PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A
MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

The Use in Additive Number Theory of Numbers without Large Prime Factors

R. C. Vaughan

Phil. Trans. R. Soc. Lond. A 1993 **345**, 363-376
doi: 10.1098/rsta.1993.0135

The use in additive number theory of numbers without large prime factors

By R. C. Vaughan

Department of Mathematics, Huxley Building, 180 Queen's Gate, Imperial College of Science, Technology and Medicine, London SW7 2BZ, U.K.

In the past few years considerable progress has been made with regard to the known upper bounds for $G(k)$ in Waring's problem, that is, the smallest s such that every sufficiently large natural number is the sum of at most s kth powers of natural numbers. This has come about through the development of techniques using properties of numbers having only relatively small prime factors. In this article an account of these developments is given, and they are illustrated initially in a historical perspective through the special case of cubes. In particular the connection with the classical work of Davenport on smaller values of k is demonstrated. It is apparent that the fundamental ideas and the underlying mean value theorems and estimates for exponential sums have numerous applications and a brief account is given of some of them.

1. Introduction

One of the questions of central interest in additive number theory is that of constructing in an efficient manner sets of numbers each element of which is the sum of s kth powers of natural numbers. A closely related question is that of obtaining bounds for the number N of solutions of the equation

$$x_1^k+\ldots+x_s^k = y_1^k+\ldots+y_s^k, \quad \text{with} \quad x_i, y_i \in \mathscr{A}_i, \quad \mathscr{A}_i \subset \mathbb{N} \cap [1,P]. \tag{1.1}$$

The ideal bound, usually unobtainable in the current state of knowledge except in special cases, is

$$N \ll (\text{card}\,\mathscr{A}_1 \ldots \text{card}\,\mathscr{A}_s + (\text{card}\,\mathscr{A}_1 \ldots \text{card}\,\mathscr{A}_s)^2 P^{-k}) P^{\epsilon}.$$

In one of their seminal papers on 'Some problems of "partitio numerorum"' concerned with Waring's problem Hardy & Littlewood (1925) make explicit use of the familiar observation that when $k > 1$ the kth powers are 'well spaced'. Thereby they are able to construct quite large subsets of $\mathbb{Z} \cap [1, X]$ each element of which is the sum of s kth powers. In the simplest possible form of this construction they take $P = (X/s)^{1/k}$, $\psi = 1-1/k$, $P_j = 2^{-(j-1)(k-1)} P^{\psi^{j-1}}$ and consider those numbers of the form $x_1^k+\ldots+x_s^k$ with the x_j lying in the 'diminishing ranges'

$$\mathscr{A}_j = \{x_j : \tfrac{1}{2}P_j < x_j \leqslant P_j\}. \tag{1.2}$$

When X is large no number can be represented more than once in this way, for otherwise we would have (1.1) with the $y_i \in \mathscr{A}_i$ and $x_i \neq y_i$ for some i. Then, if l is the smallest such i, we have $|x_l^k - y_l^k| \geqslant k(P_l/2)^{k-1}$ whereas $|x_{l+1}^k+\ldots+x_s^k-y_{l+1}^k-\ldots-y_s^k| \leqslant P_{l+1}^k + O(P_{l+2}^k) < k(P_l/2)^{k-1}$, which is absurd. Thus there are $\gg X^{\lambda}$, with $\lambda =$

$1-(1-1/k)^s$, numbers of the form $x_1^k+\ldots+x_s^k$ not exceeding X. There are a series of important refinements to the diminishing ranges construction, due principally to Davenport (1938, 1939*a–c*, 1942*a*, *b*, 1950) and Davenport & Erdös (1939) (see Davenport (1977) and ch. 5 and 6 of Vaughan (1981)), and it also plays a major role in much of Vinogradov's work (1984) on Waring's problem. More generally, suppose that $(X/s)^{1/k} \geqslant P_1 \geqslant P_2 \geqslant \ldots \geqslant P_s$ and define $R(n)$ to be the number of representations of n in the form $x_1^k+\ldots+x_s^k$ with

$$\tfrac{1}{2}P_j < x_j \leqslant P_j. \tag{1.3}$$

If one can show that

$$\sum_n R(n)^2 \ll P_1 P_2 \ldots P_s X^{\epsilon}, \tag{1.4}$$

then it follows by a simple application of Cauchy's inequality that

$$\sum_{n,\, R(n)\neq 0} 1 \gg P_1 P_2 \ldots P_s X^{-\epsilon}.$$

Thus the set $\mathscr{B}_{k,s}$ of sums of s kth powers in $[1,X] \cap \mathbb{Z}$ satisfies

$$\operatorname{card} \mathscr{B}_{k,s} \gg P_1 P_2 \ldots P_s X^{-\epsilon}. \tag{1.5}$$

