes sont dus à DAVENPORT.

On peut (mais presque rien n'a été fait dans ce sens, et c'est une des orientations possibles de nouvelles recherches) étudier la représentation comme somme de puissances de nombres satisfaisants à certaines conditions de congruence. Par exemple définir $g(k , \alpha , \mu)$ le nombre minimum de puissances k-ièmes nécessaires à représenter tous les nombres $\equiv \alpha(\mu)$. Ainsi $g(3 , \alpha , 9)$ sauf si $\alpha = 5$. On définira de la même façon $G(k , \alpha , \mu)$. Il y a des raisons de penser que, par exemple, $G(4 , \alpha , 16) \leqslant 9$ si $\alpha \leqslant 9$.

Il y a différentes généralisations du problème de Waring, par exemple :

1° Les sommes mixtes telles $m_1^2 + m_2^3 + m_3^3 = n$ (on sait que presque tous les nombres peuvent être représentés ainsi).

2° Les sommes de polynômes $n = \sum P_k(m_\nu)$.

3° Somme de puissances avec coefficients $n = \sum a_\nu\ m_\nu^k$; un exemple simple est donné par les formes quadratiques quaternaires (F) citées plus haut. Des formes cubiques particulièrement intéressantes sont $(1 , 1 , 2 , 2 , 3)$, $(1 , 1 , 2 , 3 , 4)$, $(1 , 1 , 2 , 3 , 3)$.

4° Représentation d'un entier d'un corps algébrique par une somme de puissances k d'entiers du même corps. Par exemple on connaît un théorème de Maass qui dit que "tout entier du corps $C(\sqrt{5})$ est somme de trois carrés entiers du même corps", il semble qu'il en soit de même pour les corps $C(\sqrt{2})$ et $C(\sqrt{3})$.

D'autres problèmes enfin, apparemment très distincts du problème de Waring, lui sont liés, plus ou moins, pour des raisons techniques. Nous en signalerons quelques-uns à la fin de cet exposé, un exemple intéressant est le problème de Kummer.

2. - Le théorème I fut démontré pour la première fois par HILBERT en 1909, sa démonstration, très compliquée, fut progressivement simplifiée, notamment par STRIDSBERG et REMAK. Cette preuve est très intéressante parce qu'elle est entièrement élémentaire, et peut-être est-elle trop oubliée, mais elle semble incapable de donner des renseignements numériques.

En 1919, G. H. HARDY et J. LITTLEWOOD devaient donner une démonstration tout à fait différente. Cette démonstration est fondée sur deux remarquables idées de Srinivasa RAMANUJAN.

La première est la découverte de séries très curieuses qui permettent le développement en séries de fonctions arithmétiques plus ou moins compliquées et qu'on appelle <u>séries singulières</u>. Ces séries se présentent sous la forme

$$\sum_{h(q)} \sum_{q=1}^{\infty} \delta_{h,q} \exp\left(\frac{-2\pi i n h}{q}\right)$$

où $\sum\limits_{h(q)}$ signifie que h décrit un système <u>réduit</u> de résidus modulo q , et où $\delta_{h,q}$ sont des coefficients définis par chaque couple h , q si $(h , q) = 1$. Par exemple pour la somme des diviseurs de n , on a

$$\sigma(n) = \frac{\pi^2}{6} n \sum_{h(q)} \sum_{q=1}^{\infty} \exp\left(\frac{-2\pi i n h}{q}\right) q^{-2}$$

c'est-à-dire que $\delta_{h,q} = q^{-2}$.

La seconde est une méthode permettant le calcul, au moins approximatif de certaines intégrales compliquées. Cette méthode appelée souvent méthode du cercle, ou dissection de Farey, a été sans doute le plus grand événement de la théorie des nombres de la première moitié du XXe siècle. Elle fut appliquée semble-t-il pour la première fois par HARDY et RAMANUJAN quand ils cherchèrent à évaluer asymptotiquement la fonction $p(n)$ définie par

$$\sum p(n)\, x^n = \prod_{n=1}^{\infty} (1 - x^n)^{-1} \quad .$$

Elle a permis la solution du problème de Waring et de diverses généralisations, mais aussi :

1° L'évaluation de coefficients à distribution irrégulière, par exemple

$$\sum_{\nu<n} \sigma_\alpha(\nu)\, \sigma_\beta(n-\nu) \quad \text{avec} \quad \sigma_\alpha(n) = \sum_{d \| n} d^\alpha$$

$$\sum d(\nu)\, d(n-\nu) \quad \text{avec} \quad d(n) = \sum_{d|n} 1$$

$$\sum d(\nu)\, d_3(n-\nu) \quad \text{avec} \quad \sum d_3(n)\, n^{-3} = \zeta^3(s)$$

2° Des progrès considérables dans l'étude du problème de Goldbach.

3° Sous certaines hypothèses, l'évaluation du nombre de couples de nombres premiers différents de 2α et inférieurs à n, quoique la théorie soit fort peu avancée.

4° Solution du problème des partitions (RAMANUJAN, RADEMACHER, ISEKI).

5° Représentation d'un nombre par une forme quadratique, telle (F) .

6° Sommes, telles $\sum_{n<N} d(n)\, d(n+\ell) = \Phi(N , \ell)$.

Il est très intéressant d'observer que cette méthode est le résultat de la collaboration de deux hommes de formation bien distincte, un mathématicien classique G. H. HARDY et un autodidacte imaginatif RAMANUJAN, un exemple particulièrement instructif en faveur de la collaboration d'hommes de formation et d'esprit différents et qui se complètent par leurs différences mêmes.

3. – Adoptons d'emblée quelques conventions :

p , p' , ϖ désignent des nombres premiers,

n , m , h , q , s , k des nombres entiers,

x , x' , y , z des nombres quelconques complexes (ou réels),

ρ un nombre complexe de faible amplitude,

u un nombre réel.

Rappelons maintenant quelques propriétés très classiques des fonctions elliptiques et modulaires. Soient K et K' les "périodes" d'un système de fonctions elliptiques de Jacobi de module u ,

$$\exp\left(-\frac{\pi K'}{K}\right) = x$$

et

$$\exp\left(-\frac{\pi K}{K'}\right) = x' \quad ,$$

$$x' = \exp\left(-\frac{\pi^2}{y}\right) = \exp\left(+\frac{\pi^2}{\log x}\right) \quad ,$$

$$y = -\log x \quad .$$

On a

$$\theta(x) = \left|\sqrt{\frac{2K}{\pi}}\right| = 1 + \sum_1^\infty 2x^{n^2} \quad , \quad \theta(x') = \left|\sqrt{\frac{2K'}{\pi}}\right| \quad .$$

La série de Taylor définissant $\theta(x)$ étant lacunaire, le cercle unitaire est pour elle une ligne de singularité essentielle ou une "coupure" au-delà de laquelle il n'y a pas de prolongement analytique. Mais quelle est l'allure de $\theta(x)$ au voisinage de ce cercle. Des relations précédentes on déduit

$$\text{(A)} \qquad \theta(x) = \sqrt{\frac{\pi}{y}}\,\theta(x') \quad .$$

Si x tend le long de l'axe positif vers $+1$, x' devient absolument infime et, par suite,

$$\theta(x) \sim \left|\sqrt{\frac{\pi}{y}}\right| \quad .$$

D'autre part la relation fonctionnelle A est valable quel que soit x , pourtant si on l'applique à un x complexe dont l'amplitude n'est pas suffisamment petite la convergence de $\theta(x')$ diminue rapidement. Supposons maintenant

$$x = \rho \exp \frac{2\pi i h}{q} = \rho^{\tau} \quad ;$$

alors

$$\theta(x) = -1 + \sum_{\ell=0}^{q-1} \tau^{\ell^2} \sum_{m=0}^{\infty} \rho^{(mq+\ell)^2} \quad .$$

