ANNALES SCIENTIFIQUES DE L'É.N.S.

JÖRG BRÜDERN

A sieve approach to the Waring-Goldbach problem. I. Sums of four cubes

Annales scientifiques de l'É.N.S. 4e série, tome 28, nº 4 (1995), p. 461-476

<http://www.numdam.org/item?id=ASENS_1995_4_28_4_461_0>

Ann. scient. Éc. Norm. Sup.,
4^e série, t. 28, 1995, p. 461 à 476.

A SIEVE APPROACH TO THE WARING-GOLDBACH PROBLEM, I: SUMS OF FOUR CUBES

BY JÖRG BRÜDERN

ABSTRACT. – The problem of representing integers as the sum of k-th powers of primes is known as the Waring-Goldbach problem. Traditionally results on this problem are obtained by reference to auxiliary estimates from the "ordinary" Waring problem, which are then combined with Vinogradov's estimates for exponential sums over primes. Here we describe an alternative approach, based on the linear sieve and the circle method, and show that almost all natural numbers $n \equiv 4 \bmod 24$ can be written as $n = p_1^3 + p_2^3 + p_3^3 + x^3$ where p_1, p_2, p_3 are primes, and x has at most four prime factors. Our method has the advantage that one can deal with fewer variables than is possible by Vinogradov's method, but sometimes detects an "almost prime" rather than a prime.

1. Introduction

Alongside with the traditional theory of Waring's problem there is the parallel question of solving the diophantine equation

$$x_1^k + x_2^k + \ldots + x_s^k = n \tag{1.1}$$

in primes x_i. This problem is usually referred to as the Waring-Goldbach problem. Since the work of Vinogradov [13] and Hua [8] on exponential sums over primes problems in this class are within the competence of the Hardy-Littlewood circle method. However, mainly due to our poor knowledge of the distribution of primes in arithmetic progressions, a solution of the Waring-Goldbach problem requires more variables than the original Waring problem (that is, solving (1.1) in positive integers, for sufficiently large n.) We illustrate the difference in the case of cubes. It is conjectured that all large integers n are the sum of four positive cubes, and indeed that all large $n \equiv 4 \bmod 18$ can be written as the sum of four cubes of primes. Davenport [2] showed that almost all (in the sense usually adopted in analytic number theory) natural numbers can in fact be represented as the sum of four positive cubes, and also obtained an estimate on the number of exceptions. A similar result on cubes of primes requires five variables (*see* Hua [8]). If all large numbers n are to be represented in the form $n = x_1^3 + \ldots + x_s^3$ then $s = 7$ suffices for Waring's problem, but

This paper is a modified account of parts of chapter 3 from the author's Habilitationsschrift [1] at Georg-August-Universität Göttingen which has been accepted on 6. December 1991.

the restriction of the x_i to primes make in necessary to increase the number of variables to $s = 9$, and to impose a congruence condition on n.

In the present paper we develop a method which at least "approximates" the Waring-Goldbach problem, without inflating the number of variables. In the context of sums of cubes our techniques yield the following result.

THEOREM. – *Almost all natural number* $n \equiv 4 \bmod 18$ *can be written as*

$$n = p_1^3 + p_2^3 + p_3^3 + x^3 \tag{1.2}$$

where p_i *denote primes, and* x *is a* P_4*-number. The number* $E(N)$ *of all* $n \equiv 4 \bmod 18$ *not exceeding* N *which cannot be represented in the proposed manner, satisfies* $E(N) \ll_A N(\log N)^{-A}$ *for any* $A > 0$.

As usual, a number is called a P_r-number if it contains at most r prime factors, counted with multiplicity.

Our result is the closest approximation to date to the Waring-Goldbach problem for four cubes. It supersedes work of Roth [9] who showed that (1.2) has solutions for almost all n in primes p_i and integer x. As a simple corollary we also obtain a result on sums of 8 cubes. It is readily seen that there are at least $N(\log N)^{-8}$ natural numbers not exceeding N which are sums of four cubes of primes (*see* Roth [9], for example). By the Theorem and the pingeon hole principle it follows that all sufficiently large n are representable in the form $n = p_1^3 + \ldots + p_7^3 + x^3$ with primes p_i and a P_4-number x. Again this is an improvement on a similar result of Roth [9] in which x is an arbitrary integer.

Our method combines the circle method and the linear sieve as the two main tools. Because of the appearance of a sieve method we shall not be able to detect primes for all variables. On the other hand, the method offers considerable flexibility. As the proof will show, there is an underlying principle which indicates, very roughly speaking, that whenever the circle method supplies an asymptotic formula for the number of solutions of a diophantine equation, $F(x_1, \ldots, x_s) = 0$, say, possibly with restrictions on the x_i, then the methods of this paper can be used to solve the same equation in almost-primes of some fixed order. The Theorem may be regarded as an instance of this principle, applied to the work of Roth. We have chosen the four cubes problem as a first application of the method for two reasons: Sums of four cubes have received considerable attention, as one of the outstanding problems in additive number theory. Moreover, for the problem considered here the general principle is relatively easy to establish; both the circle method and the sieve machinery enter the proof only in their basic form. In two sequels to this paper, we shall explain how more sophisticated versions of the Hardy-Littlewood method and the sieve can enhance the power of the method.

