JOURNAL DE THÉORIE DES NOMBRES DE BORDEAUX

JEAN-MARC DESHOUILLERS

Study of rational cubic forms via the circle method [after D.R. Heath-Brown, C. Hooley, and R.C. Vaughan]

Journal de Théorie des Nombres de Bordeaux 2e série, tome 2, nº 2 (1990), p. 431-450

<http://www.numdam.org/item?id=JTNB_1990__2_2_431_0>

Séminaire de Théorie des Nombres,
Bordeaux **2** *(1990), 431–450*

Study of rational cubic forms via the circle method. [after D.R. Heath-Brown, C. Hooley, and R.C. Vaughan]*

par JEAN-MARC DESHOUILLERS

The **circle method** due to Hardy, Littlewood and Ramanujan, is a powerful tool in the study of Diophantine problems of the type $P(x_1, ..., x_s) = 0$, when the number of variables is large compared with the degree of the polynomial P. The last incarnations of this method in particular enabled Heath-Brown to show that every non-singular rational cubic form in 10 variables represents 0, Hooley to shew that 9 variables suffice when there is no local obstruction and Vaughan to give an asymptotic expression for the number of representations of an integer as a sum of 8 cubes, as well as a good lower bound for the number of representations as a sum of 7 cubes.

CONTENTS

* L'auteur remercie le Séminaire de Théorie des Nombres de Bordeaux et le Séminaire Bourbaki pour leur permission de publier simultanément la version française de ce texte dans les actes du Séminaire Bourbaki (exp. 720).

Manuscrit reçu le 4 mai 1990

Introduction

The problem whether every positive integer is a sum of four squares, which may already have been considered by the ancient Greeks, has been studied by many a mathematician in the seventeenth and eighteenth centuries, and was finally solved by Lagrange in 1770. The interest in and the difficulty of this question come from the interplay between the additive and multiplicative structures of the integers.

Similar conjectures can be easily formulated ; most of the time they are intractable, but raise new mathematical developements. Historically important are Goldbach's problem (1742), **every even integer is a sum of two primes** (at that time, 1 was considered a prime), and Waring's problem (1770), **every integer is a sum of at most 4 squares, 9 cubes or 19 biquadrates**, extended to higher powers in 1782.

Additive number theory deals with those questions ; we aim here to present the so-called **circle method** which has been introduced by Hardy and Ramanujan in 1917, and improved upon by Hardy and Littlewood a few years later. This septuagenary tool has lost none of its vigour ; it is still used with benefit, as well for getting asymptotic evaluations, as we shall see here, as for effective and efficient numerical estimates. Through the -limited- study of diagonal forms (and essentially of diagonal cubic forms) we perform this exhibition, suggesting some steps in the proofs of the following results

THEOREM 1.- (D.R.Heath-Brown, 1982). *Let* $F(\mathbf{x}) := F(x_1, ...x_s)$ *be a non singular rational cubic form. For* s *larger than or equal to* 10, *there exists* $\mathbf{x}$ *in* $\mathbb{Q}^s \setminus \{0\}$ *such that* $F(\mathbf{x}) = 0$.

THEOREM 2.- (C. Hooley, 1987).*Let* $F(\mathbf{x})$ *be a non singular rational cubic form in 9 variables. The equation* $F(\mathbf{x}) = 0$ *has a rational non trivial solution if and only if it has a non singular solution in each p-adic field* $\mathbb{Q}_p$. *Theorem 3.- (R.C. Vaughan, 1985).Let* $r_8(N)$ *denote the number of representations of the integer* N *has the sum of the cubes of eight positive rational integers. As* N *tends to infinity, one has*

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

where

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

One conjectures that the non-singularity condition may be raised in the statement of Theorem 1. Davenport showed in 1963 that every rational cubic form in at least 16 variables represents 0 ; even in the case of non singular forms this was the best known result before Heath-Brown's. In the case of nonary forms, the local condition can't be dispensed with, as Mordell showed in 1936. Theorem 3 was one of Davenport's favorite conjectures and I was told that he suggested its study to all of his research students.