Par certaines transformations, on est amené alors à

$$\theta(x) = \frac{S_{h,q}}{q}\sqrt{\frac{\pi}{-\log \rho}} + 2 \sum_{m=1}^{\infty} \frac{S_{h,q,m}}{q}\sqrt{\frac{\pi}{-\log \rho}} \exp\left(\frac{\pi^2 m^2}{q \log \rho}\right) \quad ,$$

avec

$$S_{h,q} = \sum_{n=0}^{q-1} \exp \frac{2\pi i h n^2}{q} \quad ; \qquad S_{h,q,m} = \sum_{n=0} \exp\left(\frac{2\pi i h n^2}{q}\right) \cos \frac{2\pi m n}{q}$$

ce qui fait qu'aux environs du point rationnel $\exp \frac{2\pi i h}{q}$, on a

$$\theta(x) \sim \frac{S_{h,q}}{q}\sqrt{\frac{\pi}{-\log \rho}} \quad .$$

Supposons maintenant que nous parcourions un cercle de centre 0 et de rayon voisin de 1 . Si q n'est pas trop grand $\frac{S_{h,q}}{q}\sqrt{\frac{\pi}{-\log \rho}}$ est une excellente approximation de la fonction, mais si q devient grand, notre estimation ne tient plus aussi bien, tout d'abord parce que $S_{h,q} = O(q^{1/2})$, donc $\frac{S_{h,q}}{q} = O(q^{-1/2})$ ensuite parce que q , en dénominateur dans les exponentielles, rend les termes correspondants plus grands. Mais si nous parcourons le rayon $(0 \ , \exp \frac{2\pi i n}{q})$, la formule d'approximation $\sqrt{\frac{\pi}{-\log \rho}}$ tient aux environs immédiats du point $\exp \frac{2\pi i h}{q}$.

Enfin si nous parcourons le cercle le long d'un rayon menant à un point irrationnel, le comportement de la fonction sera très compliqué et dépend d'ailleurs de la nature arithmétique de ce point [1].

Maintenant, en général, une expression comme $(\log x)^{-\alpha}$ est peu maniable, mais aux environs du point 1 on peut la remplacer asymptotiquement par la fonction $\frac{Z(x\ ,\ 1-\alpha)}{\Gamma(\alpha)}$, car $(\log x)^{-\alpha} - \frac{Z(x\ ,\ 1-\alpha)}{\Gamma(\alpha)}$ est régulière aux environs du point 1.

La fonction Z est définie par

$$Z(x\ ,\ s) = \sum_{1}^{\infty} \frac{x^n}{n^s} \quad ,$$

en particulier

$$Z(x\ ,\ 0) = \frac{x}{1-x} \quad ,$$

$$Z(x\ ,\ -1) = \frac{x}{(1-x)^2}$$

et en général

$$Z(x\ ,\ -h) = \frac{xP(x)}{(1-x)^{h+1}} \quad ,$$

$P(x)$ étant un polynôme.

Nous pouvons alors représenter asymptotiquement $\theta(x)$ aux environs du point $\exp\frac{2\pi ih}{q}$ par $C(h\ ,\ q)\ Z(x \exp\frac{-2\pi ih}{q}\ ,\ \frac{1}{2})$ où $C(h\ ,\ q)$ est un coefficient.

Nous allons généraliser ces résultats. Posons

$$\theta_k(x) = 1 + 2\sum_{1}^{\infty} x^{n^k} \ ; \qquad \theta_k(x) = 1 + 2\sum_{1}^{\infty} \exp(-n^k y) \quad ,$$

$\theta_k(x)$ étant lacunaire admet le cercle unité comme coupure. Maintenant, par la formule sommatoire de Poisson :

---

[1] Il est un peu plus simple si ce point est un irrationnel <u>quadratique</u>.

$$\theta_k(x) = 2\int_0^\infty \exp(-z^k y)\,dz + 4\sum_{m=1}^{\infty}\int_0^\infty \exp(-z^k y)\cos 2\pi mz\,dz ,$$

$$\theta_k(x) = 2\Gamma(1+\frac{1}{k})\,y^{-1/k} + 4y^{-1/k}\sum_{m=1}^{\infty}\varphi_k(2\pi m y^{-1/k})$$

avec

$$\varphi_k(t) = \int_0^\infty \exp(-z^k)\cos tz\,dz .$$

Des expressions asymptotiques de $\varphi_k(t)$ sont connues, en particulier celles de BURWELL et celles de BAKHOOM, l'approximation pour $\theta_k(x)$ aux environs du point 1 le long du rayon réel $2\Gamma(1+\frac{1}{k})\,y^{-1/k}$ est très bonne si k est pair, un peu moins si k est impair.

Si nous voulons étudier l'allure de $\theta_k(x)$ le long d'un rayon dirigé vers un point rationnel, il faut transformer notre formule qui devient

$$\theta_k(x\exp\frac{2\pi ih}{q}) = 2\Gamma(1+\frac{1}{k})\,y^{-1/k}\,\frac{S_{k,h,q}}{q} + 4\sum_{m=1}^{\infty}\frac{S_{k,h,q,m}}{q}\,y^{-1/k}\,\varphi_k(\frac{2\pi m}{qy^{1/k}})$$

$$+ 4\sum_{m=1}^{\infty}\frac{S^*_{k,h,q,m}}{q}\,y^{-1/k}\,\varphi^*_k(\frac{2\pi m}{qy^{1/k}})$$

$$\varphi^*_k(t) = \int_0^\infty \exp(-z^k)\sin tz\,dz ;$$

$$S_{k,h,q} = \sum_{n=0}^{q-1}\exp(\frac{2\pi in^k h}{q}) ,$$

$$S_{k,h,q,m} = \sum_{n=0}^{q-1}\exp(\frac{2\pi in^k h}{q})\cos\frac{2\pi nm}{q} ,$$

$$S^*_{k,h,q,m} = \sum_{n=0}^{q-1} \exp\left(\frac{2\pi i n^k h}{q}\right) \sin\frac{2\pi n m}{q} \quad .$$

Si k est pair S^* est identiquement nul, et la formule se simplifie comme dans le cas $k = 2$.

De tout cela nous pouvons déduire facilement qu'aux environs du point $\exp\frac{2\pi i h}{q}$

$$\theta_k(x) = 2\Gamma\left(1 + \frac{1}{k}\right) \frac{S_{k,h,q}}{q} (-\log \rho)^{-1/k} \quad .$$

Il est maintenant clair qu'aux environs des points rationnels

$$\theta_k^s(x) = \frac{2^s\,\Gamma^s\left(1 + \frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \frac{S^s_{k,h,q}}{q^s} Z\left(x \exp\frac{-2\pi i h}{q} , 1 - \frac{s}{k}\right) \quad .$$

Maintenant nous pouvons toujours définir formellement

$$\theta_k^*(x , s) = \frac{2^s\,\Gamma^s\left(1 + \frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)} \sum_{h(q)} \sum_{q=1}^{\infty} \frac{S^s_{k,h,q}}{q^s} Z\left(x \exp\frac{-2\pi i h}{q} , 1 - \frac{s}{k}\right) \quad .$$

Si nous supposons que, pour quelques s et k , la convergence absolue est assurée, nous avons

$$\theta_k^*(x , s) = \sum \rho(k , s , n)\, x^n \quad \text{avec} \quad A_q(n) = \sum_{h(q)} \frac{S^s_{k,h,q}}{q^s} \exp\left(\frac{-2\pi i n h}{q}\right)$$

$$\rho(k\ ,\ s\ ,\ n) = \frac{2^s\,\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})}\, n^{(s/k)-1} \sum_{h(q)} \sum_{q=1}^{\infty} \frac{S^s_{k,h,q}}{q^s} \exp\left(\frac{-2\pi inh}{q}\right)$$

$$\rho(k\ ,\ s\ ,\ n) = \frac{2^s\,\Gamma(1+\frac{1}{k})^s}{\Gamma(\frac{s}{k})}\, n^{(s/k)-1}\ \mathfrak{S}(n) \qquad ;$$

$$\mathfrak{S}(n) = \sum_{q=1}^{\infty} A_q(n) \qquad .$$

Et si nous pouvons définir $\theta^*_k(x\ ,\ s)$, cette fonction et $\theta^s_k(x)$ sont asymptotiquement équivalentes aux environs des points rationnels.