2. An outline of the method

Before we proceed to describe our approach in some detail, we recall the principal results from linear sieve theory in a language convenient for our application. Let u be a non-negative integer-valued arithmetical function depending on a parameter P such that

$u(m) = 0$ for $m > 2P$ (e.g., u is a "sequence" in $\{1, 2, \dots, [2P]\}$, with multiplicities). For square-free integers d we require approximate formulae of the shape

$$\sum_{m \equiv 0 \bmod d} u(m) = \frac{\omega(d)}{d} X + R(d) \tag{2.1}$$

where $\omega(d)$ is a multiplicative function satisfying

$$0 \le \omega(p) < p; \qquad \omega(p) = 1 + O(p^{-1/2}) \tag{2.2}$$

for primes p, where X denotes a function of P which approximates the sum $\sum\limits_{m} u(m)$, and where $R(d)$ are suitable error terms. We now assume that there is a fixed integer K such that $u(m) = 0$ for $(m, K) > 1$ and $\omega(p) = 0$ for $p|K$. The errors $R(d)$ should be small on average, in the following sense. For some fixed $\theta > 0$ and certain complex numbers $\eta(d)$ with $|\eta(d)| \le 1$ we need that

$$\sum_{\substack{d \le P^\theta \\ (d,K)=1}} \mu(d)^2 \eta(d) R(d) \ll X (\log X)^{-2}. \tag{2.3}$$

Finally, a bound is required for $u(m)$ when m is divisible by a large square of a prime. We suppose that for any $\gamma > 0$ we have

$$\sum_{p > P^\gamma} \sum_{m \equiv 0 \bmod p^2} u(m) \ll X^{1-\delta} \tag{2.4}$$

for some $\delta = \delta(\gamma) > 0$. Then we have

PROPOSITION 1. – *Suppose that* (2.1), (2.2), (2.3) *and* (2.4) *hold with* $\theta^{-1} \le r - \frac{1}{8}$ *for some integer* $r \ge 2$. *Then there is a* P_r*-number* m *with* $u(m) > 0$.

This is only a special case of the results in Greaves [3,4] but any reasonable earlier version of the weighted linear sieve such as the Jurkat-Richert-theory (*see* [6], Chapter 9) would suit our needs as well. Note that Proposition 1 is a rather weak form of what is known in this context. The second condition in (2.2) is a very strong form of the "linear" sieve assumption, and the condition $\theta^{-1} \le r - \frac{1}{8}$ can be relaxed considerably for small r; *see* Greaves [3,4,5]. Our condition (2.4) is weaker than axiom $A4$ of Greaves [3] but it is clear that (2.4) can be used instead; it has been designed to allow for a simple verification in our context.

The first step in the proof of the Theorem is to construct a suitable function u. Let N be sufficiently large and put

$$P = \frac{2}{3} N^{1/3}; \quad Q = P^{5/6}. \tag{2.5}$$

For $N < n \le 2N$ let $\nu(n)$ denote the number of solutions of

$$n = x^3 + p_1^3 + p_2^3 + p_3^3 \tag{2.6}$$

subject to

$$P < x \le 2P; \qquad P < p_1 \le 2P; \qquad Q < p_2, p_3 \le 2Q. \tag{2.7}$$

For a given pair n, d we define $\nu_d(n)$ as the number of solutions to (2.6), (2.7) with $d|x$. Moreover, for a given n, we write $u(x) = u_n(x)$ for the number of solutions of (2.6), (2.7) with a prescribed value of x. It will turn out that for some appropriate choice of ω and X, the function u_n satisfies the requirements for Proposition 1 for any $\theta < \frac{1}{3}$, for almost all n, and this will finally prove the Theorem.

The formulae (2.1) and (2.4) are more easily expressed in terms of $\nu_d(n)$ by means of the obvious relations

$$\sum_{x \equiv 0 \bmod d} u_n(x) = \nu_d(n) \tag{2.8}$$

and

$$\sum_{p > P^\gamma} \sum_{x \equiv 0 \bmod p^2} u_n(x) = \sum_{p > P^\gamma} \nu_{p^2}(n). \tag{2.9}$$

A formal application of the Hardy-Littlewood method to the diophantine equation (2.6) and the identity (2.8) suggest a choice for the main term in (2.1). Indeed we are forced to choose

$$X = \mathfrak{S}(n) J(n) \tag{2.10}$$

where $\mathfrak{S}(n)$ is the formal singular series associated with the equation (2.6), and $J(n)$ is the corresponding singular integral, both to be defined below, in (3.6) and (3.10). All we need to know at the present stage is that for some $c > 0$, one has

$$(\log\log n)^{-c} (\log n)^{-3} n^{2/9} \ll X \ll (\log\log n)^{c} (\log n)^{-3} n^{2/9}. \tag{2.11}$$

This will be proved in §3. The appropriate $\omega(d)$ also is somewhat complicated to define without introducing further notation, and we postpone this to (3.12) below. Finally we observe that for any $n \equiv 4 \bmod 18$ and any solution of (2.6), (2.7) we must have $(6, x) = 1$. We shall therefore use Proposition 1 with $K = 6$. To avoid an unnecessarily complicated notation, we assume *from now on that* $n \equiv 4 \bmod 18$ *and that* d *denotes a square-free number coprime to* 6. We shall prove the following facts.

LEMMA 1. – *Let* $\theta < \frac{1}{3}$, $D = P^\theta$ *and* A *a positive real number. For any complex numbers* η_d *with* $|\eta_d| \le 1$ *we have*

$$\sum_{N < n \le 2N} \left| \sum_{d \le D} \eta_d \left(\nu_d(n) - \frac{\omega(d)}{d} X \right) \right|^2 \ll PQ^4 (\log P)^{-A}.$$

LEMMA 2. – *If* $\delta > 0$ *is sufficiently small, then*

$$\sum_{N < n \le 2N} |\sum_{p > P^\delta} \nu_{p^2}(n)|^2 \ll P^{1-2\delta} Q^4 \log P.$$

Now write $R(d) = \nu_d(n) - \dfrac{\omega(d)}{d}X$. By (2.8) this is in accordance with (2.1). Let $\mathcal{E}_1$ be the set of all $n \in [N, 2N]$ with

$$|\sum_{d\leq D} \eta(d)R(d)| > X(\log X)^{-2}.$$

By (2.5), (2.11) and Lemma 1,

$$\#\mathcal{E}_1 \ll X^{-2}(\log X)^4 \sum_{N<n\leq 2N} |\sum_{d\leq D} \eta(d)R(d)|^2 \ll N(\log N)^{11-A}.$$

Similarly we deduce from Lemma 2 that the set $\mathcal{E}_2$ of all $n \in [N, 2N]$ such that

$$\sum_{p>P^\delta} \nu_{p^2}(n) > X^{1-\frac{1}{3}\delta}$$

satisfies $\#\mathcal{E}_2 \ll N^{1-\delta}$. From (2.8) and (2.9) we see that for $n \in [N, 2N], n \notin \mathcal{E}_1 \cup \mathcal{E}_2$ the conditions (2.3) and (2.4) hold for any $\theta < \dfrac{1}{3}$. In particular, subject to proofs of (2.2) and Lemmata 1 and 2, the Theorem follows from Proposition 1.