For example, if one takes

$$P = (X/s)^{1/k}, \quad \psi = 1-1/k, \quad P_j = P^{\psi^{j-1}} (j = 1,\ldots,s-1), \quad P_s = P_{s-1}, \tag{1.6}$$

then one can establish (1.4) as follows. The left-hand side is the number of solutions of (1.1) with (1.3) and (1.6) holding for each x_j and for each x_j replaced by y_j. Given any such set of x_j it is easily seen by a simple refinement of the argument above that there are at most $O(1)$ choices for y_1. Then, given any set of x_j and any y_1 and provided $s-1>2$ there are at most $O(1)$ choices for y_2. By repeating this argument we see that given a set of x_j there are at most $O(1)$ choices for $y_1,\ldots,y_{s-2}$. Finally, given any set of x_j and any $y_1,\ldots,y_{s-2}$, the equation (1.3) reduces to $y_{s-1}^k+y_s^k = u$ for some integer u with $u \ll X$ and so the number of choices for y_{s-1}, y_s is $O(X^{\epsilon})$. This establishes (1.4) and so, by (1.5), we have

$$\operatorname{card} \mathscr{B}_{k,s} \gg X^{\lambda-\epsilon}, \quad \lambda = 1-(1-2/k)\,((1-1/k)^{s-2}) \quad (X > X_0(\epsilon,k,s)). \tag{1.7}$$

2. Three cubes: an illustrative example

When $k=3$ and $s=3$ (1.7) shows that

$$\operatorname{card} \mathscr{B}_{3,3} \gg X^{\frac{7}{9}-\epsilon} \quad (X > X_0(\epsilon)). \tag{2.1}$$

Now, as in Davenport (1939*a*), we suppose that

$$P = P_1 = (\tfrac{1}{3}X)^{\frac{1}{3}}, \quad Q = P_2 = P_3 = P^{\psi} \tag{2.2}$$

and for the time being leave ψ at our disposal subject only to the condition $\frac{2}{3} \leqslant \psi \leqslant 1$. Our aim is to establish (1.4) with a larger value of ψ than $\frac{2}{3}$.

We define $R(n)$ as above and once more interpret $\Sigma_n R(n)^2$ as the number of solutions to (1.1) subject to (1.2). The equation (1.1) can be rewritten in the form

$$y_1^3 - x_1^3 = x_2^3 + x_3^3 - y_2^3 - y_3^3. \tag{2.3}$$

The number of solutions with $x_1 = y_1$ can be bounded as before and is $O(PQ^2X^{\epsilon})$, which is acceptable. Hence, by symmetry, it suffices to bound the number S of solutions to (2.3) in which $y_1 > x_1$. In this case, let $h = y_1 - x_1$. Then (2.3) becomes

$$h(3x^2+3xh+h^2) = x_2^3+x_3^3-y_2^3-y_3^3, \tag{2.4}$$

where, for brevity, we have written x for y_1. Moreover

$$0 < h < H, \tag{2.5}$$

where

$$H = 3P^{3\psi-2}. \tag{2.6}$$

Rather than following directly Davenport's elementary argument, we introduce exponential sums as they lead naturally to the more modern developments. In the first instance our argument will mirror Davenport's. Let

$$f(\alpha;h) = \sum_{\frac{1}{2}P\leqslant x\leqslant P} e(\alpha h(3x^2+3xh+h^2)), \tag{2.7}$$

$$g(\alpha) = \sum_{\frac{1}{2}Q\leqslant x\leqslant Q} e(\alpha x^3), \tag{2.8}$$

where $e(\beta) = \exp(2\pi \mathrm{i})$. Thus, by the orthogonality of the additive characters on $\mathbb{R}/\mathbb{Z}$, we have

$$S \leqslant \int_0^1 \sum_{1\leqslant h\leqslant H} f(\alpha;h)\,|g(\alpha)|^4\,\mathrm{d}\alpha$$

and so, by Schwarz's inequality we have

$$S^2 \leqslant \left(\int_0^1 \sum_{1\leqslant h\leqslant H} |f(\alpha;h)|^2\,|g(\alpha)|^4\,\mathrm{d}\alpha\right)\left(H\int_0^1 |g(\alpha)|^4\,\mathrm{d}\alpha\right). \tag{2.9}$$

