Astérisque

JEAN-MARC DESHOUILLERS

L'étude des formes cubiques rationnelles via la méthode du cercle

Astérisque, tome 189-190 (1990), Séminaire Bourbaki, exp. n° 720, p. 155-177

<http://www.numdam.org/item?id=SB_1989-1990__32__155_0>

Séminaire BOURBAKI mars 1990
42ème année, 1989-90, n° 720

L'ÉTUDE DES FORMES CUBIQUES RATIONNELLES VIA LA MÉTHODE DU CERCLE

[d'après D.R. HEATH-BROWN, C. HOOLEY et R.C. VAUGHAN](*)

par **Jean-Marc DESHOUILLERS**

On doit à Hardy, Littlewood et Ramanujan un outil puissant, la **méthode du cercle**, pour étudier les problèmes diophantiens de la forme $P(x_1, \cdots, x_s) = 0$ lorsque le nombre de variables est grand par rapport au degré du polynôme P. Les derniers avatars de cette méthode ont notamment permis à Heath-Brown de montrer que toute forme cubique rationnelle non-singulière en 10 variables représente 0, à Hooley de réduire le nombre de variables à 9 s'il n'y a pas d'obstruction locale, à Vaughan de donner une évaluation asymptotique du nombre de représentations d'un entier en sommes de 8 cubes, et une bonne minoration pour les représentations en sommes de 7 cubes.

SOMMAIRE

(*) The author thanks the Séminaire Bourbaki and the Séminaire de Théorie des Nombres de Bordeaux for allowing him to publish the English version of this text in the latter publication.

INTRODUCTION

Le problème de savoir si tout entier positif est somme de quatre carrés, peut-être soulevé par les Grecs, a été considéré par plusieurs mathématiciens aux XVII et XVIIIème siècles et finalement résolu par Lagrange en 1770. L'intérêt ainsi que la difficulté de cette question proviennent du mélange entre les lois d'addition et de multiplication des entiers.

Si des conjectures de ce type sont faciles à proposer, elles sont en revanche le plus souvent hors d'atteinte, mais source de développements mathématiques. D'importance historique sont le problème de Goldbach (1742), **tout entier pair est somme de deux nombres premiers** (le nombre 1 était alors décompté comme premier), et le problème de Waring

(1770), **tout entier est somme d'au plus 4 carrés, 9 cubes ou 19 bicarrés**, avec adjonction de points de suspension en 1782.

La Théorie additive des Nombres traite de ces questions ; notre propos est ici de présenter la **méthode du cercle** introduite en 1917 par Hardy et Ramanujan et perfectionnée quelques années plus tard par Hardy et Littlewood. Cet outil septuagénaire n'a rien perdu de sa vigueur ; on l'utilise toujours avec profit, tant pour obtenir des estimations asymptotiques, comme nous le verrons ici, que des évaluations numériques effectives et efficaces. C'est à travers l'étude -limitée- des formes diagonales (et principalement des formes cubiques diagonales), que nous effectuons cette présentation en suggérant quelques étapes de la démonstration des résultats suivants

Théorème 1.— *(D.R. Heath-Brown, 1982) Soit* $F(\mathbf{x}) = F(x_1, \cdots x_s)$ *une forme cubique non singulière à coefficients rationnels. Si* s *est au moins égal à 10, il existe* $\mathbf{x}$ *dans* $\mathbf{Q}^s\backslash\{0\}$ *tel que* $F(\mathbf{x}) = 0$.

Théorème 2.— *(C. Hooley, 1987) Soit* $F(\mathbf{x})$ *une forme cubique non singulière à coefficients rationnels en 9 variables. L'équation* $F(\mathbf{x}) = 0$ *a une solution rationnelle non triviale dans* $\mathbf{Q}$ *si et seulement si elle a une solution non triviale dans chaque corps p-adique* $\mathbf{Q}_p$.

Théorème 3.— *(R.C. Vaughan, 1985) Soit* $r_8(N)$ *le nombre de représentations de l'entier* N *en sommes de huit cubes d'entiers positifs. Lorsque* N *tend vers l'infini, on a*

$$r_8(N) = \mathfrak{S}(N)\,\frac{\Gamma(4/3)^8}{\Gamma(8/3)}\,N^{5/3}\,(1 + o(1))\,.$$

où

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \left\{ q^{-1} \sum_{m=1}^{q} \exp(2\pi i(am^3/q)) \right\}^8 \exp(-2\pi i aN/q)\,.$$

On conjecture que la condition de non-singularité peut être levée dans l'énoncé du Théorème 1. Davenport a établi en 1963 que toute forme cubique rationnelle en au moins 16 variables représente 0 ; même dans le cas des formes non singulières, c'était le meilleur résultat connu avant le travail de Heath-Brown. La condition locale est indispensable dans le cas des formes nonaires, comme l'a montré Mordell en 1936. Le Théorème 3 était une conjecture favorite de Davenport qui, m'a-t-on dit, la proposait systématiquement à ses élèves.

Pour clore cette introduction, signalons les travaux de Colliot-Thélène, Sansuc et Swinnerton-Dyer, 1986 (on pourra consulter Colliot-Thélène, 1986, pour une présentation générale). Abordant le problème par la géométrie algébrique, ils parviennent notamment aux meilleurs résultats actuellement connus sur les systèmes de formes quadratiques. Pour ce qui est des formes cubiques, ce type de méthode permet d'établir le résultat suivant, que l'on comparera avec profit au Théorème 2 (moins de variables, mais des conditions géométriques plus subtiles).