We shall prove Lemmata 1 and 2 by two applications of the circle method. The idea of providing the main sieve input (2.3) via the circle method has also been used by Heath-Brown [7] in a different context. The proof of Lemma 1 is the main difficulty and is given in §§3-5. Lemma 2 is much easier. Indeed, by the definition of $\nu_{p^2}(n)$ we see that the left hand side in Lemma 2 is bounded by the number V of solutions to

$$p_1^6z_1^3 + x_1^3 + y_1^3 + y_2^3 = p_2^6z_2^3 + x_2^3 + y_3^3 + y_4^3$$

subject to

$$p_i > P^\delta; \quad P < p_i^2z_i \leq 2P; \quad P < x_i \leq 2P; \quad Q < y_i \leq 2Q.$$

Now we invoke a technical estimate.

LEMMA 3. – *Let $\mathcal{W}$ be a subset of $[P, 2P] \cap \mathbb{Z}$ with W elements. Let $S(\mathcal{W})$ denote the number of solutions of*

$$w_1^3 + x_1^3 + y_1^3 + y_2^3 = w_2^3 + x_2^3 + y_3^3 + y_4^3$$

subject to

$$w_i \in \mathcal{W}, \quad P < x_i \leq 2P, \quad Q < y_i \leq 2Q.$$

Then

$$S(\mathcal{W}) \ll P^{-1}W^2Q^4 \log P + P^{\frac{5}{2}+\epsilon}Q^2.$$

We take $\mathcal{W}$ as the set of all $P < w \leq 2P$ which have a representation in the form $p^2z = w$ with $p > P^\delta$. It is clear that w can have at most $(2\delta)^{-1}$ such representations, and that $\#\mathcal{W} \ll P^{1-\delta}$. Consequently,

$$V \leq (2\delta)^{-2}S(\mathcal{W}),$$

whence Lemma 2 follows from Lemma 3. A proof of Lemma 3 is given in §6.

3. Application of the Hardy-Littlewood method

In this and the next two sections we prove Lemma 1, and also (2.2) as a by-product. Our approach departs from a representation of $\nu_d(n)$ in terms of an integral. We write

$$f_d(\alpha) = \sum_{\substack{P<x\le 2P\\ x\equiv 0 \bmod d}} e(\alpha x^3); \quad g(\alpha) = \sum_{P<p\le 2P} e(\alpha p^3); \quad h(\alpha) = \sum_{Q<p\le 2Q} e(\alpha p^3)$$

and then define, for any measurable set $\mathfrak{B}$,

$$\nu_d(n, \mathfrak{B}) = \int_{\mathfrak{B}} f_d(\alpha) g(\alpha) h(\alpha)^2 e(-\alpha n) d\alpha. \tag{3.1}$$

Note that $\nu_d(n) = \nu_d(n, [0,1])$. Now define major and minor arcs as follows. Let B be a fixed real number with $B > 250$, $B > 9A$, and write

$$L = (\log P)^B. \tag{3.2}$$

Let $\mathfrak{M}(q,a)$ denote the interval $\left|\alpha - \frac{a}{q}\right| \le LP^{-3}$, and write $\mathfrak{M}$ for the union of all $\mathfrak{M}(q,a)$ with $1 \le a \le q \le L$, $(a,q) = 1$. The minor arcs $\mathfrak{m}$ are defined as the complement of $\mathfrak{M}$ in $[0,1] \bmod 1$. The main difficulty is to establish an appropriate minor arc estimate. This is contained in

LEMMA 4. – *For any $B > 250$ and any complex numbers η_d with $|\eta_d| \le 1$ one has*

$$\sum_{N<n\le 2N} |\sum_{d\le D} \eta_d \nu_d(n, \mathfrak{m})|^2 \ll PQ^4 (\log P)^{-B/9}.$$

We postpone the proof until §5. The major arcs are easier to handle. We write

$$S(q,a) = \sum_{x=1}^{q} e\left(\frac{ax^3}{q}\right); \quad S^*(q,a) = \sum_{\substack{x=1\\ (x,q)=1}}^{q} e\left(\frac{ax^3}{q}\right); \tag{3.3}$$

and

$$v(\beta) = \int_P^{2P} e(\beta t^3) dt; \quad w(\beta, \Xi) = \frac{1}{3}\int_{\Xi}^{2\Xi} \frac{e(\beta t^3)}{\log t} dt.$$

Then for $\alpha = \frac{a}{q} + \beta \in \mathfrak{M}(q,a)$ we define

$$f_d^*(\alpha) = \frac{S(q, ad^3)}{qd} v(\beta), \quad g^*(\alpha) = \frac{S^*(q,a)}{\varphi(q)} w(\beta, P), \quad h^*(\alpha) = \frac{S^*(q,a)}{\varphi(q)} w(\beta, Q).$$

Since the $\mathfrak{M}(q,a)$ are pairwise disjoint, this defines functions f_d^*, h^*, g^* on $\mathfrak{M}$. Uniformly for $\alpha \in \mathfrak{M}$ we have

$$|f_d g h^2 - f_d^* g^* h^{*2}| \ll d^{-1} P^2 Q^2 (\log P)^{-5B}.$$

This follows immediately from standard results such as Theorem 4.1 of Vaughan [10] and the corresponding analogue for prime number sums in Hua [8]. On writing

$$\nu_d^*(n) = \int_{\mathfrak{M}} f_d^*(\alpha) g^*(\alpha) h^*(\alpha)^2 e(-\alpha n) d\alpha$$

and integrating the previous inequality we deduce that

$$\sum_{d \leq D} |\nu_d(n, \mathfrak{M}) - \nu^*(n)| \ll P^{-1} Q^2 (\log P)^{-2B} \log D \tag{3.4}$$

since the measure of $\mathfrak{M}$ is $O(L^3 P^{-3})$.