To end this introduction, let us mention the work of Colliot-Thélène, Sansuc and Sir Swinnerton-Dyer, 1986 (a survey of their work is presented in Colliot-Thélène, 1986). Attacking the problem through the algebraic geometry, they get among other the presently best known results concerning systems of quadratic forms. As far as cubic forms are concerned, this approach leads to the proof of the following, which can usefully be compared with Theorem 2 (less variables, but more subtle geometric conditions).

THEOREM 4.- *(J.-L.Colliot-Thélène et P. Salberger, 1988). Let* K *be a number field and* $X \subset \mathbb{P}^n_K$ *a cubic hypersurface defined over* K, *with* $n \geq 3$.

If X contains a set of 3 conjugate singular points, and if X admits rational points over all the completions of K, then X admits a rational point over K.

1 Heuristic approach : the singular integral

1.1 Some computed data

Let us look at a table which gives, for every integer N up to 40,000 the minimal number of summands needed to writer N as a sum of positive integral cubes : the numbers 23 and 239 are the only ones for which 9 cubes are needed ; fifteen other integers, the largest of which is 8,402, require 8 cubes, and for all the other integers 7 cubes suffice. Would this table be extended to 10^{15}, we would get the feeling that, from some point onward, 4 cubes suffice... Thus, it seems easier to represent large integers than small ones.

1.2 Study of the number of representations

This aspect was not taken into account in the studies performed during the second half of the nineteeth century, from Liouville who showed in 1859 that every integer is a sum of at most 53 biquadrates, to Hilbert who proved in 1909 that every integer is a sum of a finite number of k-th powers, and Kempner who concluded a work by Wieferich, establishing in 1912 that every integer is a sum of at most 9 cubes.

The circle method, introduced in the context of Waring's problem by Hardy and Littlewood, takes into account this ability of large integers to be more easily represented ; to know whether the integer N can be represented as a sum of s integral k-th powers, they tried to determine the **asymptotic behaviour of the number of representations** *of N as a sum of k-th powers.Thus, they concentrated on large integers, hence the success of their method.*

1.3 Integral expression for the number of representations

Let us first fix some notation. k represents an integer which is at least 2. We can restrict ourselves to the value 3.

N denotes an integer, which is assumed to tend to infinity.

For a given positive integer s, we denote by $r_s(N)$ the number of representations of N as a sum of s k-th powers

$e(\cdot)$ denotes the complex exponential $\exp(2\pi i.)$

The reader will easily give a proof of relation

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

by appealing, either to the orthogonality of characters $e(h.)$, or to Cauchy's integral formula. We give here a probabilistic proof, leaving aside its interest for a given explicit computation (Deshouillers, 1985).

We consider s independent random variables $X_1, ..., X_s$ with common law $\lambda \sum_{n \le N^{1/k}} \delta(n)$, where $\delta(a)$ denotes the Dirac measure at the point a, and the normalizing factor λ is equal to $\lfloor N^{1/k} + 1 \rfloor^{-1}$. Each random variable X_i^k follows the law $\lambda \sum_{n \le N^{1/k}} \delta(n^k)$. The law of the variable $X := X_1^k + ... + X_s^k$ is the s-th convolution power of that of each X_i^k ; it is thus equal to $\lambda^s \sum_m r_s^*(m) \delta(m)$, where $r_s^*(m)$ is the number of ways to write m as a sum of s integral k-th powers, each of which is at most N ; the coefficient $r_s^*(m)$ is readily obtained from the characteristic function (Fourier series) of X, which is the s-th power of that of X_1^k. Formula 1.3.a. follows from that fact and the trivial equality of $r_s(N)$ and $r_s^*(N)$.