Théorème 4.— *(J.-L. Colliot-Thélène et P. Salberger, 1988). Soit K un corps de nombres et $X \subset \mathbf{P}_K^n$ une hypersurface cubique définie sur K, avec ($n \geq 3$). Si X contient un ensemble de 3 points singuliers conjugués, et si X admet des points rationnels sur tous les complétés de K, alors X admet un point rationnel sur K.*

§1 ABORD HEURISTIQUE : L'INTÉGRALE SINGULIÈRE

1.1 Expérimentation

Observons une table donnant, pour chaque entier N jusqu'à 40 000 le nombre minimal de termes intervenant dans la décomposition de N en somme de cubes positifs : les nombres 23 et 239 sont les seuls à nécessiter 9 cubes ; quinze autres entiers, dont le plus grand est 8402, nécessitent 8 cubes, et tous les autres au plus 7 cubes. Si l'on poursuivait cette table jusque vers 10^{15}, on en retirerait l'impression qu'à partir d'un certain rang, 4 cubes seulement sont suffisants !... Ainsi, il semble plus facile de représenter les grands entiers que les petits.

1.2 Étude du nombre des représentations

Cet aspect n'était pas pris en compte dans les travaux développés dans la seconde moitié du XIXème siècle, de Liouville qui montre en 1859 que tout nombre est somme d'au plus 53 bicarrés, à Hilbert qui montre en 1909 que tout entier est somme d'un nombre fini (ne dépendant que de k) de puissances k-ièmes et à Kempner qui complète un travail de Wieferich et établit en 1912 que tout nombre est somme d'au plus 9 cubes.

La méthode du cercle, introduite par Hardy et Littlewood dans le contexte du problème de Waring, prend en compte cette plus grande facilité à représenter de grands entiers : pour savoir si l'entier N est représentable comme somme de s puissances k-ièmes, ils cherchent à déterminer le **comportement asymptotique du nombre de représentations** de N comme somme de s puissances k-ièmes. De ce point de vue, ils ne s'intéressent qu'aux entiers assez grands, et de là provient le succès de leur méthode.

1.3 Ecriture intégrale du nombre de représentations

Commençons par fixer quelques notations :

k désigne un entier supérieur ou égal à 2. On pourra se limiter à ne considérer que la valeur 3 pour k.

N désigne un entier, qui sera amené à tendre vers l'infini.

Pour s entier positif, on note $r_s(N)$ le nombre de représentations de N en somme de s puissances k-ièmes.

$e(\cdot)$ désigne l'exponentielle complexe $\exp(2\pi i \cdot)$

Le lecteur n'aura aucune peine à donner une démonstration de la relation

1.3.a
$$r_s(N) = \int_{\mathbf{R}/\mathbf{Z}} \Big(\sum_{0 \leq n^k \leq N} e(\alpha n^k)\Big)^s e(-\alpha N) d\alpha$$

en se fondant soit sur l'orthogonalité des caractères $e(h\cdot)$, soit sur la formule intégrale de Cauchy. Nous en donnons ici une présentation probabiliste, dont nous ne mentionnons que pour mémoire l'intérêt pour certain calcul explicite (Deshouillers, 1985).

On considère s variables aléatoires indépendantes $X_1, \cdots, X_s$ de loi commune $\lambda \sum_{n \leq N^{1/k}} \delta(n)$, où $\delta(a)$ désigne la mesure de Dirac en a, et le facteur de normalisation λ vaut $[N^{1/k}+1]^{-1}$. Chaque variable aléatoire X_i^k a pour loi $\lambda \sum_{n \leq N^{1/k}} \delta(n^k)$. La loi de la variable aléatoire $X := X_1^k + \cdots + X_s^k$ est la puissance s-ième de convolution de la loi commune de X_i^k ; elle vaut donc $\lambda^s \sum_m r_s^*(m)\delta(m)$, où $r_s^*(m)$ est le nombre de façons d'écrire m comme somme de s puissances k-ièmes au plus égales à N ; le coefficient $r_s^*(m)$ s'obtient de façon classique à partir de la fonction génératrice (ou série de Fourier) de X, qui est la puissance s-ième de celle de X_1^k. La formule 1.3.a découle de cela et de l'égalité banale de $r_s(N)$ et $r_s^*(N)$.

1.4 Ordre de grandeur heuristique de $r_s(N)$

On donne une approximation continue du problème considéré : on considère s variables aléatoires indépendantes $Z_1, \cdots, Z_s$ de loi uniforme sur $[0, N^{1/k}]$ et on note Z la somme $Z_1^k + \cdots + Z_s^k$. La fonction caractéristique (alias transformée de Fourier) de Z est la puissance s-ième de celle de Z_1^k ; par transformation de Fourier inverse, on obtient la densité $\rho_s(t)$ de Z au point t :

$$\rho_s(t) = \int_{-\infty}^{\infty} (\int_0^{N^{1/k}} e(\beta x^k)dx)^s e(-\beta t)d\beta \tag{1.4.a}$$

Le membre de droite s'appelle l'**intégrale singulière**. Par changement de variables, on obtient dans le cas où t vaut N :

$$\rho_s(N) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{s/k-1}, \tag{1.4.b}$$

car on a

$$\int_{-\infty}^{\infty} (\int_0^1 e(\gamma\xi^k)d\xi)^s e(-\gamma)d\gamma = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)}. \tag{1.4.c}$$

Ainsi, la valeur moyenne de $r_s(N)$ est-elle $N^{s/k-1}$ à un facteur eulérien près. On notera la présence de l'intégrale singulière dans la formule asymptotique pour le nombre de représentations en somme de 8 cubes (cf. Théorème 3).

§2 ABORD p-ADIQUE : LA SÉRIE SINGULIÈRE

Après avoir expliqué la présence de l'intégrale singulière dans le théorème 3, nous allons interpréter la **série singulière** $\mathfrak{S}(N)$, selon la terminologie introduite par Hardy et Littlewood.