Next we evaluate $\nu_d^*(n)$. To this end we introduce some further notation. Let

$$T_d(q,n) = \sum_{\substack{a=1 \\ (a,q)=1}}^{q} \frac{S(q, ad^3) S^*(q,a)^3}{q\varphi(q)^3} e\Big(-\frac{an}{q}\Big), \tag{3.5}$$

$$J(n) = \int_{-LP^{-3}}^{LP^{-3}} v(\beta) w(\beta, P) w(\beta, Q)^2 e(-\beta n)\, d\beta. \tag{3.6}$$

Then

$$\nu_d^*(n) = d^{-1} \sum_{q \leq L} T_d(q,n) J(n). \tag{3.7}$$

Routine endgame techniques in the Hardy-Littlewood method readily yield the bounds

$$n^{2/9} (\log n)^{-3} \ll J(n) \ll n^{2/9} (\log n)^{-3} \tag{3.8}$$

for $N < n \leq 2N$; we may omit the details. In the next section we shall prove that

$$T_d(q,n) \ll q^{\epsilon - 2} (q,n)(q,d)^{1/2}. \tag{3.9}$$

Hence the singular series

$$\mathfrak{S}_d(n) = \sum_{q=1}^{\infty} T_d(q,n) \tag{3.10}$$

converges absolutely. For simplicity we write $\mathfrak{S}_1(n) = \mathfrak{S}(n)$. Note that $\mathfrak{S}(n)$ is exactly the singular series discussed in Roth [9] so we may quote his bounds $\mathfrak{S}(n) > 0$ for all n, and

$$(\log\log n)^{-c} < \mathfrak{S}(n) < (\log\log n)^{c} \tag{3.11}$$

for some fixed $c > 0$ and sufficiently large n. By (3.8) and (3.11) we now deduce the inequalities (2.11). Moreover we can now define the function $\omega(d)$ for square-free d by

$$\omega(d) = \frac{\mathfrak{S}_d(n)}{\mathfrak{S}(n)}. \tag{3.12}$$

A detailed analysis of $\omega(d)$ is given in §4. By (2.10), (3.7), (3.9), (3.10) and (3.12), we have

$$\sum_{d\le D}\left|\nu_d^*(n)-\frac{\omega(d)}{d}X\right| \ll J(n)\sum_{d\le D}\sum_{q>L}\frac{(q,n)(q,d)^{1/2}}{q^{2-\epsilon}d}$$
$$\ll J(n)(\log D)L^{-\frac{1}{2}}\sum_{q=1}^{\infty}\frac{(q,n)}{q^{5/4}} \ll J(n)d(n)L^{-\frac{1}{2}}\log D;$$

here $d(n)$ denotes the number of divisors of n. We take squares and sum over $N<n\le 2N$, and apply the same procedure to (3.4). Then, by (3.8),

$$\sum_{N<n\le 2N}\left(\sum_{d\le D}\left|\nu_d(n,\mathfrak{M})-\frac{\omega(d)}{d}X\right|\right)^2 \ll PQ^4L^{-1}. \tag{3.13}$$

Since $\nu_d(n)=\nu_d(n,\mathfrak{m})+\nu_d(n,\mathfrak{M})$, Lemma 1 now follows from Lemma 4 and (3.13).

4. The singular series

We begin this section with a proof of (3.9). By standard methods it is readily shown that $T_d(q,n)$ is a multiplicative function of q (*see* chapters 2 and 4 of Vaughan [10], for example), so that it actually suffices to show that

$$T_d(p^t,n) \ll p^{-2t}(p^t,n)(p^t,d)^{1/2} \tag{4.1}$$

for all primes p and all $t\in\mathbb{N}$.

By a result of Hua [8] we have $S^*(p^t,a)=0$ whenever $p\nmid a$, and $t\ge t_0(p)$ where $t_0(p)=2$ for $p\ne 3$, and $t_0(3)=3$. From (3.9) we infer

$$T_d(p^t,n)=0 \quad \text{if} \quad t\ge t_0(p), \tag{4.2}$$

so that it now suffices to verify (4.1) when $p\ne 3, t=1$.

First suppose that $p\nmid d$. Then $S(p,ad^3)=S(p,a)$ by (3.3), whence $T_d(p,n)=T_1(p,n)$ by (3.9). Moreover, by (3.3), $S^*(p,a)=S(p,a)-1$. By (3.9),

$$T_1(p,n)=p^{-1}(p-1)^{-3}(G_4(p,n)-3G_3(p,n)+3G_2(p,n)-G_1(p,n))$$

where

$$G_s(p,n)=\sum_{a=1}^{p-1}S(p,a)^s e\left(-\frac{an}{p}\right).$$

By Lemma 4.7 of Vaughan [10] we have

$$G_s(p,n) \ll p^{s/2}(p,n) \tag{4.3}$$

for any $s\ge 1$. We deduce that $T_1(p,n)\ll p^{-2}(p,n)$ as required.