Pour le moment notre raisonnement est tout à fait formel. Néanmoins il amène à une définition intéressante : celle de la série singulière attachée à une fonction ayant un certain comportement aux environs des points rationnels.

4. - Maintenant beaucoup de propriétés relatives aux sommes de Gauss ([2]) sont connues.

La formule-clef est

$$S_{h,qq'} = S_{hq^{k-1},q'} \times S_{hq'^{k-1},q} \quad \text{si} \quad (q\ ,\ q') = 1 \qquad .$$

Il suffit donc de pouvoir calculer S_{h,p^α}

Maintenant si $(p\ ,\ k) = 1$, c'est-à-dire si $p \nmid k$

$$S_{h,p^{\mu k}} = p^{\mu(k-1)} \ , \qquad S_{h,p^{\mu k+\beta}} = S_{h,p^{\mu k}} \times S_{h,p^\beta}$$

([2]) L'indice k sera omis quand il n'est pas nécessaire à la compréhension du texte.

et

$$S_{h,p^\beta} = p^{\beta-1} \quad \text{si} \quad 2 \leqslant \beta \leqslant k \quad .$$

On est donc amené à déterminer les S_{h,p^α} si $p|k$, et les $S_{h,p}$.

1° Si k est impair et si $(p-1, k) = 1$, $S_{h,p} = 0$.

2° Si k est pair et si $(p-1, k) = 2$, $S_{h,p}$ se réduit à la somme $S_{2,h,p}$ et plus généralement si $(p-1, k) = \delta$, $S_{k,h,p}$ se réduit à la somme $S_{\delta,h,p}$.

Il ne semble pas que des règles absolument générales aient été données par le cas $p|k$ qui est compliqué, surtout si $p = 2$.

Supposons maintenant que $k|p-1$; on peut toujours construire un système de caractères primitifs χ modulo p et de puissance k-ième, c'est-à-dire que $\chi(n+p) = \chi(n)$, $\chi(nn') = \chi(n)\,\chi(n')$ et $\chi(0) = 0$, enfin $\chi(n)$ est une racine primitive de l'unité si n est une racine primitive modulo p .

On a

$$\sum \chi(n) \exp \frac{2\pi inh}{p} = T_1(h, p)$$

$$\sum \chi^\alpha(n) \exp \frac{2\pi inh}{p} = T_\alpha(h, p)$$

et

$$S_{k,h,p} = \sum_{\alpha=1}^{k-1} T_\alpha(h, p) \quad .$$

Or il est facile de montrer

$$|T_\alpha(h, p)| = |\sqrt{p}| \quad ,$$

donc

$$|S_{h,p}| \leqslant (h-1)|\sqrt{p}| \quad .$$

Il y a d'ailleurs k valeurs possibles de $S_{h,p}$ selon la valeur de $\chi(h)$ dans le système de caractères primitifs adopté, c'est-à-dire que si $\chi(h) = \chi(h')$, $S_{h,p} = S_{h',p}$.

Règles particulières pour $S_{2,h,p}$:

1° $S_{h,2} = 0$, $S_{h,4^{\mu}} = 2^{\mu}(1 + i^{h})$, $S_{h,2^{2\mu+1}} = 2^{\mu+1} \exp \frac{\pi i h}{4}$

2° $S_{h,p} = (\frac{h}{p}) S_{1,p}$ si $p \neq 2$.

$S_{h,p}$ est racine de $x^2 - p^* = 0$ avec $p^* = (\frac{-1}{p})p$, donc $p^* \equiv 1(4)$.

En conclusion si q n'a pas de facteur cubique et si $(q , k) = \frac{1}{k}$,

$$S_{k,h,q} < d_k(q) \, |\sqrt{q}| \quad \text{avec} \quad \zeta^k(s) = \sum_1^{\infty} d_k(n) \, n^{-s} \qquad ,$$

$\zeta(s)$ étant la fonction de Riemann.

Reste le cas des sommes $S_{h,q,m}$ et $S^*_{h,q,m}$, or très peu de choses sont connues. Cependant, bien après les premiers travaux de HARDY et LITTLEWOOD, Loo Keng HUA a publié la relation

$$S_{h,q,m} = O(q^{(k-1)/k}) \ , \qquad S^*_{h,q,m} = O(q^{(k-1)/k})$$

et il semble surtout que l'on puisse attendre beaucoup de certaines relations découvertes par André WEIL ([3]). Signalons tout de suite que le cas $k = 2$ ne pose pas de difficulté grave et que les cas $k = 3$ et $k = 4$ sont sans doute beaucoup plus abordables que si $k \geqslant 5$.

Les règles que nous venons d'énumérer permettent déjà de préciser certaines règles de convergence pour la série $\theta^*(x , s , k)$ sur lesquelles on pourra revenir, en tout cas il est clair qu'il y a toujours une valeur s_0 pour laquelle, pour tout $s \geqslant s_0$, $\theta^*_k(s , x)$ converge.

([3]) Voir à ce sujet :

CARLITZ (L.) and UCHIYAMA (S.). - Bounds for exponential sums, Duke math. J., t. 24, 1957, p. 37-41.

5. - A chaque nombre fractionnaire h/q faisons correspondre le point $\exp \frac{2\pi i h}{q}$ ou $P_{h,q}$. On appelle suite de Farey d'ordre N l'ensemble des nombres fractionnaires irréductibles compris entre 0 et 1 et dont le dénominateur est $\leq N$. Ces nombres fractionnaires étant rangés par ordre de grandeur. Par exemple, la suite de Farey d'ordre 4 est $0, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, 1$. On sait que si h/q et h'/q' sont deux termes successifs d'une suite de Farey, on a $h'q - hq' = 1$. Considérons maintenant les points médiants situés chacun entre deux termes consécutifs $\frac{h}{q} + \frac{1}{q(q+q')}$, et faisons correspondre à chacun de ces médiants un point $P^*_{h,q}$ on voit que le point $P_{h',q'}$ est situé toujours entre $P^*_{h,q}$ et $P^*_{h',q'}$. Chaque point P se trouve à l'intérieur d'un segment $j_{h,g}$ limité par deux points médiants P^*, et le cercle est complètement divisé, sans hiatus, par ces segments. De plus les fractions $\frac{1}{q(q+q')}$ vérifient toujours

$$\frac{1}{2qN} < \frac{1}{q(q+q')} < \frac{1}{qN}$$

ce qui donne à la distribution des segments une régularité relative.

Considérons maintenant l'intégrale

$$I = \frac{1}{2\pi i} \int_C F(x)\, dx \qquad ,$$

le contour étant fermé sans point double et intérieur à une coupure cirulaire.

Nous pouvons décomposer cette courbe fermée en segments correspondants ~~aux arcs~~ de Farey que nous venons de définir et poser alors

$$2\pi i I = \sum_{\substack{h,q \\ q\leq N}} \int F(x)\, dx = 2\pi i \sum I_{h,q} \qquad .$$

Il serait très difficile d'apprécier exactement chaque intégrale partielle $I_{h,q}$, mais on peut lui substituer une valeur approchée et estimer le terme d'erreur

$$I_{h,q} = J_{h,q} + J^*_{h,q} \qquad ;$$

on a alors

$$I = \sum_{h,q} J_{h,q} + \sum_{h,q} J^*_{h,q} = J_N + J^*_N \quad .$$

Dans certains cas particuliers on peut montrer que J^*_N tend vers 0 quand N croît ; dans d'autres cas on peut estimer l'ordre de grandeur de J^*_N ou lui fixer une borne.