2.1 Nombre de solutions de la congruence $m_1^k + \cdots + m_s^k \equiv N \pmod{q}$

Notons $M(q)$ le nombre de solutions de la congruence considérée. L'égalité

2.1.a
$$M(q) = \frac{1}{q} \sum_{r=1}^{q} \left(\sum_{m=1}^{q} e(rm^k/q) \right)^s e(-rN/q)$$

qui s'obtient aisément à partir des relations d'orthogonalité

$$\frac{1}{q} \sum_{r=1}^{q} e(rh/q) = \begin{cases} 1 & \text{si} \quad q \mid h \\ 0 & \text{si} \quad q \nmid h, \end{cases}$$

est l'équivalent, dans $\mathbf{Z}/q\mathbf{Z}$, de l'expression intégrale 1.3.a . En réordonnant les termes du membre de droite de 2.1.a en fonction de la valeur de (r, q), on a

$$M(q) = \frac{1}{q} \sum_{d|q} \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \left(\frac{q}{d} \sum_{m=1}^{d} e(am^k/d) \right)^s e(-aN/d),$$

ou encore

2.1.b
$$M(q) = q^{s-1} \sum_{d|q} G(d) \ ,$$

où

$$G(d) = \sum_{\substack{a=1 \\ (a,d)=1}}^{d} \{d^{-1} \sum_{m=1}^{d} e(am^3/d)\}^s e(-aN/d).$$

Voilà qui commence à fleurer le théorème 3 !

2.2 Interprétation de la série singulière

La multiplicativité de la fonction G (qui découle directement du théorème chinois, ou indirectement via la relation 2.1.b), permet d'écrire la série singulière

$$\mathfrak{S}(N) = \sum_{q=1}^{\infty} G(q)$$

comme un produit eulérien

$$\mathfrak{S}(N) = \prod_p \sum_{h=0}^{\infty} G(p^h) .$$

Par la relation 2.1.b, on a donc

2.2.a $$\mathfrak{S}(N) = \prod_p \lim_{\ell \to \infty} p^{\ell(1-s)} M(p^\ell) .$$

En remarquant que $p^{\ell(s-1)}$ est le cardinal d'un hyperplan dans $(\mathbf{Z}/p^\ell\mathbf{Z})^s$, on interprète chaque facteur de $\mathfrak{S}(N)$ comme une densité des solutions de $x_1^k + \cdots + x_s^k = N$ dans $\mathbf{Z}_p$.

Le lecteur sera peut-être tenté d'aller plus loin dans cette direction : nous lui recommandons la lecture de Lachaud, 1982, pour une présentation adélique de la méthode du cercle.

§3 DISSECTION DE FAREY CLASSIQUE : ARCS MAJEURS, SÉRIE ET INTÉGRALE SINGULIÈRES

Nous abordons maintenant le calcul de $r_s(N)$ à partir de la représentation intégrale 1.3.a . L'expression cruciale figurant dans l'intégrande est la somme exponentielle

3.0.a $$S(\alpha) := \sum_{n \leq P-1} e(\alpha n^k) \quad , \quad \text{où} \quad P := \lfloor N^{1/k} + 1 \rfloor$$

Son module est clairement maximal lorsque α est entier ; nous commencerons par étudier la contribution à $r_s(N)$ des α proches de 0 dans $\mathbf{R}/\mathbf{Z}$, ou encore proches de 0 dans $\mathbf{R}$ en identifiant $\mathbf{R}/\mathbf{Z}$ à un voisinage de 0.

3.1 Contribution du premier arc majeur (α proches de 0)

Puisque $S(\alpha)$ est une fonction continue de α et que $S(\alpha) = P$ (cette égalité justifie la gaucherie de la définition de P), l'analyse nous permet d'évaluer $S(\alpha)$ pour α proche de 0.

Supposons effectivement que $|\alpha| \leq \varepsilon N^{-1}$, où ε est n'importe quelle fonction de N tendant vers 0 à l'infini. Par la formule de Taylor, on a :

$$S(\alpha) = P + o(P) \quad \text{et} \quad e(-\alpha N) = 1 + o(1), \quad \text{d'où}$$

$$\begin{aligned}\int_{-\varepsilon N^{-1}}^{\varepsilon N^{-1}} S(\alpha)^s e(-\alpha N) d\alpha &= 2\varepsilon N^{-1} P^s (1 + o(1)) \\ &= 2\varepsilon N^{s/k-1}(1 + o(1)).\end{aligned}$$

Il est remarquable que la contribution à $r_s(N)$ d'un tel intervalle autour de 0 soit de l'ordre de grandeur de la valeur heuristique.

En fait, nous avons utilisé la formule de Taylor qui est quelque peu sommaire (ne l'enseignons-nous pas à nos étudiants dès la première année ?). La formule sommatoire de Poisson (quand l'enseignons-nous à nos étudiants ?) est un outil beaucoup plus efficace. Posons

$$f(x) := \begin{cases} e(\alpha x^k) & \text{pour} \quad 0 \leq x \leq P \\ 0 & \text{sinon} \end{cases}$$

et notons $\hat{f}$ sa transformée de Fourier ($\hat{f}(t) = \int_{-\infty}^{\infty} f(x) e(xt) dx$) ; on a

$$\sum_{n \in \mathbf{Z}} f(x) = \sum_{\nu \in \mathbf{Z}} \hat{f}(\nu) + \mathrm{O}(1) ,$$

et donc

3.1.a $$S(\alpha) = \sum_{\nu \in \mathbf{Z}} \int_0^P e(\alpha x^k + \nu x) dx + \mathrm{O}(1).$$

Lorsque $|\alpha|$ est assez petit ($k|\alpha| P^{k-1} \leq 1/2$), la fonction $e(\alpha x^k + \nu x)$ oscille sur l'intervalle $[0, P]$ pour $\nu \neq 0$, et l'intégrale $\int_0^P e(\alpha x^k + \nu x) dx$ est petite, comme on le voit en intégrant par parties ; il n'est pas difficile de montrer que l'on a

3.1.b
$$S(\alpha) = \int_0^P e(\alpha x^k)dx + \mathrm{O}(1)$$

c'est alors un calcul de routine de vérifier que, pour $s \geq k+1$, la contribution de l'intervalle

3.1.c
$$\mathfrak{M}_{0,1} := \{\alpha / |\alpha| \leq (2kP^{k-1})^{-1}\}$$

est équivalente à $\rho_s(N)$, le nombre moyen de représentations. (cf. 1.4.a et 1.4.b) !