1.4 Heuristic order of magnitude of $r_s(N)$

We give a continuous approximation to the problem under consideration : let $Z_1, ... Z_s$ be s independent random variables each of which is uniformly distributed on $[0, N^{1/k}]$, and let us denote by Z the sum $Z_1^k + ... + Z_s^k$. The characteristic function (alias Fourier transform) of Z is the s-th power of that of Z_1^k ; by inverse Fourier transform, we get the density $\rho_s(t)$ of Z at t :

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

The right-hand side is called the **singular integral**. *When $t = N$, we get*

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

since one has

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

Thus, the mean-value of $r_s(N)$ is $N^{s/k-1}$, up to an Eulerian factor. It is worth noticing that the singular integral does occur in the asymptotic formula for the number of representations as a sum of 8 cubes (cf. Theorem 3).

2 A p-adic approach : the singular series

Having explained the occuring of the singular integral in Theorem 3, we turn to the interpretation of the **singular series** $\mathfrak{S}(N)$, *according to Hardy and Littlewood's terminology.*

2.1 Number of solutions of the congruence $m_1^k+...+m_s^k \equiv N(\bmod q)$

Let us denote by $M(q)$ the number of solutions of the congruence under consideration. The equality

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

follows easily from the orthogonality relations

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

and is the counterpart, in $\mathbb{Z}/q\mathbb{Z}$, to the integral formula 1.3.a. By rearranging the right hand side of 2.1.a according to the value of (r,q), we get

$$M(q) = \frac{1}{q}\sum_{d|q}\sum_{\substack{a=1 \\ (a,d)=1}}^{d}\left(\frac{q}{d}\sum_{m=1}^{d} e(am^3/d)\right)^s e(-aN/d),$$

or

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

where

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

Now we start to enjoy the fragrance of Theorem 3 !

2.2 Interpretation of the singular series

As it can be seen either directly from the Chinese remainder theorem, or indirectly through 2.1.b, the function G is multiplicative, and this enables one to write the singular series

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

as an Euler product

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

By 2.1.b, we thus get

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

Noticing that $p^{\ell(s-1)}$ is the cardinality of a hyperplane in $(\mathbb{Z}/p^\ell\mathbb{Z})^s$, we may interpret each factor in $\mathfrak{S}(N)$ as a density for the solutions of $x_1^k + \ldots + x_s^k = N$ in $\mathbb{Z}_p$.

To the reader who might be tempted to go further in this direction we recommand the paper of Lachaud, 1982, for an adelic formulation of the circle method.

3. Classical Farey dissection : major arcs, singular series and integral

We are now concerned with the computation of $r_s(N)$ from the integral formula 1.3.a. The main expression in the integrand is the exponential sum

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

Its modulus is clearly maximal when α is an integer ; we start by studying the contribution to $r_s(N)$ of those α's close to 0 in $\mathbb{R}/\mathbb{Z}$, or, what is the same under the identification of $\mathbb{R}/\mathbb{Z}$ to a neighbourhood of 0 in $\mathbb{R}$, of those α's close to 0.

3.1 Contribution of the first major arc (α close to 0)

Since $\mathcal{S}(\alpha)$ is a continuous function of α, and $\mathcal{S}(0) = P$ (this equality justifies the clumsy definition of P), analysis allows us to evaluate $\mathcal{S}(\alpha)$ for α close to zero.

Let us suppose that $|\alpha| \leq \epsilon N^{-1}$, where ϵ is any function of N tending to zero at infinity. By Taylor's formula, we get

$$\mathcal{S}(\alpha) = P + o(P) \text{ and } e(-\alpha N) = 1 + o(1), \text{ hence}$$

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

One should notice that the contribution to $r_s(N)$ of such an interval around 0 has the same order of magnitude as the heuristic value.

Indeed, we used Taylor's formula, which is somewhat weak (don't we teach it to our first year students ?). The Poisson's summation formula (when do we teach it to our students ?) is a much more efficient tool. Let

$$f(x) := \begin{cases} e(\alpha x^k) \text{ for } 0 \leq x \leq P \\ 0 \text{ otherwise} \end{cases}$$

and let $\hat{f}$ denote its Fourier transform ($\hat{f}(t) := \int_{-\infty}^{\infty} f(x)e(xt)dx$) ; one has

$$\sum_{n \in \mathbb{Z}} f(x) = \sum_{\nu \in \mathbb{Z}} \hat{f}(\nu) + O(1).$$

hence

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

When $|\alpha|$ is small enough ($k|\alpha|P^{k-1} \leq 1/2$), the function $e(\alpha x^k + \nu x)$ does oscillate on $[0, P]$ for $\nu \neq 0$, and the integral $\int_0^P e(\alpha x^k + \nu x)dx$ is small, as can be seen by integrating by parts ; it is not difficult to show that one has