La difficulté est alors de choisir le contour, et l'ordre N de façon aussi avantageuse que possible et d'évaluer aussi précisémment que possible l'ordre de grandeur de J^*_N .

Considérons maintenant la fonction $\theta_k(x)$ et soit $\theta^s_k(x) = \sum z(n)\, x^n$ et $z(n) = z_{k,s}(n)$ s'il y a équivoque ; $z(n)$ représente le nombre de représentations de n comme somme de s puissances k-ièmes - avec la convention, si k est pair, que l'on considère comme distinctes les représentations qui diffèrent par l'ordre et le signe. Cette convention subsiste pour k impair, si l'on parle de modules de puissances.

Nous avons donc $$z(n) = \int \theta^s(x) \frac{dx}{x^{n+1}} \quad .$$

HARDY et LITTLEWOOD adoptent pour contour un cercle de rayon $1 - \frac{1}{n}$ ou $\exp \frac{-1}{n}$ (la différence est négligeable), et pour ordre de la dissection de Farey, défini plus haut, $N = [n^{(k-1)/k}]$. Ils ne donnent aucun argument tendant à faire croire que ce sont là les meilleurs choix possibles. En fait dans des problèmes voisins on a été amené à utiliser d'autres contours avec succès.

De plus ils opposent arcs majeurs et arcs mineurs ; pour un arc majeur $q \leqslant n^{1/k}$ pour un arc mineur $q > n^{1/k}$. La raison de cette distinction est assez claire. Il s'agit d'exprimer de façon aussi simple que possible l'allure de la fonction $\theta_k(x)$ le long du cercle d'intégration. Dans le cas des arcs majeurs, la relation fonctionnelle donne une approximation rapide de la fonction $\theta_k(x)$, dans le cas des arcs mineurs au contraire, la relation fonctionnelle, quoique correcte, est peu utilisable et on peut se contenter d'estimer directement la fonction à partir de sa série de Taylor limitée à quelques termes. On doit observer que la distinction entre arcs majeurs et arcs mineurs est liée aux modalités techniques adoptées par le calcul, qu'elle n'a rien d'absolu et qu'elle dépend, non seulement de N , mais du contour choisi.

Sur les arcs majeurs on va voir que la fonction est réellement dominée par le terme $2\Gamma(1+\frac{1}{k})\,\frac{S_{h,q}}{q}\,(-\log\rho)^{-1/k}$, mais ce n'est plus le cas pour les arcs mineurs, tant à cause de la convergence médiocre de la série que du rôle du dénominateur q.

Posons $C = 2\Gamma(1+\frac{1}{k})$, le long d'un arc majeur on peut écrire

$$\theta_k(x) = C\,\frac{S_{h,q}}{q}\,(-\log\rho)^{-1/k} + \psi_{h,q} \quad .$$

Il faut estimer l'ordre de grandeur de $\psi_{h,q}$ qui dépend à la fois de celui des sommes $S_{h,q,m}$, $S^*_{h,q,m}$ et du comportement asymptotique des fonctions $\varphi_k(x)$ et φ^* que nous avons définies. Sur le rayon $(0\ ,\ \exp\frac{2\pi ih}{q})$ la contribution des φ et φ^* est très faible, mais aux extrémités de l'arc elle est plus importante.

Pour évaluer $S_{h,q,m}$, HARDY et LITTLEWOOD utilisent une estimation assez médiocre

$$T = \sum_{z=0}^{q-1} \exp\frac{2\pi i}{q}\,(hz^k + h_1\,z^{k+1} + \dots) = O(q^{k^*})$$

avec $k^* = 1 - 2^{-k+1}$.

Cette formule est dérivée du théorème dit des <u>sommes de Weyl</u>. Nous savons qu'en réalité $T = O(q^{(k-1)/k})$. Combinant cette évaluation avec une formule asymptotique pour Φ , ils obtiennent finalement la formule

$$\theta_k(x) = C\,\frac{S_{h,q}}{q}\,(-\log\rho)^{-1/k} + O(q^{k^*/k}) \quad .$$

Dans le cas $k \equiv 1(2)$, une légère complication se produit ; en effet, la somme $S_{k,h,q,m}$ est toujours réelle et la somme S^* toujours imaginaire, et il est avantageux d'écrire

$$\frac{1}{q}\,\varphi^*\Big(\frac{2\pi m}{q(-\log\rho)^{1/k}}\Big) = \varphi^{**} + \frac{1}{2\pi m} \quad .$$

On a donc

$$\theta_k(x) = C\,\frac{S_{h,q}}{q}\,(-\log\rho)^{-1/k} + \psi^*_{h,q} + \tilde{\varepsilon}_{h,q}$$

avec

$$\tilde{\varepsilon}_{h,q} = \frac{2}{\pi}\sum \frac{S^*_{k,q,m}}{m} \qquad .$$

La contribution du nombre imaginaire pur $\varepsilon_{h,q}$ n'est pas importante, mais il est intéressant à envisager, quand on considère l'allure de la fonction $\theta_k(x)$ au voisinage du cercle unité. Mais rien ne semble connu de ces nombres $\tilde{\varepsilon}_{h,q}$.

Arcs mineurs. - HARDY et LITTLEWOOD commencent par établir un lemme.

Si

$$n^{(1/k)-\eta} < q < n^{1-(1/k)+\eta} \quad \text{et} \quad 0 < \mu < n^{(1/k)+\zeta}$$

$$\sum_{m=0}^{\mu} \exp\left(\frac{2\pi i}{q}\, hm^k\right) = O\left(n^{(k^*/k)+\lambda}\right) \qquad ,$$

λ pouvant être calculé en fonction de η et de ζ .

De bien meilleurs résultats sont connus. Par exemple MORDELL a montré que

$$\sum_{m=0}^{\mu} \exp\left(\frac{2\pi i h}{q}\, m^k\right) = \frac{\mu}{q}\, S_{k,h,q} + O\left(q^{(3/4)+\varepsilon}\right) \qquad .$$

D'autre part

$$\theta_k(x) = -1 + 2\sum_{0}^{\omega} x^{m^k} + 2\sum_{\omega+1}^{\infty} x^{m^k} = 1 + \theta_1 + \theta_2$$

avec

$$\omega = n^{(1/k)+\zeta} \quad \text{et} \quad \theta_a = o(1) \qquad .$$

Il nous reste à calculer maintenant l'intégrale

$$\frac{1}{2\pi i} \int_{j_{h,q}} \frac{\theta_k^s(x)}{x^{n+1}}\, dx = I_{h,q}(n)$$

en sorte que

$$\sum_{h,q} I_{h,q}(n) = z(n) \qquad ;$$

on trouve

$$I_{h,q}(n) = \frac{S_{h,q}^s}{q^s} \frac{C^s}{\Gamma(s/k)}\, n^{(s/k)-1} \exp(-\, 2\pi i n^k/q) \;+\; O(q^{(sk^*/k)+\varepsilon})$$

et finalement

$$z_{k,s}(n) = \frac{C^s}{\Gamma(s/k)}\, n^{(s/k)-1}\, \mathfrak{S}(n) + O(n^{sk^*/k}) \qquad .$$

Le terme $O(n^{sk^*/k})$ est négligeable tant que $s > k2^{k-1}$, mais l'estimation est très grossière.

Loo Keng HUA a pu, en raffinant, ramener cette limite à 2^k .

Dans le cas $k = 2$, il est facile d'obtenir

$$z_{2,s}(n) = \frac{\pi^{s/2}}{\Gamma(s/2)}\, n^{(s/a)-1}\, \mathfrak{S}(n) + O(n^{s/4}) \qquad .$$

Signalons enfin qu'une méthode très puissante, mais très compliquée, d'estimation de sommes trigonométriques est due à VINOGRADOV, mais elle exigerait trop de commentaires et est hors de notre sujet, citons seulement le résultat

$$g(k) = O(k \log k) \quad .$$

Théorie de la série singulière. - Il nous faut étudier maintenant la série singulière. Pour cela nous rappellerons d'abord un théorème d'André GUINAND qui n'est pas indispensable, mais qui aide à comprendre certaines questions.