3.2 Contribution des arcs majeurs : répartition des puissances dans les progressions arithmétiques

Dans le paragraphe 2.2, nous avons réécrit la série singulière en terme du nombre de solutions des congruences $x_1^k + \cdots + x_s^k \equiv N \pmod q$. Nous voulons ici expliquer comment la moyenne des sommes de Gauss que nous avons notée $G(q)$ intervient lorsque l'on étudie la contribution à $r_s(N)$ de petits intervalles centrés aux rationnels de dénominateur q.

Commençons par évaluer $S(a/q)$; on a

$$S(a/q) = \sum_{n \leq P-1} e(an^k/q) = \sum_{m=1}^{q} \sum_{\substack{n \leq P-1 \\ n \equiv m (\mathrm{mod} q)}} e(an^k/q)$$

$$= \sum_{m=1}^{q} e(am^k/q) \sum_{\substack{n \leq P-1 \\ n \equiv m (\mathrm{mod} q)}} 1 = \frac{P}{q} \sum_{m=1}^{q} e(am^k/q) + \mathrm{O(q)}$$

Or la somme de Gauss $\sum_{m=1}^{q} e(am^k/q)$ n'a aucune raison d'être nulle (ainsi, pour $k = 3$ et $a/q = 1/4$, elle vaut 2) ; cela correspond aux irrégularités de répartition des puissances k-ièmes dans les progressions arithmétiques. Il en résulte que $S(a/q)$ a (parfois) un ordre de grandeur comparable à $S(0)$. On étudie alors le comportement local de S en a/q comme en 0 : on introduit les **arcs majeurs**

3.2.a
$$\mathfrak{M}_{a,q} := \{\alpha / |\alpha - \frac{a}{q}| \leq (2kP^{k-1}q)^{-1}\} ,$$

où $0 < a < q$, $(a,q) = 1$ et $q \leq Q$. Disons à ce stade que le choix de Q n'a pas une très grande importance ; on prend généralement une puissance de P, e.g. P lui même. Notons dès maintenant que le choix d'un Q supérieur à P est possible, mais demande beaucoup de délicatesse : cela revient à étudier la répartition d'un ensemble de P entiers dans les classes modulo un entier supérieur à P.

La formule sommatoire de Poisson permet d'approcher

$$S(\alpha) \quad \text{par} \quad \left(\frac{1}{q}\sum_{m=1}^{q} e(am^k/q)\right)\int_0^P e((\alpha - \frac{a}{q})x^k)dx \quad \text{sur} \quad \mathfrak{M}_{a,q} \ .$$

En regroupant les contributions des différents arcs majeurs (on note $\mathfrak{M}$ leur réunion) on a

Proposition.— *Pour $s \geq 4k$ (et $s \geq 4$ dans le cas des cubes), il existe un réel A strictement positif, tel que l'on ait, lorsque N tend vers l'infini*

$$\text{3.2.}b \quad \int_{\mathfrak{M}} S(\alpha)^s e(-\alpha N)d\alpha = (1+o(1))\rho_s(N).\mathfrak{S}(N) \quad \text{avec} \quad \mathfrak{S}(N) \geq A \ .$$

On rappelle que $\rho_s(N) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{s/k-1}$.

§4 DISSECTION DE FAREY CLASSIQUE : ARCS MINEURS

Bien qu'elle soit la substance d'une mise en oeuvre traditionnelle de la méthode du cercle, nous traitons sommairement cette partie qui dépend fondamentalement de la nature diagonale des formes impliquées dans le problème de Waring.

La réunion des arcs majeurs ne peut recouvrir tout $\mathbf{R}/\mathbf{Z}$; une façon simple de le voir est de mesurer la longueur totale des arcs majeurs. Considérons le cas des cubes, on a

$$|\mathfrak{M}| = \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{1}{3P^2 q} \leq \frac{Q}{3P^2} \ ;$$

non seulement la longueur des arcs majeurs est inférieure à 1, mais encore elle tend vers 0 quand N tend vers l'infini ! On appelle **arcs mineurs** le complémentaire des arcs majeurs et on le note $\mathfrak{m}$.

4.1 Majoration de Weyl : 13 cubes

La somme $S(\alpha)$, pour α irrationnel, a été considérée sous un angle "dual" par Weyl en 1916 : pour α donné et P tendant vers l'infini, il a montré que la quantité $S(\alpha)/P$ tend vers 0. De ce point de vue que nous ne développons pas ici, cela correspond au fait que les nombres αn^3 sont "uniformément répartis" dans $\mathbf{R}/\mathbf{Z}$. La méthode de Weyl pour majorer $|S(\alpha)|$ conduit à la majoration valable dans le cas des cubes et pour tout $\varepsilon > 0$:

4.1.a $$|S(\alpha)| = \mathrm{O}_\varepsilon(\mathrm{P}^{3/4+\varepsilon}) \quad \text{uniformément pour} \quad \alpha \in \mathfrak{m}$$

(Pour les puissances k-ièmes, l'exposant est $1 - 2^{1-k}$).

De la majoration 4.1.a, on déduit aisément

4.1.b $$|\int_{\mathfrak{m}} (S(\alpha))^s e(-\alpha N) d\alpha| = \mathrm{O}_\varepsilon(\mathrm{P}^{3s/4+\varepsilon}) \; .$$

En regroupant ce résultat avec 3.2.b (contribution des arcs majeurs), on obtient un équivalent pour le nombre de représentations en somme de s cubes dès que

$$s - 3 > 3s/4 \; ,$$

c'est-à-dire dès que s est strictement supérieur à 12. On obtient de même un équivalent pour le nombre de représentations en somme de $k2^{k-1} + 1$ puissances $k$ièmes.