Now suppose that $p|d$. Then $S(p, ad^3) = p$ so that

$$\begin{aligned} T_d(p,n) = T_p(p,n) &= (p-1)^{-3} \sum_{a=1}^{p-1} S^*(p,a)^3 e\Big(-\frac{an}{p}\Big) \\ &= (p-1)^{-3}(G_3(p,n) - 3G_2(p,n) + 3G_1(p,n) - G_0(p,n)). \quad (4.4) \end{aligned}$$

But $G_0(p,n)$ is Ramanujan's sum whence (4.3) also holds for $s = 0$. Now we find that $T_d(p,n) \ll p^{-3/2}(p,n) = p^{-2}(p,d)^{1/2}(p,n)$. This gives (4.1).

Next we investigate the function $\omega(d)$. Since $T_d(q,n)$ is multiplicative in q we can write the series (3.10) as a product. By (4.3) we find that

$$\mathfrak{S}_d(n) = C_3(n) \prod_{\substack{p \neq 3 \\ p \nmid d}} \Big(1 + T_1(p,n)\Big) \prod_{p|d} \Big(1 + T_p(p,n)\Big) \tag{4.5}$$

where $C_3(n) = 1 + T_1(3,n) + T_1(9,n)$ (in verifying this recall that $(d,6) = 1$).

Now, for a short digression. We deduce the results on $\mathfrak{S}(n)$ quoted from Roth [9] in §3 because the underlying idea will also be needed in the sequel. Note that $\varphi(9)^3 C_3(n)$ equals the number of solutions of the congruence

$$x^3 + y_1^3 + y_2^3 + y_3^3 \equiv n \bmod 9$$

with $1 \leq x \leq 9, 1 \leq y_i \leq 9, 3 \nmid y_i$. In particular, $C_3(n) > 0$. Similarly $(p-1)^3(1+T_1(p,n))$ equals the number of solutions $H(p,n)$ of the congruence

$$x^3 + y_1^3 + y_2^3 + y_3^3 \equiv n \bmod p$$

with $1 \leq x \leq p$, $1 \leq y_i \leq p-1$. At this point it is useful to have at hand the following easy result.

LEMMA 5. – *Let $K(p,n)$ denote the number of solutions of the congruence $y_1^3 + y_2^3 + y_3^3 \equiv n \bmod p$ with $1 \leq y_i \leq p-1$. If $p \neq 2, 7$ or 13 then $K(p,n) > 0$ for all n. Moreover, for large p,*

$$K(p,n) = p^2 + O(p^{3/2}).$$

For the exceptional primes p not covered by Lemma 5 a direct verification shows that the only cases where $K(p,n) = 0$ are $K(2,0)$, $K(7,0)$, $K(7,5)$, $K(7,2)$ and $K(13,0)$. We easily deduce that $H(p,n) > 0$ for all p and all n. Now $\mathfrak{S}(n) > 0$ and (3.11) follow from (4.5) and (4.1).

From (4.5) and (3.12) we also deduce that $\omega(d)$ is multiplicative, and that

$$\omega(p) = \frac{1 + T_p(p,n)}{1 + T_1(p,n)}.$$

By the first half of (4.4), $p(p-1)^{-3}K(p,n) = 1 + T_p(p,n)$. Hence

$$\omega(p) = p\frac{K(p,n)}{H(p,n)} \tag{4.6}$$

However, directly from the definition,

$$H(p,n) = \sum_{x=1}^{p} K(p, n - x^3) = K(p,n) + \sum_{x=1}^{p-1} K(p, n - x^3). \tag{4.7}$$

From Lemma 5 we see that $H(p,n) > K(p,n)$ for $p \geq 5, p \neq 7, 13, 19$; and for $p = 7, 13$ or 19 this is also true, as a short calculation shows. This gives $0 \leq \omega(p) < p$. For large p, we have $H(p,n) = p^3 + O(p^{5/2})$ from (4.7) and Lemma 5. From (4.6) and Lemma 5 we now deduce $\omega(p) = 1 + O(p^{-1/2})$. This establishes (2.2).

It remains to prove Lemma 5. If $p \equiv 2 \bmod 3$ or $p = 3$ the mapping $x \to x^3$ is a bijection of the set of reduced residues modulo p. Hence $K(p,n)$ counts the solutions of $z_1 + z_2 + z_3 \equiv n \bmod p$ in reduced residues z_i. So in these cases the Lemma is trivial.

We may therefore suppose that $p \equiv 1 \bmod 3$. By the orthogonality of additive characters,

$$pK(p,n) = \sum_{a=1}^{p} S^*(p,a)^3 e\left(-\frac{an}{p}\right) = (p-1)^3 + E$$

where

$$E = \sum_{a=1}^{p-1} S^*(p,a)^3 e\left(-\frac{an}{p}\right).$$

By Lemma 4.3 of Vaughan [10] one has $|S^*(p,a)| \leq 2\sqrt{p} + 1$ whenever $p \nmid a$. Moreover,

$$\sum_{a=1}^{p-1} |S^*(p,a)|^2 = \sum_{a=1}^{p} |S^*(p,a)|^2 - (p-1)^2, \tag{4.8}$$

and the sum on the right equals p times the number of solutions of $x^3 \equiv y^3 \bmod p$ with $1 \leq x, y \leq p-1$. Since $p \equiv 1 \bmod 3$ there are exactly $3(p-1)$ such solutions x, y. It follows that the expression in (4.8) equals $(p-1)(2p+1)$, and therefore,

$$|E| \leq (2\sqrt{p} + 1)(p-1)(2p+1).$$

We deduce that $E \ll p^{5/2}$ and $|E| < (p-1)^3$ for $p > 30$. The case $p = 19$ can be checked by hand. This establishes the Lemma.

5. The minor arc estimate

In this section we prove Lemma 4. In fact we shall prove the following technical result which will also be useful in a later paper in this series.