Si

$$A_{h,q} = \sum_1^q \frac{B_{h,q}}{\sqrt{q}} \exp\left(\frac{2\pi inh}{q}\right) \quad ,$$

$$B_{h,q} = \sum_1^q \frac{A_{h,q}}{\sqrt{q}} \exp\left(- \frac{2\pi inh}{q}\right) \quad .$$

Cette relation de réciprocité est une forme particulière de la loi générale de réciprocité de Fourier.

On voit que les suites $A_q(n)$ et $S^s_{k,n,q}$ sont ainsi rapprochées.

Il nous faut rappeler aussi le théorème de factorisation

$$\zeta(s) = \sum_1^\infty n^{-s} = \prod_p (1 - p^{-s})^{-1} \quad \text{si} \quad R(s) > 1 \quad ;$$

soit

$$\zeta(s) = \prod_p \overline{\xi}(p \, , \, s) \quad .$$

Considérons maintenant les sommes

$$A_q(n) = \sum_{h(q)} \left(\frac{S_{h,q}}{q}\right)^s \exp - \frac{2\pi inh}{q} \quad .$$

THÉORÈMES.

1° Si $(q \, , \, q') = 1$

$$A_q(n)\ A_{q'}(n) = A_{qq'}(n)$$

la conséquence immédiate est que si [4]

$$\xi(p\ ,\ n) = 1 + \sum_{\nu=1}^{\infty} A_{p^\nu}(n) \qquad ,$$

alors

$$\sigma(n) = \prod_p \xi(p\ ,\ n) \qquad .$$

2° Supposons maintenant que $p \nmid k$ et $p^c | n$ et $p^{c+1} \nmid n$, $\beta < k$.

$$A_{p^\alpha}(n) = 0 \quad \text{si} \quad \alpha > c + 1$$

$$A_{p^\alpha}(n) = 0 \quad \text{si} \quad p \nmid n \quad \text{et} \quad \alpha > 1$$

$$\xi(p\ ,\ n) = 1 + A_p(n) \quad \text{si} \quad p \nmid n\ ,\quad p \nmid k$$

$$A_{p^{k\alpha+\beta}} = p^{\alpha(k-s)}\ A_{p^\beta}\ (\frac{n}{p^{\alpha k}})$$

$$\begin{aligned} A_{p^\beta}(n) &= 0 \quad \text{si} \quad \beta > c + 1 \\ &= -\ p^{\beta-s-1} \quad \text{si} \quad \beta = c + 1 \\ &= (p - 1)\ p^{\beta-s-1} \quad \text{si} \quad \beta < c + 1 \end{aligned}$$

---

[4] On notera la similitude avec la factorisation de $\zeta(s)$.

$$A_{p^{k\alpha}}(n) = 0 \quad \text{si} \quad \alpha k > c + 1$$

$$= - p^{\alpha(k-s)-1} \quad \text{si} \quad k = c + 1$$

$$= (p - 1)\, p^{\alpha(k-s)-1} \quad \text{si} \quad k < c + 1$$

si $p | k$, les formules sont plus complexes, mais si $c = k\alpha + \mu$ et $p^{\lambda} | k$, $p^{\lambda+1} \not| k$,

$$A_{p^{\gamma}}(n) = 0 \quad \text{si} \quad \gamma > \max(c + 1 \,, \; k\alpha + \lambda + 1) \,, \quad p \neq 2$$

$$A_{2^{\gamma}}(n) = 0 \quad \text{si} \quad \gamma > \max(c + 1 \,, \; 2\alpha + \lambda + 2) \quad .$$

Ce qui fait que dans tous les cas les séries $\xi(p , n)$ sont finies, les diviseurs de kn sont évidemment en nombre fini et

$$\text{si} \quad p \not| n \qquad |A_p(n)| < Cp^{\frac{1}{2}-\frac{s}{2}}$$

$$\text{si} \quad p | n \qquad |A_p(n)| < Cp^{1-\frac{s}{2}} \quad .$$

Pour simplifier les choses on observera que

$$A_p(n) = 0 \quad \text{si} \quad (p - 1 \,, k) = 1 \quad \text{et} \quad p \not| n$$

$$\mathfrak{S}(n) = \prod_{p | kn} \xi_p(n) \prod_{\substack{p \not| kn \\ (p-1,k)>1}} [1 + A_p(n)] \quad .$$

Conséquence : La série singulière est absolument convergente si $s \geqslant 4$.

Remarque : Nous ne savons pas, en général, calculer $A_p(n)$.

Interprétation arithmétique de la série singulière. - Nous allons maintenant généraliser le problème de Waring à un système de résidus de congruence, c'est-à-dire à un corps fini.

Il s'agit de trouver le nombre de solutions de l'équation

$$\sum_{\alpha=1}^{\alpha=s} m_\alpha^k \equiv n \pmod q \quad .$$

Or HARDY et LITTLEWOOD ont trouvé

$$\sum_{\alpha=0}^{\mu} A_{p^\alpha}(n) = p^{\mu(1-s)} M(p^\mu , n) \quad .$$

Maintenant, soit $p^c | n$, $p^{c+1} \nmid n$, la série $\xi(p , n)$ a tous ses termes nuls à partir de $c + \beta$, β étant égal à 2 si $p \nmid k$, sinon β est un peu plus compliqué, donc

$$\mathfrak{S}(n) = \prod_p p^{(c+\gamma)(1-s)} M(p^{(\gamma+c)} , n)$$

et

$$\mathfrak{S}(n) = n^{1-s} \prod_p p^{\gamma(1-s)} M(p^{c+\gamma} , n) - \gamma$$

est facile à déterminer, en particulier si $p \nmid kn$, $\gamma = 1$.

On observera que si, quel que soit p , $\xi(p , n)$ est nul, non seulement $\mathfrak{S}(n)$ est nul, mais aussi $z_{k,s}(n)$ ce qui suggère une représentation

$$z(n) = \rho(n)[1 + \alpha_{k,s}(n)] \quad ;$$

enfin nous avons

$$\rho(n) = \frac{C^s}{\Gamma(s/k)} n^{((1-k)/k)s} \prod p^{\gamma(1-s)} M(p^{c+\gamma} , n) \quad .$$

Cette interprétation arithmétique de $\rho(n)$ que HARDY et LITTLEWOOD n'ont pas explicitée n'est pas éblouissante, mais elle a l'intérêt de montrer que la série singulière n'est pas un simple artifice mathématique, mais est liée à la nature arithmétique du problème, et qu'elle est susceptible d'une définition arithmétique assez obscure.

Hypothèse K. - HARDY et LITTLEWOOD ont montré que si

$$z_{k,k}(n) = O(n^{\varepsilon}) \quad .$$

Alors presque tous les nombres sont somme de $k + 1$ puissances K, sauf quant à des conditions de congruence, et tous les nombres suffisamment grands sont sommes de $2k + 1$ puissances.

L'histoire de l'hypothèse K est curieuse. Elle est vraie si $k = 2$ et fausse si $k = 3$, et MAHLER, qui démontra la fausseté de l'hypothèse dans ce cas, en conclut que "même pour $k = 3$ elle est fausse". Pourtant le raisonnement de MAHLER est hâtif car $\rho_{k,k}(n) = O(n^{\varepsilon})$ si $k \geqslant 3$, mais $\rho_{3,3}(n)$ correspond à une série formelle qui ne semble pas converger, du moins absolument. Curieusement, dans ce cas $k = 3$, il est vrai que $G(k) \leqslant 7$, $G_1(k) = 4$.