4.2 Relation de Parseval : 9 cubes

La force de la relation 4.1.a ne réside pas tant dans l'exposant (on aimerait bien remplacer 3/4 par 1/2, majoration probabiliste de la marche aléatoire des $e(\alpha n^3)$), que dans son uniformité sur $\mathfrak{m}$. Or cette uniformité est gaspillée dans l'application que l'on en donne en 4.1.b, où la norme ℓ^s est recherchée. La relation de Parseval nous donne l'exposant $s/2$ dans la relation 4.1.b, au moins pour $s = 2$, ce qui est banal, et $s = 4$, ce qui est un peu plus subtil : l'identité $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ permet de majorer $r_2(n)$ par le nombre de diviseurs de n, d'où la majoration

$$4.2.a \qquad r_2(n) = \mathrm{O}_\varepsilon(\mathrm{n}^\varepsilon) \ .$$

On peut alors écrire, pour $s \geq 4$:

$$\int_{\mathfrak{m}} |S(\alpha)|^s d\alpha \leq \max_{\alpha \in \mathfrak{m}} |S(\alpha)|^{s-4} \int_0^1 |S(\alpha)|^4 d\alpha$$

d'où l'on déduit un équivalent pour le nombre de représentations en somme de s cubes dès que

$$s - 3 > \frac{3}{4}(s-4) + \frac{4}{2} \ ,$$

c'est-à-dire dès que s est strictement supérieur à 8, et puisque s est entier, cela signifie seulement $s \geq 9$.

Dans le cas des puissances k-ièmes, Hua a généralisé la relation de Parseval et obtenu la majoration

$$4.2.b \qquad \int_0^1 |S(\alpha)|^{2^k} d\alpha = \mathrm{O}_{\varepsilon,\mathrm{k}}(\mathrm{P}^{2^\mathrm{k} - \mathrm{k} + \varepsilon}) \ .$$

d'où un équivalent pour $r_s(N)$ lorsque $s \geq 2^k + 1$. C'est seulement pour mémoire que nous mentionnons ici les améliorations de Vinogradov (amélioration du Lemme de Weyl pour $k \geq 12$), de Heath-Brown (amélioration de l'inégalité de Hua pour $k \geq 6$), de Vinogradov, Davenport, Vaughan et autres (résolubilité de $x_1^k + \cdots + x_s^k = N$, sans équivalent de $r_s(N)$).

4.3 Nombre de représentations en somme de huit cubes : le théorème 3

Reprenons l'inégalité de Hua 4.2.b pour les cubes. Elle implique

$$\int_0^1 |S(\alpha)|^8 d\alpha = \mathrm{O}_\varepsilon(\mathrm{P}^{5+\varepsilon}) \ ,$$

alors que la contribution des arcs majeurs est de l'ordre de P^5. Comme Hooley l'a remarqué, la considération en moyenne des fonctions de diviseurs permettent de remplacer le terme P^ε par une puissance de $\log P$; un résultat de Hall et Tenenbaum conduit même à

$$\text{4.3.}a \qquad \int_0^1 |S(\alpha)|^8 d\alpha = \mathrm{O}_\varepsilon(\mathrm{P}^5(\log \mathrm{P})^\varepsilon),$$

et donc à

$$\text{4.3.}b \qquad r_8(N) = \mathrm{O}_\varepsilon(\mathrm{N}^{5/3}(\log \mathrm{N})^\varepsilon) \ .$$

Le théorème 3 découle directement de l'existence d'un réel $C > 0$ tel que l'on ait

$$\text{4.3.}c \qquad \int_{\mathfrak{m}} |S(\alpha)|^8 d\alpha = \mathrm{O}(\mathrm{P}^5(\log \mathrm{P})^{-\mathrm{c}})$$

On notera combien faible est la marge entre les majorations 4.3.a et 4.3.b. Pour la franchir, Vaughan introduit plusieurs dissections : sur $\mathfrak{m}$, selon les propriétés diophantiennes des α, et sur les entiers de 0 à P (sur lesquels est effectuée la somme $S(\alpha)$), selon leurs propriétés arithmétiques. Il se ramène alors à de nouvelles équations diophantiennes avec un gain global d'un logarithme si l'on sait évaluer le nombre de leurs solutions ; des majorations du type 4.3.b sont alors suffisantes pour conserver les avantages acquis : on peut ainsi prendre pour c tout réel inférieur à 1 dans 4.3.c .

4.4 Nombre de représentations en somme de sept cubes

Cette méthode itérative est à la base de la minoration

4.4.a $$r_7(N) \geq cN^{4/3},$$

pour un réel $C > 0$ et tout entier N assez grand, obtenue par Vaughan, 1987. R.C. Baker et J. Brüdern ont récemment étendu ce résultat aux formes diagonales en 7 variables.

Linnik, 1942 a démontré la positivité de $r_7(N)$, pour tout N assez grand, par des considérations différentes (formes quadratiques ternaires, répartition des nombres premiers dans les progressions arithmétiques).

L'évaluation asymptotique de $r_7(N)$ a été conditionnellement établie par Hooley, 1984 sous l'hypothèse de Riemann pour certaines fonctions L globales de Hasse-Weil.

§5 FORMES CUBIQUES NON DIAGONALES

5.1 Une situation atypique : le cas des formes normiques

Comme nous venons de le voir, ce n'est que très récemment que l'on a su adapter la méthode du cercle pour démontrer que tout entier assez grand est somme de sept cubes. Le résultat de Davenport sur les formes cubiques en 16 variables, mentionné dans l'introduction, et les théorèmes 1 et 2 laissent penser que les formes générales sont plus délicates à manipuler. Le théorème 4 montre l'utilisation qui peut être faite de certaines particularités géométriques. Il est également possible de tenir compte de certaines particularités algébriques, comme en témoigne le résultat suivant qui concerne des formes cubiques en 7 variables (et plus généralement des formes de degré k en $2k+1$ variables).

Théorème 5.— *(B.J. Birch, H. Davenport, D.J. Lewis, 1962) Soient K_1 (resp. K_2) un corps cubique et $N_1(x_1, y_1, z_1)$ (resp. $N_2(x_2, y_2, z_2)$) la forme normique par rapport à une base d'entiers donnée. Si l'équation*

$$N_1(x_1, y_1, z_1) + N_2(x_2, y_2, z_2) + t^3 = N$$

admet une solution non singulière pour tout nombre premier p qui divise $d(K_1)d(K_2)$ (produit des discriminants de K_1 et K_2), alors elle admet une infinité de solutions en entiers rationnels.