PROPOSITION 2. – *Let η_d be any complex numbers satisfying $|\eta_d| \le 1$. In the notation of* §3, *let*

$$F(\alpha) = \sum_{d \le D} \eta_d f_d(\alpha) \tag{5.1}$$

where D is supposed to satisfy the conditions of Lemma 1. *Then, for $B > 250$, one has*

$$\int_{\mathfrak{m}} |F(\alpha)g(\alpha)h(\alpha)^2|^2 d\alpha \ll PQ^4(\log P)^{-B/9}.$$

This implies Lemma 4. To see this note that by (3.1)

$$\sum_{d \le D} \eta_d \nu_d(n, \mathfrak{m}) = \int_{\mathfrak{m}} F(\alpha)g(\alpha)h(\alpha)^2 e(-\alpha n) d\alpha$$

whence the number on the left is the n-th Fourier coefficient of the function of period 1 which is $F(\alpha)g(\alpha)h(\alpha)^2$ on $\mathfrak{m}$, and 0 elsewhere $(\bmod 1)$. By Bessel's inequality,

$$\sum_{N < n \le 2N} |\sum_{d \le D} \eta_d \nu_d(n, \mathfrak{m})|^2 \le \int_{\mathfrak{m}} |Fgh^2|^2 d\alpha$$

so that indeed Lemma 4 follows from Proposition 2. As a first step towards Proposition 2 we examine the exponential sum $F(\alpha)$.

LEMMA 6. – *Let $F(\alpha)$ be the exponential sum defined in* (5.1). *Suppose that $\left|\alpha - \frac{a}{q}\right| \le q^{-1}P^{-3/2}$ where $(a, q) = 1$ and $q \le P^{3/2}$. Then*

$$F(\alpha) \ll P^{\frac{3}{4}+\epsilon} D^{\frac{1}{4}} + q^{\epsilon - \frac{1}{3}} P(\log P) \left(1 + P^3 \left|\alpha - \frac{a}{q}\right|\right)^{-1/3}$$

Proof. – We rewrite $F(\alpha)$ as

$$F(\alpha) = \sum_{d \le D} \eta_d \sum_{P/d < y \le 2P/d} e(\alpha d^3 y^3).$$

By Dirichlet's theorem on diophantine approximation, there are coprime integers $b = b(d), r = r(d)$ with $r \le 8P^2 d^{-2}$, $\left|d^3\alpha - \frac{b}{r}\right| \le \frac{1}{8} r^{-1} d^2 P^{-2}$. By Weyl's inequality, the sum over y is $O(P^{3/4+\epsilon} d^{-3/4})$ unless $r \le P/d$ in which case it is

$$\ll r^{-\frac{1}{3}} \frac{P}{d} \left(1 + \left(\frac{P}{d}\right)^3 \left|\alpha d^3 - \frac{b}{r}\right|\right)^{-\frac{1}{3}} + \left(\frac{P}{d}\right)^{\frac{1}{2}+\epsilon},$$

this bound being a consequence of Theorems 4.1 and 2.8 of Vaughan [10]. Again, the sum over y is $O(P^{3/4} d^{-3/4})$ unless one has

$$r \le (P/d)^{3/4}; \quad \left|\alpha d^3 - \frac{b}{r}\right| \le \frac{1}{r}\left(\frac{d}{P}\right)^{\frac{9}{4}}. \tag{5.2}$$

On summing over d it follows that

$$F(\alpha) \ll P^{3/4+\epsilon}D^{1/4} + P\sum_{d\in\mathcal{D}} d^{-1}r^{-\frac{1}{3}}\left(1+\left(\frac{P}{d}\right)^3\left|\alpha d^3-\frac{b}{r}\right|\right)^{-\frac{1}{3}}$$

where $\mathcal{D}$ is the set of all $d \leq D$ for which (5.2) holds. For any $d \in \mathcal{D}$ we compare (5.2) with the approximation to α postulated in the Lemma. This yields

$$\left|\frac{b}{r}-\frac{ad^3}{q}\right| \leq \frac{1}{r}\left(\frac{d}{P}\right)^{9/4} + \frac{d^3}{qP^{3/2}}$$

so that

$$|bq-ad^3r| \leq qd^{9/4}P^{-9/4} + rP^{-3/2}d^3 \leq 2D^{9/4}P^{-3/4} < 1$$

if P is sufficiently large $\left(\text{recall that } D = P^\theta \text{ with } \theta < \frac{1}{3}\right)$. It follows that $\frac{ad^3}{q} = \frac{b}{r}$ whence $r = q/(q,d^3)$. Using the trivial bound $(q,d^3) \leq (q,d)^3$ we deduce that

$$\sum_{d\in\mathcal{D}} d^{-1}r^{-\frac{1}{3}}\left(1+\left(\frac{P}{d}\right)^3\left|\alpha d^3-\frac{b}{r}\right|\right)^{-\frac{1}{3}} \leq q^{-\frac{1}{3}}\left(1+P^3\left|\alpha-\frac{a}{q}\right|\right)^{-\frac{1}{3}}\sum_{d\leq D}\frac{(q,d)}{d},$$

and the Lemma follows immediately.

We also need the following result of Vaughan [12].

LEMMA 7. – *Let T denote the number of solutions of $x_1^3+y_1^3+y_2^3 = x_2^3+y_3^3+y_4^3$ subject to $P < x_i \leq 2P, Q \leq y_i \leq 2Q$ where P, Q satisfy* (2.5). *Then*

$$T \ll P^{1+\epsilon}Q^2.$$

For future reference, we note that by considering the underlying diophantine equation we have

$$\int_0^1 |g(\alpha)h(\alpha)^2|^2 d\alpha \leq T. \tag{5.3}$$

Let $\delta > 0$ be so small that $D^{1/4}P^{3/4} \leq P^{\frac{5}{6}-2\delta}$; by the upper bound imposed on D this is always possible. Let $\mathfrak{N}(q,a)$ denote the interval $|q\alpha - a| \leq P^{4\delta-\frac{5}{2}}$, and let $\mathfrak{N}$ be the union of all $\mathfrak{N}(q,a)$ with $1 \leq a \leq q \leq P^{\frac{1}{2}+4\delta}$, $(a,q) = 1$. By a standard argument, Lemma 5 shows that $|F(\alpha)| > P^{\frac{5}{6}-\delta}$ implies $\alpha \in \mathfrak{N}$ (modulo 1). Now, defining a function Φ on $\mathfrak{N}$ by