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

and it is then a routine computation to check that, for $s \geq k+1$, *the contribution of the interval*

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

is equivalent to $\rho_s(N)$, *the mean number of representations (cf. 1.4.a and 1.4.b) !*

3.2 Contribution of the major arcs : distribution of powers in arithmetic progressions

In section 2.2, we rewrote the singular series in terms of the number of solutions of the congruences $x_1^k + ... + x_s^k \equiv N(\mod q)$. *We wish to explain here how the mean value* $G(q)$ *of Gauss sums occurs when studying the contribution to* $r_s(N)$ *of small intervals centered at rational points with* q *as their denominator.*

Let us start by estimating $S(a/q)$; *we have*

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

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

There is no reason why the Gauss sum $\sum_{m=1}^{q} e(am^k/q)$ *should vanish, and indeed it usually does not ; for example, in the case when* $k=3$ *and* $a/q = 1/4$, *it is equal to 2. This corresponds to irregularities in the distribution of the* k*-th powers in arithmetic progressions. Hence,* $S(a/q)$ *may have an order of magnitude comparable with that of* $S(0)$. *We study therefore the local behaviour of* S *around* a/q *as we did around 0 : we introduce the* **major arcs**

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

where $0 < a < q$, $(a,q) = 1$ and $q \leq Q$. We should mention that the choice of Q is at that stage somewhat irrelevant ; generally Q is to be taken as a power of P, e.g. P itself. It's important to notice that choosing Q greater than P is possible, but very delicate : it is equivalent to studying the distribution of a set of P integers in classes modulo an integer larger than P.

The Poisson's summation formula allows us to approximate

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

Collecting the contributions of the different major arcs, the union of which is denoted by $\mathfrak{M}$, we get

PROPOSITION. *For $s \geq 4k$ (and $s \geq 4$ in the case of cubes), there exists an $A > 0$ such that, when N tends to infinity, one has*

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

We recall that $\rho_s(N) = \frac{\Gamma(1+1/k)^s}{\Gamma(s/k)} N^{s/k-1}$.

4 Classical Farey dissection : minor arcs

Although it is the "core" in a traditional use of the circle method, we treat this part briefly which depends in a fundamental way on the diagonal nature of the forms implied in Waring's problem.

The union of the major arcs does not cover $\mathbb{R}/\mathbb{Z}$; a simple way to see this is to compute the total length of the major arcs. In the case of cubes, we have

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

and so the total length of the major arcs tends to 0 when N tends to infinity ! We call **minor arcs** the complementary set of the major arcs, the **minor arcs** and denote it by $\mathfrak{m}$.

4.1 Weyl upper bound : 13 cubes

The sum $\mathcal{S}(\alpha)$, for α irrational, has been considered under a "dual" look by Weyl in 1916 : for given α, and P tending to infinity, he showed that

$\mathcal{S}(\alpha)/P$ tends to 0. From this point of view, that we do not develop here, the result corresponds to the uniform distribution of the sequence (αn^k) in $\mathbb{R}/\mathbb{Z}$. Weyl's method for majorizing $|\mathcal{S}(\alpha)|$ leads, in the case of cubes, to the upper bound valid for every $\epsilon > 0$.

4.1.a $$|\mathcal{S}(\alpha)| = \mathrm{O}_\epsilon(p^{3/4+\epsilon}) \text{ uniformly for } \alpha \in m.$$

(For k-th powers, the exponent is $1 - 2^{1-k}$).