Par des méthodes de crible, H. Iwaniec a même obtenu des résultats sur le nombre de représentations par certaines formes cubiques en 6 variables. Pour la simplicité, nous ne citons qu'un corollaire de son résultat :

Théorème 6.— *(H. Iwaniec, 1977) Soit $K/\mathbf{Q}$ une extension cubique galoisienne ; on note N_K la forme normique par rapport à une base d'entiers donnée. (Il existe un entier D et une famille H de classes modulo D tels qu'un nombre premier p se décompose totalement dans K si et seulement si p est congru à un élément de H modulo D).*

Tout entier pair assez grand et congru modulo D à la somme de deux éléments de H, est représentable par la forme $N_K(x_1, y_1, z_1) + N_K(x_2, y_2, z_2)$.

5.2 Le prolongement des arcs majeurs, d'après Vaughan

Dans les quatre premiers chapitres, nous n'avons considéré que des formes **diagonales**. Toute la partie concernant les arcs majeurs peut en fait s'étendre aux formes non diagonales, via la transformation de Fourier sur $\mathbf{Z}^s$. La première utilisation vraiment cruciale de l'aspect diagonal n'est intervenue que dans l'inégalité de Weyl (formule 4.1.a).

A la fin des années 1970, Vaughan a remarqué que le choix de l'arc majeur $\mathfrak{M}_{0,1}$ effectué en 3.1.c n'était commandé que par le souci de négliger le nombre maximal de termes dans la formule sommatoire de Poisson 3.1.a et obtenir la relation 3.1.b . Si l'on choisit un arc majeur plus grand, la fonction $e(\alpha x^k + \nu x)$ n'oscille plus nécessairement, et il faut conserver d'autant plus de termes que l'arc majeur est prolongé. Un agrandissement raisonnable permet encore de contrôler la somme $\sum_{N_1<\nu<N_2} \int_0^P e(\alpha x^k + \nu x) dx$, dans laquelle chaque terme est traité par la méthode de la phase stationnaire (développement limité autour du point où $k\alpha x^{k-1} + \nu$ s'annule, conduisant à une intégrale de Fresnel). Bilan : dans le cas des cubes, on récupère exactement l'exposant 3/4 de la majoration de Weyl, tandis que pour les puissances supérieures, on trouve un exposant supérieur ou égal à 1, ce qui présente peu d'intérêt. Signalons tout de même une utilisation de l'idée de Vaughan pour les bicarrés, dans un contexte où une certaine subtilité numérique était recherchée (Deshouillers, 1985). Autre avantage, la méthode de Vaughan permet d'écrire $S(\alpha)$ comme une somme

trigonométrique qui, traitée trivialement, conduit à la majoration de Weyl ; mais rien n'interdit de conserver explicite ladite somme exponentielle, en vue de futures compensations. Le lecteur, je le remercie d'être encore du voyage, devrait être désormais convaincu que, de même que "13 cubes" provient de la seule majoration de Weyl, on doit pouvoir démontrer le Théorème 1 pour une forme non-singulière en 13 variables à partir d'une bonne connaissance des sommes de Gauss généralisées (Théorème de Deligne !).

Avant d'expliquer d'où vient le gain de 3 variables supplémentaires, je signale l'utilisation faite par Cherly, 1989 de la méthode de Vaughan pour obtenir une inégalité du type Weyl pour les sommes trigonométriques cubiques sur $\mathbf{F}_2[X]$, impossible à obtenir par la méthode classique, puisque dans $\mathbf{F}_2$, on a $3! = 0$.

5.3 Intermède : la dissection de Farey-Kloosterman

Si l'on tient à garder explicites les sommes trigonométriques considérées, pour tout $\alpha \in \mathbf{R}/\mathbf{Z}$, il faut obtenir une **partition** de $\mathbf{R}/\mathbf{Z}$ en arcs majeurs. En étudiant les formes quadriques diagonales en quatre variables, Kloosterman a rencontré la même difficulté il y a un peu plus de soixante ans. La solution qu'il y a apportée se trouvera être une des clefs des Théorèmes 1 et 2. Elle mérite d'autant plus d'être présentée que Kloosterman lui-même l'a réutilisée pour obtenir la première majoration non triviale des coefficients de Fourier de formes modulaires paraboliques holomorphes ; repolie par Petersson, cette idée devait ultérieurement se développer dans les travaux de Selberg, Kuznecov, Iwaniec *et al.* pour étudier les sommes de Kloosterman en moyenne (via les formes modulaires non holomorphes), mettant en oeuvre ce que Hooley redécouvre dans un contexte différent et nomme "double Kloosterman reffinement".

A la suite de Farey d'ordre Q, c'est-à-dire l'ensemble des rationnels $\frac{a}{q}$ de $\mathbf{R}/\mathbf{Z}$, avec $(a,q) = 1$ et $q \leq Q$, Kloosterman associe la partition

5.3.a $$\mathbf{R}/\mathbf{Z} = \coprod_{q \leq Q} \coprod_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}'_{a,q} \ ,$$

où

5.3.b $$\mathfrak{M}'_{a,q} = \left]\frac{a+a'}{q+q'}\,,\ \frac{a+a''}{q+q''}\right]\ ;$$

on a noté $\frac{a'}{q'}$ et $\frac{a''}{q''}$ les voisins de $\frac{a}{q}$ dans la suite de Farey d'ordre Q.

Le défi consiste à déterminer les extrémités de $\mathfrak{M}'_{a,q}$ connaissant seulement a et q ! Pour cela, on utilise la propriété fondamentale de la suite de Farey :

5.3.c $$aq' - a'q = 1$$

Cela implique que l'on a

$$\mathfrak{M}'_{a,q} = \left]\frac{a}{q} - \frac{1}{q(q+q')}, \frac{a}{q} + \frac{1}{q(q+q'')}\right],$$

où la référence à a' et a'' a disparu.