D'autre part, on sait que $z_{k,k}(n) = O(\log \log n)$. En association de ce problème on peut se demander "Combien y a-t-il de nombres inférieurs à n et susceptibles d'être somme de k puissances k ? Soit $V_k(n)$ ce nombre. Si $k = 2$, on sait que $v_2(n) \sim \frac{Cn}{\sqrt{\log n}}$. Si $k > 2$, on ne sait que très peu de choses.

Cependant DAVENPORT a obtenu

$$v_3(n) = O(n^{(13/15)-\varepsilon})$$

$$v_4(n) = O(n^{(19/24)-\varepsilon})$$

$$v_5(n) = O(n^{(7/8)+\varepsilon}) \quad .$$

D'autre part aucune limite supérieure n'est connue, croyons-nous. On peut supposer

$$v_k(n) = o(n) \quad .$$

<u>Autres applications de la dissection de Farey.</u> - Nous allons maintenant considérer des fonctions tout à fait différentes. Soit

$$\lambda_u(x) = \sum n^u \frac{x^u}{1 - x^u} = \sum \sigma_u(n)\ x^n \qquad ,$$

avec $\sigma_u(n) = \sum\limits_{d|n} d^u$ avec $u \neq 0$.

Nous avons

$$\sigma_{-u}(n) = \sigma_u(n)$$

et

$$n\frac{x^n}{1 - x^n} = \sum_{d|n} F_d(x) \quad \text{avec} \quad F_d(x) = \sum_{h(d)} \frac{x \exp(-(2\pi i h)/q)}{1 - x \exp(-(2\pi i h)/q)} \qquad .$$

Partant, si u est <u>négatif</u>,

$$\lambda_u(x) = \sum_{h(d)} \sum_{d|n} \sum_{n=1}^{\infty} n^{u-1} \frac{x \exp(-(2\pi i h)/q)}{1 - x \exp(-(2\pi i h)/q)} \qquad ;$$

en regroupant les coefficients on aura

$$\sigma_u(n) = \zeta(1 - u) \sum_q c_q(n)\ n^{u-1} \quad \text{si} \quad c_q(n) = \sum_{h(q)} \exp(-(2\pi i n h)/q)$$

cette formule est due à RAMANUJAN, et est classique, mais la démonstration qui en est donnée ici est nouvelle.

Nous pouvons maintenant essayer de construire une série singulière qui serait susceptible, dans certaines conditions, de donner une approximation pour la fonction

$$\lambda^*(u_1\ , u_2\ , u_3\ , \dots ; x) = \prod_{u=u_1, u_2, \dots} \lambda_u(x) = \sum \delta(n)\ x^n \qquad .$$

Dans le cas particulier $\lambda^*(u_1\ , u_2\ ; x)$ on trouve

$$\delta(n) \sim C_{u_1,u_2}\, \sigma_{u_1+u_2+1}(n)$$

avec

$$C_{u_1,u_2} = \frac{\Gamma(1+u_1)\,\Gamma(1+u_2)}{\Gamma(u_1+u_2+2)} \times \frac{\zeta(1+u_1)\,\zeta(1+u_2)}{\zeta(2+u_1+u_2)} \quad .$$

HALBERSTAM a pu évaluer avec précision l'ordre du terme d'erreur si $\min(u_1 , u_2) < 1$ et $u_1 + u_2 < 1$, on peut préciser un peu ce résultat

$$\delta(n) = C_{u_1,u_2}\, \sigma_{u_1+u_2+1}(n) + D_{-u_1,u_2}\, \sigma_{-u_1+u_2+1}(n) + D_{u_1,-u_2}\, \sigma_{u_1-u_2+1}(n)$$
$$+ D_{-u_1,-u_2}\, \sigma_{-u_1-u_2+1}(n) + O(n^{\omega+\varepsilon})$$

avec

$$\omega = \frac{3}{4} + \frac{u_1+u_2}{2} \quad \text{si} \quad \alpha+\beta < \frac{1}{2}$$

$$\omega = \frac{1}{2} + u_1 + u_2 \quad \text{si} \quad \alpha+\beta \geqslant \frac{1}{2}$$

et le terme d'erreur peut être même mis sous la forme $O(n^{\omega} \log^4 n)$. On a

$$D_{u_1,u_2} = \frac{\zeta(1+u_1)\,\zeta(1+u_2)}{\zeta(2+u_1+u_2)} \quad .$$

Si $d(n)$ est le nombre de diviseurs de n , le problème est un peu plus compliqué.

Convenons

$$\left(\sum d(n)\, x^n\right)^k = \sum \alpha_k(n)\, x^n \quad .$$

ESTERMAN a donné une expression asymptotique de

$$\alpha_3(n) = \frac{1}{2\zeta(3)} \sigma_2(n) \log^3 n + O(n^{2+\varepsilon})$$

$\alpha_3(n)$ peut être défini comme le nombre de représentation de n comme somme de trois produits $u_1 u_2 + u_3 u_4 + u_5 u_6 = n$. on a aussi

$$\alpha_2(n) \sim \frac{6}{\pi^2} \sigma(n) \log^2(n) \quad .$$

Un problème bien différent est celui de la représentation de u par une forme quadratique

$$\text{(F)} \qquad \sum_{\nu=1}^{s} \alpha_\nu m_\nu^2 = n \quad .$$

L'analyse que l'on peut faire est extrêmement voisine de celle que nous avons donnée, la seule différence est qu'il y a lieu, dans la factorisation de la série singulière de traiter à part non seulement le nombre premier 2, mais encore les diviseurs de $\prod_{\nu=1}^{s} \alpha_\nu$.

On a

$$z(n , F) = \rho(n , F) + O(n^{s/4}) \quad \text{si} \quad s > 4$$

où $\rho(n , F)$ est la fonction dérivée de la série singulière et si $s = 4$

$$z(n , F) = \rho(n , F) + O(n^{17/18}) \quad .$$

Ces résultats sont dus à KLOOSTERMAN.

Le cas $k = 2$. - Le cas $K = 2$ est complètement à part, car alors, on peut raffiner beaucoup l'analyse ; rappelons que, pour p impair, on a $S_{h,p} = (\frac{h}{p}) S_{1,p}$.

Partant on considère le nombre de représentations de n comme somme de $2s'$ carrés, on a à évaluer les sommes $\sum_{h}\sum_{q} \frac{S_{h,q}^{2s'}}{q^{2s'}} \exp(-(2\pi i n h)/q)$ et le caractère $(\frac{h}{p})$ disparaît, la sommation est alors très facile : on a $(\frac{-1}{p})^{s'} C_p(n)$ avec $p \neq 2$, $C_p(n) = -1$ si $p \nmid n$, $C_p(n) = p - 1$ si $p \mid n$, etc. La sommation de la série singulière se ramène alors à

$$\mathfrak{S}(n) = \prod_{p|2n} \xi(p\ ,\ n) \prod_{p\nmid 2n} [1 - (\frac{-1}{p})\ p^{-s'}] \qquad ,$$

d'où, par une transformation aisée,

$$\mathfrak{S}(n) = \prod_{p|2n} \xi^*(p\ ,\ n).F(s')$$

avec

$$F(s') = \sum_{h\equiv 1\,(2)} (\frac{-1}{n})^{s'} \frac{1}{n^{s'}} \qquad .$$

$F(s')$ se ramène donc si $s' \equiv 1(2)$ à $L(s) = 1 - 3^{-s} + 5^{-s} - 7^{-s} \ldots$, et si $s' \equiv 0(2)$ à $\zeta(s')(1 - 2^{-s'})$.

Reste à sommer $\xi^*(p\ ,\ n)$, si $p = 2$ il y a de nombreux cas à considérer, sinon on trouve qu'il est facile d'exprimer les $\xi^*(p\ ,\ n)$. Finalement on peut exprimer les fonctions $\mathfrak{S}(n)$ et donc $\rho(n)$ par des fonctions des diviseurs d de n qui, si s' est impair, font intervenir $(\frac{-1}{d})$.

Le cas $s = 2s' + 1$ est un peu plus compliqué.