From the upper bound 4.1.a, one easily deduces

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

Combining this result with 3.2.b (contribution of major arcs), we get an asymptotic formula for the number of representations as sums of s cubes as soon as

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

i.e. as soon as s is strictly larger than 12. In the same way, we get an asymptotic formula for the number or representations as sums of $k\ 2^{k-1} + 1$ integral k-th powers.

4.2 Parseval relation : 9 cubes

Though relation 4.1.a presents some weakness in that its exponent is probably not the best possible one (considering the random walk with step $e(\alpha n^3)$ one would expect 1/2 to be right exponent), the real strength of that formula is its uniformity over $\mathfrak{m}$. In applying 4.1.a to 4.1.b we waste this uniformity since we look only for an ℓ^s norm. Parseval's relation provides us with an exponent $s/2$ in 4.1.b for $s = 2$, which is common, and also for $s = 4$, which is a little more subtle : the identity $x^3 + y^3 = (x+y)(x^2 - xy + y^2)$ permits one to majorize $r_2(n)$ by twice the number of divisors of n, hence the upper bound

4.2.a $$r_2(n) = O_\epsilon(n^\epsilon) \ .$$

For $s \geq 4$, we may thus write :

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

wich leads to an asymptotic formula for the number of reprentations of an integer as a sum of s cubes as soon as

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

that is to say as soon as s is strictly larger than 8, and, since s is an integer, it means only that s should be as least 9.

In the case of k-th powers, Hua could suitably generalize Parseval's relation and obtained the upper bound

$$\text{4.2.b} \qquad \int_0^1 |S(\alpha)|^{2^k}\,d\alpha = O_{\epsilon,k}(P^{2^k-k+\epsilon})$$

which leads to an asymptotic formula for $r_s(N)$ when $s \geq 2^k+1$.

We just briefly mention here the works by Vinogradov (improvement on Weyl's lemma for $k \leq 12$), Heath-Brown (improvement on Hua's lemma for $k \geq 6$), Vinogradov, Davenport, Vaughan and others (solubility of $x_1^k + \cdots + x_s^k = N$ when s has the order $k \log k$, without estimating $r_s(N)$).

4.3 Number of representations as a sum of 8 cubes, after Vaughan

Let us go back to Hua's inequality 4.2.b for cubes. It implies

$$\int_0^1 |S(\alpha)|^8 d\alpha = O_\epsilon(P^{5+\epsilon})$$

whereas the contribution of the major arcs has order P^5. As was noticed by Hooley, using mean value results for divisor functions permits one to replace P^ϵ by a power of $\log P$; a result by Hall and Tenenbaum even leads to

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

and therefore to

$$\text{4.3.b} \qquad r_8(N) = O_\epsilon(N^{5/3}\log\ N)^\epsilon).$$

Theorem 3 directly comes from the existence of a real $C>0$ such that

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

We can see how narrow is the margin between 4.3.a and 4.3.b. To cover it, Vaughan introduces several dissections : on $\mathfrak{m}$, according to the diophantine properties of α, and on the integers between 0 and P (on which the summation for $S(\alpha)$ is performed), according to their aritmetical properties. He can reinterpret the new diophantine equations and save a logarithm through the estimation of the number of their solutions. Upper bounds of type 4.3.b are then suffisant, and one can thus take as a suitable C in 4.3.c any integer strictly less than 1.

4.4 Number of representations as a sum of 7 cubes

This iterative method is the root of the lower bound

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

obtained by Vaughan in 1987 for some $c > 0$ and any sufficiently large N. R. C. Baker and J. Brüdern recently entended this result to diagonal forms in 7 variables.

In 1942, Linnik could prove the positivity of $r_7(N)$ for sufficiently large N, by different considerations (ternary quadratic forms, distribution of prime numbers in arithmetical progressions).

An asymptotic expression for $r_7(N)$ has been conditionally given by Hooley, 1984, under the validity of the Riemann hypothesis for some global Hasse-Weil L-functions.