Il reste à exprimer q' (et de même q'') en terme de a et q uniquement. On commence par remarquer que q' est bien localisé dans un intervalle de longueur q ; on a en effet

5.3.d $$Q < q + q' \leq Q + q$$

(la minoration provient de ce que $\frac{a}{q}$ et $\frac{a'}{q'}$ sont voisins dans la suite de Farey d'ordre Q, et donc $\frac{a+a'}{q+q'}$ n'appartient à cette suite).

Kloosterman remarque alors que la relation 5.3.c permet de localiser q' modulo q ; en notant $\bar{a}$ l'inverse de a modulo q, on a

5.3.e $$q' \equiv \bar{a}(\mathrm{mod} q)$$

Les deux relations 5.3.d et 5.3.e déterminent parfaitement q', et donc l'extrémité gauche de $\mathfrak{M}'_{a,q}$, en terme de a et q uniquement. On procède de même pour l'extrémité droite.

On notera que la partition de $\mathbf{R}/\mathbf{Z}$ considérée (5.3.a) présente cet aspect désagréable que les arcs $\mathfrak{M}'_{a,q}$ relatifs au même q ont des longueurs différentes. Pour pouvoir cependant les surperposer, Kloosterman développe leurs fonctions indicatrices en série de Fourier, introduisant un terme $\psi_q(\bar{a})$, où ψ_q est un caractère additif modulo q. Le cas le plus simple conduit aux sommes de Kloosterman

5.3.f $$K(m,n;q) := \sum_{a \bmod q}^{*} e\left(\frac{m\bar{a}+na}{q}\right)$$

pour lesquelles il donne une majoration non triviale.

5.4 Formes cubiques en 10 variables, d'après Heath-Brown

Les acteurs sont maintenant en place ! Soit F une forme cubique et P un nombre réel positif. L'intégrale

5.4.a $$r_F(P) = \int_0^1 \Big(\sum_{\|\mathbf{x}\|_\infty \leq P} e(\alpha F(\mathbf{x}))\Big) d\alpha$$

donne le nombre de solutions de l'équation $F(\mathbf{x}) = 0$, sous la condition $\|\mathbf{x}\|_\infty \leq P$. Si l'on montre que $r_F(P) > 1$ pour un certain P (par exemple en obtenant un équivalent, ou une minoration asymptotique de $r_F(P)$), on en déduit que l'équation $F(\mathbf{x}) = 0$ admet une solution non triviale.

On utilise alors la partition de Farey-Kloosterman (5.3.a), d'ordre $P^{3/2}$ (on se souviendra de la remarque introduite après la définition 3.2.a) : sur chaque arc majeur, on transforme la somme $\sum_{\|\mathbf{x}\|_\infty \leq P} e(\alpha F(\mathbf{x}))$ par la formule sommatoire de Poisson. Les contributions des arcs majeurs de même dénominateur sont alors regroupées par la méthode de Kloosterman. Bilan de l'opération : yaka évaluer les sommes

5.4.b $$S_u(q;\mathbf{b}) := \sum_{s=1}^{q}{}^{*} \sum_{\mathbf{c} \bmod q} e(\bar{s}F(\mathbf{c}) + us - \mathbf{b}.\mathbf{c}).$$

Si la voie est clairement tracée sur la carte (à nous Deligne !), la situation sur le terrain est bien plus rocailleuse et embroussaillée. Voici les deux obstacles majeurs que doit contourner Heath-Brown :

- Avec l'aide de Katz, il majore $|S_u(p;\mathbf{b})|$ par $\mathrm{O}(\mathrm{p}^{(\mathrm{n}+1)/2})$, ce qui est la compensation maximale espérée. La difficulté provient du terme $\bar{s}$ dans

5.4.b, ce qui complique la nature de la variété sur laquelle est effectuée la sommation (prisme à base hyperbolique), et donc la majoration de S_u, même dans la meilleure hypothèse où F est non-singulière.

- Le traitement des sommes $S_u(p^\ell; \mathbf{b})$, pour $\ell > 1$, est en principe plus simple ; malheureusement, la compensation maximale espérée pour $S_u(p^\ell; \mathbf{b})$ n'a pas toujours lieu. Heath-Brown montre que ce cas n'est pas très fréquent (on pourra aussi consulter S. Cohen, 1979) ce qui prouve qu'en moyenne, on peut majorer $|S_u(q; \mathbf{b})|$ par $O(q^{(n+1)/2+\varepsilon})$.

De fait, ce n'est pas l'intégrale 5.4.a qui est considérée, mais une version pondérée

$$\int_0^1 (\sum_{\|\mathbf{x}\|} w(\mathbf{x}) e(\alpha F(\mathbf{x}))) d\alpha \ ,$$

où le poids lisse w fait bien meilleur ménage avec la transformation de Fourier que la fonction indicatrice de la boite $\|\mathbf{x}\| \leq P$.

5.5 Formes cubiques en 9 variables, d'après Hooley

Cette section entretient avec la précédente une relation similaire à celle qui connecte la section 4.3 (somme de 8 cubes) à la section 4.2 (somme de s cubes pour $s > 8$).

Un premier effort consiste à poursuivre la méthode de Heath-Brown pour traiter les sommes $S_u(k; \mathbf{b})$ avec autant d'efficacité lorsque k est le carré d'un nombre sans facteur carré, que lorsque k est lui-même sans facteur carré ; le cas des puissances d'exposant supérieur à 2 peut alors être traité de façon élémentaire dans la plupart des cas. On gagne ainsi un facteur de l'ordre d'une puissance de P.

Quelques puissances du logarithme de P sont également économisées : les unes en choisissant un poids w à support compact, les autres par un lissage des extrémités des arcs $\mathfrak{M}'_{aq}$ définis en 5.3.b.