On a alors finalement

$$\mathfrak{S}(n) = \prod_{p|2n} \xi(p\ ,\ n) \prod_{p\nmid 2n} [1 + \Lambda_p(n)]$$

$$\mathfrak{S}(n) = \prod_{p|2n} \xi(p\ ,\ n)\ L^*(n\ ,\ s') \qquad ,$$

$L^*(n\ ,\ s')$ étant une fonction L avec caractères $(\frac{\pm n}{m})$. La valeur exacte de $L(n\ ,\ s')$ est d'ailleurs facile à sommer en calculant des sommes finies de type $\sum(\frac{\pm n}{m})\ m^{\alpha}$.

D'autre part, par la théorie des fonctions elliptiques on peut montrer que $\rho(n) = z(n)$ si, et seulement si $3 \leqslant s \leqslant 8$ sinon on a $z(n) = \rho(n) + \varepsilon(n)$.

Or les fonctions $\varepsilon(n)$ ainsi définies ont des propriétés remarquables :

1° Les fonctions génératrices de $z(n)$, $\rho(n)$, $\varepsilon(n)$ vérifient la même relation fonctionnelle

$$\sum f(n)\ x^n = \left(\frac{\pi}{-\log x}\right)^{s/2} \sum f(n)\ x'^n$$

[avec des conventions définissant $f(0)$].

2° On a

$$\theta^*(x\ ,\ s) = \theta_2^s(x) - \sum_{s-8\mu>0} \bar{A}_{\mu,s}\ \theta^{s-8\mu}(x)\ \theta^{4\mu}(-x)\ \tilde{\theta}^{4\mu}(x)$$

où $\tilde{\theta}(x)$ représente la fonction désignée classiquement dans la théorie des fonctions elliptiques par θ_2 .

Rien n'est connu des coefficients $\bar{A}_{\mu,s}$ qu'on calcule directement. On a par exemple

$$\theta(x\ ,\ g) = \theta^9(x) - \frac{2}{17}\ \theta(x)\ \theta^4(-x)\ \tilde{\theta}^4(x) \qquad .$$

3° Mais dans certains cas pour s pair on peut exprimer $\varepsilon(n)$ à l'aide des diviseurs complexes de n , dans le corps $C(\sqrt{-1})$, et on est amené à étudier des fonctions telles $\frac{1}{4} \sum_{a^2+b^2=n} (a+bi)^4$.

Celle-ci en particulier est multiplicative.

La fonction $\varepsilon(n)$ associée à $s = 24$ est remarquable, mais on ne lui connaît aucune représentation arithmétique simple.

Pour en finir avec le cas $k = 2$, citons seulement :

1° Que si s est entier impair, la fonction $\sum \sigma_s(n)\ x^n$ est aussi une fonction elliptique modulaire et que l'on peut exprimer exactement des produits de Cauchy $\sum \sigma_s(\nu)\ \sigma_{s'}(n-\nu)$ si $s \equiv s' \equiv 1 (2)$. Par exemple, avec certaines conventions sur $\sigma_s(o)$,

$$\sum_{\nu=0}^{n} \sigma_7(\nu)\ \sigma_5(n-\nu) = \frac{\sigma_{13}(n)}{10.080} \qquad .$$

2° Que l'on sait, au moins dans certains cas, exprimer de façon <u>exacte</u> le nombre $z(n, F)$ de représentation par une forme quadratique $F(a, b, c, d)$, car la série singulière, si $a = b$ et $c = d$, s'exprime aisément par une fonction de diviseurs, et l'on peut même, comme le montrent les travaux récents de LOMADZÉ, calculer exactement le nombre de représentations de n par certaines formes ternaires $n = am_1^2 + bm_2^2 + cm_2^2$.

<u>Le cas $k = 3$</u>. - Le cas $k = 3$ présente des particularités intéressantes.

1° Les méthodes analytiques, que ce soit celles de HARDY ou de VINOGRADOV, donnent péniblement $G(3) = 9$. Or on sait que $g(3) = 9$ et $G(3) \leqslant 7$, mais ceci a été obtenu par l'algèbre uniquement.

2° $G_1(3) = 4$ (Théorème de Davenport), mais la démonstration est très difficile.

3° Les sommes de Gauss par les cubes vérifient les relations (dues à KUMMER)

$$S_{h,p^{3\alpha+\beta}} = S_{h,p^{3\alpha}} S_{h,p^\beta} \quad ;$$

$$S_{h,p^{3\alpha}} = p^{2\alpha}$$

$$S_{h,p^2} = p \quad \text{sauf si} \quad p = 3 \quad ,$$

$$S_{h,q} = 1 + 2 \cos \frac{2\pi h}{9}$$

$$S_{h,p} = 0 \quad \text{sauf si} \quad p \equiv 1 (3)$$

et dans ce cas $S_{h,p}$ est une des racines de

$$x^3 - 3px - pL = 0 \ , \qquad 4p = L^2 + 27M^2 \ , \qquad L \equiv 1 (3)$$

donc

$$S_{1,p} = 2\sqrt{p} \cos \omega \quad \text{avec} \quad \operatorname{arctg} \frac{3\sqrt{3}\, M}{L} \equiv 3\omega (\mathrm{mod}\ 2\pi) \quad \text{si} \quad M > 0 \quad .$$

Soit $2p_1 = L - i3\sqrt{3}M$. La valeur de ω n'est connue par ces formules qu'à $\pm\frac{2\pi}{3}$ près. Mais si on connaît $S_{1,p}$ on détermine $S_{h,p}$ par

$$S_{h,p} = 2\sqrt{p}\cos(\omega + \frac{4\pi}{3}\varepsilon'_h)$$

avec

$$\varepsilon_h = P.R[\frac{h}{p_1}] = 1 \quad \text{ou} \quad -\frac{1}{2}$$

$$\varepsilon'_h = -\frac{PI}{\sqrt{3}}[\frac{h}{p_1}] = \pm\frac{1}{2} \quad \text{ou} \quad 0 \qquad ,$$

$[\frac{h}{p_1}]$ étant le symbole d'Eisenstein, c'est-à-dire un caractère cubique, mais il est essentiel que ce caractère soit déterminé modulo p_1 et non modulo $\overline{p_1}$.

On peut alors calculer $\Lambda_p(n)$ et sommer la série singulière

$$p^s\,\Lambda_p(n) = (p-1)\varphi_s \quad \text{si} \quad p|n$$

et

$$p^s\,\Lambda_p(n) = -\varphi_s + \varepsilon_n\,\varphi_{s+1} + \varepsilon'_n\,\psi_s \quad \text{si} \quad p\nmid n$$

$3\varphi_s$ étant la somme des puissances s des racines de l'équation cyclotomique

$$x^3 - 3px - pL = 0$$

et

$$\psi_s = \frac{1}{3M}(4p\varphi_s + L\varphi_{s+1} - 2\varphi_{s+2})$$

d'où finalement

$$\mathfrak{S}(n) = \prod_{p|3n} \xi(p\,,\,n)\,L^*(s\,,\,h\,,\,s)$$

$$L^*(\nu , n , s) = \prod_{\substack{p\equiv 1 (3)\\ p\nmid n}} [1 - \frac{\varphi_\nu}{p^s} + \frac{\varepsilon_n \varphi_{\nu+1}}{p^s} + \frac{\varepsilon'_n \psi_\nu}{p^s}]$$

Toutes ces formules permettent le calcul théorique de la série singulière et attirent l'attention sur la fonction $L^*(\nu , n , s)$.

Il est intéressant d'observer ici que DAVENPORT et HEILBRONN avaient pu sommer la série singulière associée à la fonction $\theta_3^2(x)\ \theta_2(x)$, série qui peut se sommer grâce à la fonction

$$M(s) = \prod_{p\equiv 1} [1 + 2(\frac{n}{p})\ p^{-s} + 2(\frac{n}{p})\ \varepsilon_{4n}\ p^{-s}] \quad .$$

Or $M(s)$ s'exprime grâce à certaines généralisations de la fonction de Riemann.