5 - Non diagonal cubic forms

5.1 A non typical situation : the case of norm forms

As we have just seen, proving through the circle method that every sufficiently large integer is a sum of seven cubes, is fairly recent. The abovementionned result by Davenport concerning cubic forms in 16 variables, as well as Theorem 1 and 2 suggest that general forms are harder to handle. Theorem 4 illustrate a possible use of certain geometrical considerations. It is also possible to make use of some algebraic features, as in the following results, the first of which deals with cubic forms in 7 variables (and more generally with forms of degree k in $2k+1$ variables).

THEOREM 5. - (B.J. Birch, H. Davenport, D.J. Lewis, 1962). *Let K_1 (resp. K_2) be a cubic number field and $N_1(x_1, y_1, z_1)$ (resp. $N_2(x_2, y_2, z_2)$) the norm form expressed with respect to a given integral bases. If the equation*

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

has a non-singular solution modulo p for every prime p which divides $d(K_1)d(K_2)$ (the product of the discriminants of K_1 and K_2), then it has infinitely many solutions with rational integral arguments.

By sieve methods, H. Iwaniec has even obtained results concerning the number of representations by some cubic forms in 6 variables. For the sake of simplicity, we quote only a corollary of this result :

THEOREM 6. - (H. Iwaniec, 1977) *Let $K/\mathbb{Q}$ be a cubic Galois extension ; we denote by N_K the norm form with respect to a given integral basis. (There exists an integer D and a family H of classes mod D such that a prime number p totaly splits in K if and only if p is congruent to an element of H modulo D).*

Every sufficiently large even integer which is congruent modulo D to the sum of two elements of H can be represented as $N_K(x_1, y_1, z_1) + N_K(x_2, y_2, z_2)$ with integral arguments.

5.2 Extension of the major arcs, after Vaughan

In the first four sections, we consider only **diagonal** forms. All that concerns majors arcs can indeed be extended to non diagonal forms, thanks to Fourier transform on $\mathbb{Z}^s$. The first really curcial use of the diagonal aspect occured in Weyl's inequality (formula 4.1.a).

At the end of the 70's, Vaughan noticed that the choice of the major arc $\mathfrak{M}_{0,1}$ we made in 3.1.c was only governed by a will to neglect as many terms as possible in Poisson summation formula 3.1.a in order to get 3.1.b. if a larger major arc is chosen, the function $e(\alpha x^k + \nu x)$ does not necessarily oscillate any longer, and the number of terms that can't be neglected increases with the size of the major arc. A decent extension still permits to control the sum $\sum_{N_1<\nu<N_2} \int_0^P e(\alpha x^k + \nu x)dx$ in which each term is taken care of by the stationary phase method (expansion around the point where $k\alpha x^{k-1} + \nu$ vanishes, leading to a Fresnel integral). Global out put : in the case of cubes, one gets exactly the 3/4 exponant of Weyl upper bound, and for higher powers an exponant which is at least 1, and this has little value. However, one should notice that Vaughan's idea has been used for biquadrates, in a context where a certain numerical subtlety was looked for. (Deshouillers, 1985). Vaughan's method permits to write $S(\alpha)$ as a trigonometrical sum which, trivially treated, leads to Weyl upper ; but as a further advantage, we have the possibility of keeping that sum explicit, for subsequent cancellation. The reader, whom I thank for still being aboard, should now be convinced that Theorem 1 for a non-singular cubic form

in 13 variables depends on a good knowledge of generalized Gauss sums (Deligne's Theorem) in the same way as "13 cubes" depends on the mere Weyl's upper bound.

Before explaining how one gains 3 extra variables, I mention the use of Vaughan's method by Cherly, 1989, who obtained a Weyl type extimate for cubic trigonometrical sums on $\mathbb{F}_2[X]$, which is not possible to get by the classical tools since, in $\mathbb{F}_2$, one has $3! = 0$.