$$\Phi(\alpha) = q^{\epsilon-\frac{1}{3}}\left(1+P^3\left|\alpha-\frac{a}{q}\right|\right)^{-1/3}$$

if $\alpha \in \mathfrak{N}(q,a)$, it follows from another application of Lemma 6 that

$$\int_{\mathfrak{m}} |Fgh^2|^2 d\alpha \ll P^{\frac{5}{3}-2\delta}\int_0^1 |gh^2|^2 d\alpha + P^2(\log P)^2\int_{\mathfrak{N}\cap\mathfrak{m}} |\Phi gh^2|^2 d\alpha. \tag{5.4}$$

By Hölder's inequality,

$$\int_{\mathfrak{N}\cap\mathfrak{m}} |\Phi g h^2|^2 d\alpha \le \left(\int_{\mathfrak{N}\cap\mathfrak{m}} |\Phi|^8 d\alpha\right)^{\frac{1}{4}} U_1^{\frac{1}{4}} U_2^{\frac{1}{2}} \tag{5.5}$$

where

$$U_1 = \int_0^1 |g(\alpha)h(\alpha)|^4 d\alpha; \quad U_2 = \int_0^1 |g(\alpha)h(\alpha)^3|^2 d\alpha. \tag{5.6}$$

For the first factor on the right of (5.5) it is straightforward to show that

$$\int_{\mathfrak{N}\cap\mathfrak{m}} |\Phi(\alpha)|^8 d\alpha \ll P^{-3} L^{-1/2}. \tag{5.7}$$

Moreover, by Lemma 3 and on considering the underlying diophantine equation, we have

$$U_1 \le S([P, 2P] \cap \mathbb{Z}) \ll PQ^4 \log P. \tag{5.8}$$

As we shall see in the next section, we also have

$$U_2 \ll P^{-1} Q^6. \tag{5.9}$$

From (5.4), (5.3), Lemma 7, (5.5), (5.7), (5.8) and (5.9) we deduce

$$\int_{\mathfrak{m}} |F\, g\, h^2|^2 d\alpha \ll PQ^4 (\log P)^{3-\frac{B}{8}}$$

which gives the Lemma.

6. Some technical proofs

It remains to establish Lemma 3 and (5.9) which both follow from another though primitive application of the Hardy-Littlewood method. We begin by introducing the Weyl sums

$$G(\alpha) = \sum_{P<x\le 2P} e(\alpha x^3); \quad H(\alpha) = \sum_{Q<y\le 2Q} e(\alpha y^3); \quad W(\alpha) = \sum_{w\in\mathcal{W}} e(\alpha w^3).$$

Then, in the notation of Lemma 3,

$$S(\mathcal{W}) = \int_0^1 |G(\alpha)W(\alpha)H(\alpha)^2|^2 d\alpha. \tag{6.1}$$

Let $\mathfrak{K}(q,a)$ denote the interval $|q\alpha - a| \le P^{-9/4}$, and let $\mathfrak{K}$ denote the union of all $\mathfrak{K}(q,a)$ with $1 \le a \le q \le P^{3/4}, (a,q) = 1$. By Dirichlet's theorem, there are coprime numbers

b, r such that $r \leq P^{3/2}$; $\left|\alpha - \frac{b}{r}\right| \leq r^{-1}P^{-3/2}$. Theorem 2 of Vaughan [11] and Lemma 6.3 of Vaughan [10] now imply

$$G(\alpha) \ll r^{-\frac{1}{3}}P\left(1 + P^3\left|\alpha - \frac{b}{r}\right|\right)^{-1} + P^{3/4+\epsilon}.$$

In particular, $|G(\alpha)| > P^{3/4+2\epsilon}$ implies $\alpha \in \mathfrak{K}\,(\mathrm{mod}\,1)$, and from (6.1) we see that

$$S(\mathcal{W}) \ll P^{\frac{3}{2}+\epsilon}\int_0^1 |W(\alpha)H(\alpha)^2|^2 d\alpha + P^2\int_{\mathfrak{K}} |\Psi(\alpha)W(\alpha)H(\alpha)^2|^2 d\alpha \tag{6.2}$$

when $\Psi(\alpha)$ is defined on $\mathfrak{K}$ by

$$\Psi(\alpha) = q^{-\frac{1}{3}}\left(1 + P^3\left|\alpha - \frac{a}{q}\right|\right)^{-1}$$

when $\alpha \in \mathfrak{K}(q, a)$. Now $|W(\alpha)| \leq W(0) = W$, and by Theorem 4.1 and Lemma 6.3 of Vaughan [10], one has

$$H(\alpha) \ll q^{-1/3}Q + Q^{1/2} \ll q^{-1/3}Q \tag{6.3}$$

when $\alpha \in \mathfrak{K}(q, a)$. It follows that

$$\int_{\mathfrak{K}} |\Psi(\alpha)W(\alpha)H(\alpha)^2|^2 d\alpha \ll W^2Q^4 \sum_{q \leq P^{3/4}} \sum_{\substack{a=1 \\ (a,q)=1}}^{q} q^{-2}\int_{\mathfrak{K}(q,a)} \left(1 + P^3\left|\alpha - \frac{a}{q}\right|\right)^{-2} d\alpha$$
$$\ll W^2Q^4P^{-3}\log P.$$

On considering the underlying diophantine equation, we see that

$$\int_0^1 |W(\alpha)H(\alpha)^2|^2 d\alpha \leq T$$

where T is the number estimated in Lemma 7. Collecting together, we now find that

$$S(\mathcal{W}) \ll P^{\frac{5}{2}+\epsilon}Q^2 + P^{-1}W^2Q^4\log P$$

as required.