D'autre part, si on ne sait rien des sommes $S_{h,q,m}$ et $S^*_{h,q,m}$, leur étude semble très réalisable en raison des rapports étroits qu'elles ont avec certains résultats de CAUCHY et d'OLTRA MARE. En outre, les fonctions $\varphi(x)$ et $\varphi^*(x)$ sont très voisines des fonctions de Bessel.

Dans un autre ordre d'idées nous avons personnellement, avec une machine Bull Gamma ET, calculé les $z_{k,s}(n)$ par différentes valeurs de k et de s , et en particulier si $k = 3$, $s \leqslant 6$ jusqu'à $n = 2047$.

L'examen des résultats a montré que ces nombres ont des propriétés de congruences très intéressantes.

Dans le cas $k = 2$, nous avons pu montrer par exemple,

$$z_{2,3\alpha+1}(3m + 2) \equiv 0(3)$$

de même

$z_{3,6}(n)$ est presque toujours divisible par 960 ,

$z_{3,4}(n)$ est presque toujours divisible par 192 .

Suggestions et conclusion. - L'étude du problème de Waring amène à des réflexions diverses.

1° Si employée qu'elle soit, la méthode du cercle ne semble pas avoir fait l'objet d'une étude systématique. En particulier HARDY et LITTLEWOOD n'ont jamais justifié le choix de leur contour d'intégration et de l'ordre de la dissection. De plus, bien souvent on constate que certains problèmes ont progressé à partir du moment où ce contour a été transformé.

Il y a un certain nombre de raisons qui suggèrent d'autres contours.

2° Tout l'effort fait par VINOGRADOV et ses disciples a porté sur la détermination de $g(k)$ par k grand. Mais le problème de $g(3)$, très abordable, n'a guère été traité.

3° La série singulière a été définie par une voie purement analytique. Cependant ses propriétés arithmétiques sont intéressantes.

Si on arrivait par une méthode purement arithmétique à établir directement les relations que nous avons signalées, on peut penser qu'un grand pas serait fait.

4° Enfin les propriétés de la série singulière nous échappent totalement. En particulier quelles sont les propriétés de fonctions telle $\sum \rho(n) x^n$. Il y a des raisons qui suggèrent une généralisation des fonctions elliptiques modulaires, mais la question est très obscure.

Quelques problèmes connexes. - Nous voulons ici attirer l'attention sur quelques problèmes connexes.

1° Les $S_{k,h,q}$ sont racines d'une équation de k-ième degré. Mais laquelle des k solutions possibles choisir ?

Sauf si $k = 2$ on ne connaît aucune solution.

2° Quelle est la distribution des nombres qui sont sommes de trois cubes, quatre bicarrés, etc. ; en particulier soit λ_n ces nombres rangés par ordre croissant ; déterminer la distribution de $\lambda_{n+1} - \lambda_n$, et peut-on affirmer que $v_k(n) = o(n)$?

3° Que peut-on dire de la fonction $\sum \rho(n) x^n$; en particulier déterminer son allure au voisinage du cercle unitaire ?

4° Peut-on calculer exactement les sommes $S_{k,h,q,m}$ et $S^*_{k,h,q,m}$ si $k = 3$ ou $k = 4$?

TABLE

k	$g(k)$	$g^*(k)$	$G(k)$ (5)
2	4	4	4
3	9	9	7
4	≤ 35	19	16
5	≤ 40	37	23
6	73	73	36
7	143	143	52
8	279	279	73
9	548	548	99

BIBLIOGRAPHIE

[1] BAKHOOM (N. G.). - Asymptotic expansions of the function $F_k(x)$ ..., Proc. London math. Soc., Series 2, t. 35, 1933, p. 83-100.

[2] BARRUCAND (Pierre). - Sommes de Gauss et séries singulières de Hardy pour les cubes, C. R. Acad. Sc. Paris, t. 250, 1960, p. 4249-4251.

[3] BARRUCAND (Pierre). - Propriétés de congruence pour les coefficients de Waring-Hardy, C. R. Acad. Sc. Paris, t. 253, 1961, p. 2306-2308.

[4] BURWELL (W. R.). - Asymptotic expansions of generalized hypergeometric functions, Proc. London math. Soc., Series 2, t. 22, 1923, p. 57-72.

[5] DAVENPORT (H.). - On Waring's problem for cubes, Acta Mathematica, t. 71, 1939, p. 123-143.

[6] DAVENPORT (H.). - On Waring's problem for fourth powers, Annals of Math., Series 2, t. 40, 1939, p. 731-747.

[7] DAVENPORT (H.). - On Waring's problem for fifth and sixth powers, Amer. J. of Math., t. 64, 1942, p. 199-207.

(5) Il s'agit des valeurs possibles les plus élevées et la table doit se lire $G(k) \leq$ au nombre lu.

[8] DAVENPORT (H.). - On sums of positive integral k-th powers, Proc. royal Soc. London, Series A, t. 170, 1939, p. 293-299.

[9] DAVENPORT (H.). - On sums of positive integral k-th powers, Amer. J. of Math., t. 64, 1942, p. 189-198.

[10] DAVENPORT (H.) and HEILBRONN (H.). - On an exponential sum, Proc. London math. Soc., Series 2, t. 41, 1936, p. 449-453.

[11] DAVENPORT (H.) and HEILBRONN (H.). - On Waring's problem : Two cubes and one square, Proc. London math. Soc., Series 2, t. 43, 1937, p. 73-104.

[12] DICKSON (L. E.). - Proof of the ideal Waring theorem for exponents, Amer. J. of Math., t. 58, 1936, p. 521-529.

[13] DICKSON (L. E.). - Solution of Waring's problem, Amer. J. of Math., t. 58, 1936, p. 530-535.

[14] ESTERMANN (T.). - On the representations of a number as the sum of two products, Proc. London math. Soc., t. 31, 1930, p. 123-133.

[15] ESTERMANN (T.). - On the representations of a number as the sum of three or more products, Proc. London math. Soc., t. 34, 1932, p. 190-195.

[16] HALBERSTAM (H.). - Four asymptotic formulae in the theory of numbers, J. London math. Soc., t. 24, 1949, p. 13-21.

[17] HALBERSTAM (H.). - An asymptotic formula in the theory of numbers, Trans. Amer. math. Soc., t. 84, 1957, p. 338-351.

[18] HARDY (G. H.) and LITTLEWOOD (J. E.). - Some problems of "Partitio numerorum", I, Götting. Nachr., 1920, p. 33-54 ; II, Math. Z., t. 9, 1921, p. 14-27 ; IV, Math. Z., t. 12, 1922, p. 161-188 ; VI, Math. Z., t. 23, 1925, p. 1-37 ; VIII, Proc. London math. Soc., Series 2, t. 28, 1928, p. 518-542.

[19] HARDY (G. H.) and LITTLEWOOD (J. E.). - A new solution of Waring's problem, Quart. J. of pure and appl. Math., t. 48, 1919, p. 272-293.

[20] HUA (Loo Keng). - On Waring's problem, Quart. J. of Math., Oxford Series, t. 9, 1938, p. 199-202.

[21] KLOOSTERMAN (H. D.). - On the representation of numbers in the form $ax^2 + by^2 + cz^2 + dt^2$, Acta Mathematica, t. 49, 1926, p. 407-464.

[22] NEČAEV (V. I.). - Waring's problem for polynomials, Amer. math. Soc. Translations, Series 2, t. 3, 1956, p. 39-90 [Trudy Mat. Inst. Steklov., t. 38, 1951, p. 190-243].

[23] VAL'FIŠ (A. Z.). - On the representation of numbers by sums of squares asymptotic formules, Amer. math. Soc. Translations, Series 2, t. 3, 1956, p. 163-248 [Uspekhi Mat. Nauk, N. S., t. 7, 1952, p. 97-178].