5.3 Intermezzo : Farey - Kloosterman dissection

Since we wish to keep explicit the above-mentionned trigonometrical sums for any $\alpha \in \mathbb{R}/\mathbb{Z}$, we need a **partition** of $\mathbb{R}/\mathbb{Z}$ consisting of major arcs. When studying diagonal quadratic forms in four variables, Kloosterman met the same difficulty over sixty years ago. The solution he gave turns out to be one of the keys to Theorems 1 and 2. it is worth mentionning that Kloosterman himself re-used it to obtain the first non trivial upper bound for Fourier coefficients of holomorphic modular cusp forms ; polished by Peterson, this idea was to be further developped by Selberg, Kuznecov, Iwaniec *et al.* for studying Kloosterman sums on average (via non holomorphic cusp forms), introducing what Hooley rediscover in a different context, and calls "double Kloosterman reffinement".

To the Farey sequence of order Q, i.e. the set of rationals $\frac{a}{q}$ in $\mathbb{R}/\mathbb{Z}$ with $(a,q) = 1$ and $q \leq \mathbb{Q}$, Kloosterman connects the partition

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

where

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

the neighbours of $\frac{a}{q}$ in the Farey sequence of order Q have been denoted by $\frac{a'}{q'}$ and $\frac{a''}{q''}$.

The challenge is to determine the endpoints of $\mathfrak{M}'_{a,q}$ from the mere knowledge of a and q ! In that aim, we use the fundamental property of Farey sequences

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

This implies

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

where nor a' nor a'' are explicity refered to.

It remains to express q' (and similarly q'') in terms of a and q only. We first notice that q' is well localised in an interval of lenght q ; we have indeed

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

(the lower bound comes from the fact that $\frac{a}{q}$ and $\frac{a'}{q'}$ are neighbours in the Farey sequence of order Q, so that $\frac{a+a'}{q+q'}$ can't belong to it).

Kloosterman then notices that relation 5.3.c permits to localise q' modulo q ; denoting by $\overline{a}$ the inverse of a modulo q, we have

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

Both relations 5.3.d and 5.3.e perfectly determine q', thus the left endpoint of $\mathfrak{M}'_{a,q}$ in terms of a and q only. The right endpoint is treated in a similar way.

An important and annoying aspect of the partition of $\mathbb{R}/\mathbb{Z}$ considered in 5.3.a is that the arc $\mathfrak{M}'_{a,q}$ related to the same q have different lengths. In order to treat at the same time their contributions to the integral 1.3.a, Kloosterman expands their characteristic functions in Fourier series, thus introducing a term $\psi_q(\overline{a})$, where ψ_q is an additif character modulo q. The simplest case leads to the so-called Kloosterman sums

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

for which he gives a nontrivial upper bound.

5.4 Cubic forms in 10 variables, after Heath-Brown

Actors are now on the stage ! Let F be a cubic form and P a positive real number. The integral

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

gives the number of solutions of the equation $F(\mathbf{x}) = 0$, under the condition $||\mathbf{x}||_\infty \le P$. If we show that $r_F(P) > 1$ for a certain P (for example in getting an asymptotic expression, or an asymptotic lower bound for $r_F(P)$), we deduce that the equation $F(\mathbf{x}) = 0$ has non trivial solution.

We then use the Farey-Kloosterman partition 5.3.a, with the order $Q = P^{3/2}$ (one should keep in mind the remark formulated after definition 3.2.a): on each major arc, the sum $\sum_{||\mathbf{x}||_\infty \le P} e(\alpha F(\mathbf{x}))$ is transformed through the use of the Poisson summation formula. The contributions of those major arcs related to the same denominator are then gathered by Kloosterman's method. Output : we just have to evaluate the sums

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

On the map, the road is clear (Deligne with us !), but on the ground, the situation is more rocky and bushy. Here are two main difficulties that Heath-Brown has to overcome :

- With the help of Katz, he gets the upper bound $O(p^{(n+1)/2})$ for the modulus of the sum $S_u(p;\mathbf{b})$, which correspond to the maximal expected cancellation. The difficulty comes from the term $\overline{s}$ in 5.4.b, which makes more intricate the geometrical nature of the variety on which the sum is performed (prism with hyperbolic base), and consequently majorizing $|S_u|$ is harder, even in the best case when F is non-singular.