A proof of (5.9) can be given along the same lines. By considering the underlying diophantine equations we obtain the basic inequality

$$\int_0^1 |g(\alpha)|^2|h(\alpha)|^6 d\alpha \leq \int_0^1 |G(\alpha)|^2|H(\alpha)|^6 d\alpha. \tag{6.4}$$

Let $\mathfrak{L}(q, a)$ denote the interval $|q\alpha - a| \leq Q^{-9/4}$, and let $\mathfrak{L}$ denote the union of all $\mathfrak{L}(q, a)$ with $1 \leq a \leq q \leq Q^{3/4}$, $(a, q) = 1$. On $\mathfrak{L}$ we define a function Ψ^* by

$\Psi^*(\alpha) = q^{-1/3}Q\left(1 + Q^3\left|\alpha - \frac{a}{q}\right|\right)^{-1}$ for $\alpha \in \mathfrak{L}(q,a)$. By the argument leading to (6.2), but with G replaced by H, we find that

$$\int_0^1 |G(\alpha)|^2|H(\alpha)|^6 d\alpha$$
$$\leq Q^{\frac{3}{2}+\epsilon}\int_0^1 |G(\alpha)H(\alpha)^2|^2 d\alpha + Q^2\int_{\mathfrak{L}} |\Psi^*(\alpha)G(\alpha)H(\alpha)^2|^2 d\alpha. \tag{6.5}$$

The first integral on the right equals T. Hence, by Lemma 7, the first term on the right is $O(Q^{3/2+\epsilon}P^{1+\epsilon}Q^2) = O(P^{-1}Q^6)$ which is acceptable. The treatment of the integral over $\mathfrak{L}$ requires more care. When $\alpha \in \mathfrak{L}(q,a)$, we invoke Theorem 2 of Vaughan [11] and Lemma 6.3 of Vaughan [10] to see that

$$G(\alpha) \ll P\Psi(\alpha) + q^\epsilon(q + P^3|q\alpha - a|)^{\frac{1}{2}}$$

where Ψ is the same function as in the previous argument (now defined on $\mathfrak{L}$). A short calculation shows that the second term on the right is $O(P^{9/16+\epsilon})$, uniformly for $\alpha \in \mathfrak{L}$. Hence

$$\int_{\mathfrak{L}} |\Psi(\alpha)G(\alpha)H(\alpha)^2|^2 d\alpha \ll P^2 I_1 + P^{9/8+2\epsilon} I_2$$

where

$$I_1 = \int_{\mathfrak{L}} |\Psi(\alpha)\Psi^*(\alpha)H(\alpha)^2|^2 d\alpha; \quad I_2 = \int_{\mathfrak{L}} |\Psi^*(\alpha)H(\alpha)^2|^2 d\alpha.$$

It is clear that (6.3) remains valid for $\alpha \in \mathfrak{L}(q,a)$. Straightforward estimates now show that

$$I_1 \ll Q^4 \sum_{q \leq Q^{3/4}} q^{-\frac{8}{3}} \sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{L}(q,a)} \left(1 + P^3\left|\alpha - \frac{a}{q}\right|\right)^{-2} d\alpha \ll P^{-3}Q^4$$

and

$$I_2 \ll Q^4 \sum_{q \leq Q^{3/4}} q^{-2} \sum_{\substack{a=1\\(a,q)=1}}^{q} \int_{\mathfrak{L}(q,a)} \left(1 + Q^3\left|\alpha - \frac{a}{q}\right|\right)^{-2} d\alpha \ll Q \log Q.$$

By (6.5), it is now readily confirmed that the right hand side of (6.4) is $O(P^{-1}Q^6)$. By (5.6), this establishes (5.9). The proof of our Theorem is now complete.

REFERENCES

[1] J. Brüdern, *Sieves, the circle method, and Waring's problem for cubes* (*Habilitationsschrift, Göttingen 1991 = Mathematica Gottingensis* 51, 1991).

[2] H. Davenport, *On Waring's Problem for cubes* (*Acta Math.*, Vol. 71, 1939, pp. 123-143).

[3] G. Greaves, *A weighted sieve of Brun's type* (*Acta Arith.*, Vol. 40, 1981, pp. 297-332).

[4] G. Greaves, *Rosser's sieve with weights. Recent progress in analytic number theory,* vol. I; H. Halberstam, C. Hooley edts. Academic Press, London, 1981, pp. 61-68.

[5] G. Greaves, *The weighted linear sieve and Selberg's λ^2-method* (*Acta Arith.*, Vol. 47, 1986, pp. 71-96).

[6] H. Halberstam and H. E. Richert, *Sieve methods*, Academic Press, London, 1974.

[7] D. R. Heath-Brown, *Three primes and an almost-prime in arithmetic progression* (*J. London Math. Soc.*, (2) Vol. 23, 1981, pp. 396-414).

[8] L. K. Hua, *Some results in additive prime number theory* (*Quart. J. Math. Oxford*, Vol. 9, 1938, pp. 68-80).

[9] F. K. Roth, *On Waring's problem for cubes* (*Proc. London Math. Soc.*, (2) Vol. 53, 1951, pp. 268-279).

[10] R. C. Vaughan, *The Hardy-Littlewood method,* University Press, Cambridge, 1981.

[11] R. C. Vaughan, *Some remarks on Weyl sums* (*Topics in classical number theory, Colloq. Math. Soc. J. Bolyai*, North Holland, Amsterdam, Vol. 34, 1984, pp. 1585-1602).

[12] R. C. Vaughan, *Sums of three cubes* (*Bull. London Math. Soc.*, Vol. 17, 1985, pp. 17-20).

[13] I. M. Vinogradov, *Selected works*, Springer, Berlin 1985.

(Manuscript received October 7, 1993;
revised March 4, 1994.)

Jörg Brüdern
Mathematisches Institut
Bunsenstrasse 3-5
D-37073 Göttingen