L'estocade est portée avec la complicité de Katz. Une estimation délicate des moments d'ordre 4 de sommes trigonométriques permet d'obtenir pour une famille de nombre premiers de densité positive des majorations dont la forme générale est

$$\sum_{\mathbf{a} \bmod p} \Big| \sum_{\substack{\mathbf{x} \bmod p \\ f(\mathbf{x}) \equiv 0(p)}} e(\mathbf{a}.\mathbf{x}/P) \Big| \leq (1-\delta) p^{(3n-1)/2}$$

avec une constante miraculeusement inférieure à 1 ! En moyenne sur les dénominateurs q des points de Farey (cf. l'alinea introductif de la section 5.3), on économise une puissance du logarithme de P, faible, mais décisive.

Pour terminer, signalons les travaux en cours de Hooley concernant le cas de formes nonaires dont les lieux singuliers de dimension zéro ne sont que des points doubles linéairement indépendants.

BIBLIOGRAPHIE

[1] R.C. BAKER, 1988 - *Diagonal cubic equations*, II, Acta Arithmetica 53 (1989) 217-250

[2] B.J. BIRCH, H. DAVENPORT, D.J. LEWIS, 1962 - *The addition of norm forms* Mathematika 9 (1962) 75-82.

[3] J. CHERLY, 1989 - *Sommes d'exponentielles cubiques dans l'anneau des polynômes en une variable sur le corps à deux éléments, et application au problème de Waring,* Thèse de Doctorat d'Etat, Univ. Bordeaux I, 1989.

[4] S.D. COHEN, 1979 - *The distribution of Galois groups and Hilbert's irreducibility theorem*, Proc. London Math. Soc. (3), 43 (1981) 227-250.

[5] J.-L. COLLIOT-THÉLÈNE, 1986 - *Arithmétique des variétés rationnelles et problèmes birationnels,* Proc. Int. Congress Math., (1987) 641-653.

[6] J.-L. COLLIOT-THÉLÈNE, J. SANSUC, Sir P. SWINNERTON-DYER, 1986 - *Intersection of two quadrics and Châtelet surfaces, II,* J. reine ang. Math. 374 (1987) 72-168.

[7] J.-L. COLLIOT-THÉLÈNE, P. SALBERGER, 1988 - *Arithmetic on some singular cubic hypersurfaces.* Proc. London Math. Soc. (3), 58 (1989) 519-549.

[8] H. DAVENPORT, 1962 - *Analytic methods for Diophantine equations and Diophantine inequalities*, Univ. Michigan, 1962.

[9] H. DAVENPORT - *Cubic forms in sixteen variables*, Proc. Roy. Soc. London ser. A, 272 (1963) 285-303.

[10] P. DELIGNE - *La conjecture de Weil, I,* Pub. Math. 43 (IHES, Paris, 1974) 273-307.

[11] J.-M. DESHOUILLERS, 1985 - *Problème de Waring pour les bicarrés*, Sem. Th. Nb. Bordeaux (1984-1985), exposé 14, 47 p.

[12] R.R. HALL, G. TENENBAUM, 1988 - *Divisors,* Cambridge University Press.

[13] G.H. HARDY, J.E. LITTLEWOOD, 1919-1928 - cf. Several papers on Partitio Numerorum, in G.H. HARDY's collected papers, Oxford, 1966.

[14] G.H. HARDY, S. RAMANUJAN, 1917 - *Asymptotic formulae in combinatory analysis,* Proc. London Math. Soc. (2), 17 (1918) 75-115.

[15] D.R. HEATH-BROWN, 1982 - *Cubic forms in ten variables*, Proc. London Math. Soc. (3), 47 (1983) 225-257.

[16] C. HOOLEY, 1977 - *On a new technique and its applications to the theory of numbers*, Proc. London Math. Soc. (3), 38 (1979) 115-151.

[17] C. HOOLEY, 1984 - *On Waring's problem*, Acta Math. 157 (1986) 49-97.

[18] C. HOOLEY, 1987 - *On nonary cubic forms*, J. reine ang. Math. 386 (1988), 32-98.

[19] H. IWANIEC, 1977 - *On sums of two norms from cubic fields*, in *Journées de théorie additive des nombres* (Université de Bordeaux I, 1977)

[20] N.M. KATZ, - *Perversity and exponential sums*, à paraître.

[21] H.D. KLOOSTERMAN, 1925 - *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. Acta Math. 49 (1926) 407-464.

[22] H.D. KLOOSTERMAN, 1925 - *On the representation of numbers in the form* $ax^2 + by^2 + cz^2 + dt^2$. Proc. London Math. Soc. (2), 25 (1926) 143-173.

[23] G. LACHAUD, 1982 - *Une présentation adéligne de la série singulière et du problème de Waring*, Ens. Math. 28 (1982) 139-169.

[24] Ju.V. LINNIK - *On the representation of large numbers as sums of seven cubes.* Doklady Akad. Nauk SSSR 35 (1942), 162 and Mat. Sbornik 12 (1943) 218-224.

[25] L.J. MORDELL 1936 - *A remark on indeterminate forms in several variables*, J. London Math. Soc. 12 (1937) 127-129.

[26] H. RADEMACHER, 1969 - *Topics in Analytic Number Theory*, Springer-Verlag, 1973.

[27] R.G. VAUGHAN, 1981 - *Some remarks on Weyl sums*, Coll. Math. Soc. Janos Bolyai 34 (Halasz ed.) Amsterdam, 1984, 1585-1602.

[28] R.G. VAUGHAN, 1981 - *The Hardy-Littlewood method*, Cambridge, 1981.

[29] R.G. VAUGHAN, 1985 - *On Waring's problem for cubes*, J. reine ang. Math. 365 (1986) 122-170.

[30] R.G. VAUGHAN, 1987 - *On Waring's problem for cubes, II*, J. London Math. Soc. 39 (1989) 205-218.

[31] H. WEYL, 1914 - *Über die Gleichverteilung von Zahlen mod. Eins*, Math. Ann. 77 (1916) 313-352.

Jean-Marc DESHOUILLERS

Centre de Recherche en Mathématiques
Université Bordeaux I
351, cours de la Libération
F-33405 TALENCE CEDEX

dezou at frbdx11.bitnet