- In principle, it is easier to deal with sums $S_u(p^\ell;\mathbf{b})$, for $\ell > 1$; unfortunately, the maximal expected cancellation in $S_u(p^\ell;\mathbf{b})$ is not always observed. Heath-Brown shows that this cannot occur to often (one can also consult S. Cohen, 1979) and proves that, on average, $O_\epsilon(q^{(n+1)/2+\epsilon})$ is an admissible upper bound for $|S_u(q;\mathbf{b})|$ with arbitrary ϵ.

Indeed, instead of the integral 5.4.a, Heath-Brown uses the weighted one

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

where the smooth weight w lives in better harmony with the Fourier transform than the characteristic function of the box $||\mathbf{x}|| \le P$.

5.5 Cubic forms in 9 variables, after Hooley

This section has with the previous a relationship similar to that which correct section 4.3 (sums of 8 cubes) with section 4.2 (sums of s cubes for $s > 8$).

A first effort consists in pursuing Heath-Brown method in order to treat sums $S_n(k;\mathbf{b})$ with the same efficiency when k is the square of a squarefree number, as when k is itself squarefree ; the case of higher powers can be elementary treated in most cases. In this way, a factor of the order P^2 may be won.

A few powers of $\log P$ are gained as well : some by choosing a compact supported weight w, some others by smoothing the ends of the arcs $\mathfrak{M}'_{a,q}$ defined in 5.3.b.

The final thrust needs the complicity of Katz. A delicate estimate of four power moments of trigonometrical sums allows to get, for a family of prime numbers with positive density, upper bounds of the shape

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

with a constant strictly less than 1! On average over the denominators of Farey points (cf. the introduction to section 5.3), one saves a power of $\log P$, small, but crucial.

Let us last mention current works by Hooley, concerning nonary cubic forms for which singular loci of dimension zero are only linearly independant double points.

REFERENCES

R.C. BAKER, 1988, *Diagonal cubic equations II*, Acta Arith. **53** (1989), 217–250.

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

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).

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

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

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

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

H. DAVENPORT, 1962, *Analytic methods for Diophantine equations and Diophantine inequalities, Univ. Michigan, (1962).*

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

P. DELIGNE, *La conjoncture de Weil, I*, Pub. Math. **43** (IHES, Paris, 1974), 273–307..

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

R.R. HALL, G. TENENBAUM, 1988, *Divisors*, Cambridge University Press.

G.H. HARDY, J.E. LITTLEWOOD, 1919-1928, *cf. several papers on Partitio Numerorum, in G.H. HARDY's collected papers*, Oxford, (1966).

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

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

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

C. HOOLEY, 1984, *On Waring's problem*, Acta Math. **157** (1986), 49–97.

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

H. IWANIEC, 1977, *On sums of two norms from cubic field, in Journées de Théorie additive des Nombres (Université Bordeaux I, 1977).*

N.M. KATZ, *Perversity and exponential sums.* à paraître

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.

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.

G. LACHAUD, 1982, *Une présentation adélique de la série singulière et du problème de Waring*, Ens. Math. **28** (1982), 139–169.

Ju.V. LINNIK, *On the represention of large numbers as sums of seven cubes*, Doklady Akad. Nauk SSSR **12** (1943), 218–224.

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

H. RADEMACHER, 1969, *Topics in Analytic Number Theory, Springer-Verlag.*

R.C. VAUGHAN, 1981, *Some remarks on Weyl sums*, Coll. Math. Soc. Janos Bolyai **34** (Halász ed.) Amsterdam (1984), 1585–1602.

R.C. VAUGHAN, 1981, *The Hardy-Littlewood method*, Cambridge (1981).

R.C. VAUGHAN, 1985, *On Waring's problem for cubes*, J. reine ang. Math. **365** (1986), 122–170.

R.C. VAUGHAN, 1987, *On Waring's problem for cubes, II*, J. London Math. Soc. **39** (1989), 205–218.

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

Centre de Recherche en Mathématiques de Bordeaux, C.N.R.S. U.A. 226
Université Bordeaux I
351, cours de la Libération
33405 Talence Cedex, FRANCE.
dezou@ frbdx11. bitnet