The first integral here is the number of solutions of the equation $3h(y_1^2-x_1^2)+3h^2(y_1-x_1) = x_2^3+x_3^3-y_2^3-y_3^3$. The number of solutions of this with $y_1 = x_1$ is $O(HPQ^{2+\epsilon})$ and the number of solutions with $y_1 \neq x_1$ is $O(Q^{4+\epsilon})$. Moreover the second integral is the number of solutions of the equation $x_2^3+x_3^3 = x_2'^3+x_3'^3$, and this has $O(Q^{2+\epsilon})$ solutions. We combine these estimates and obtain $S \ll PQ^{2+\epsilon}(HP^{-\frac{1}{2}}+H^{\frac{1}{2}}QP^{-1})$. Thus (1.4) will follow provided that $H = O(P^{\frac{1}{2}})$ and $H^{\frac{1}{2}}Q = (P)$. Hence, by (2.2) and (2.6), $\psi = \frac{4}{5}$ is an acceptable value of ψ and then we have

$$\operatorname{card}\mathscr{B}_{3,3} \gg X^{\frac{13}{15}-\epsilon} \quad (X > X_0(\epsilon)). \tag{2.10}$$

The use of exponential sums here suggests at once a possible improvement in the argument. The expression $\sum_{1\leqslant h\leqslant H}|f(\alpha;h)|^2$ occurring in (2.9) can be treated in a standard way, for example as in Vaughan (1985) or Lemma 3.1 of Vaughan (1989*a*). Thus, if a and q satisfy $(a,q) = 1$, $q \leqslant X$ and $|q\alpha - a| \leqslant 1/X$ where $P \ll X \ll HP$, then

$$\sum_{1\leqslant h\leqslant H} |f(\alpha;h)|^2 \ll \frac{HP^{2+\epsilon}}{q+Q^3\,|q\alpha-a|}+HP^{1+\epsilon}.$$

Now for most α in the unit interval there will be $q \leqslant X$ and a with $(a,q) = 1$ such that $|q\alpha - a| \leqslant 1/X$ and either $q \gg P$ or $Q^3\,|q\alpha-a| \gg P$. Let the set of such α in $(0,1]$ be denoted by $\mathfrak{m}$. Then for α on these 'minor arcs' $\mathfrak{m}$ we have $\sum_{1\leqslant h\leqslant H}|f(\alpha;h)|^2 \ll HP^{1+\epsilon}$, and so

$$\int_{\mathfrak{m}} \sum_{1\leqslant h\leqslant H} |f(\alpha;h)|^2\,|g(\alpha)|^4\,\mathrm{d}\alpha \ll HP^{1+\epsilon}Q^2.$$

For the range of ψ in which we shall be interested it transpires that the contribution to the integral from the 'major arcs' $\mathfrak{M} = (0,1]\backslash\mathfrak{m}$ is smaller (see Vaughan 1985). Thus we now have $S \ll HP^{\frac{1}{2}+\epsilon}Q^2$ and (1.4) will follow provided only that $H \ll P^{\frac{1}{2}}$. thus $\psi = \frac{5}{6}$ is an acceptable value of ψ and then we have

$$\text{card}\,\mathscr{B}_{3,3} \gg X^{\frac{8}{9}-\epsilon} \quad (X > X_0(\epsilon)). \tag{2.11}$$

The above arguments can be imitated by a so-called 'p-adic' method which has its genesis in Davenport (1942a) and this played an important role in suggesting the modern developments. The p-adic method runs along the following lines.

Let

$$\theta = 1-\psi, \quad P = (X/20)^{1/3}, \quad Q = P^{\psi}, \quad M = P/Q = P^{\theta}, \quad H = PM^{-3}. \tag{2.12}$$

We now define $R(n,p)$ to be the number of representations of n in the form

$$x^3+p^3(y_1^3+y_2^3) \quad \text{with} \quad (x,p)=1, x \leqslant P, y_j \leqslant Q \tag{2.13}$$

and take $R(n) = \Sigma_p R(n,p)$ where the sum is over the primes p with $M < p \leqslant 2M$, $p \equiv 2 \pmod 3$. If we can show that

$$\sum_n R(n)^2 \ll M^2PQ^2X^{\epsilon}, \tag{2.14}$$

then, as in §1, we have

$$\sum_{n,\,R(n)\neq 0} 1 \gg PQ^2X^{-2\epsilon}. \tag{2.15}$$

By Cauchy's inequality, we have $\Sigma_n R(n)^2 \leqslant M\Sigma_p\Sigma_n R(n,p)^2$, and here the double sum on the right is the number of solutions of

$$x'^3-x^3 = p^3(y_1^3+y_2^3-y_1'^3-y_2'^3) \tag{2.16}$$

with the variables as before. The number of solutions with $x'=x$ is $O(PQ^2MX^{\epsilon})$. Thus it remains to consider the solutions with $x'>x$. We have $p \equiv 2 \pmod 3$, $(xx',p) = 1$ and $x^3 \equiv x'^3 \pmod{p^3}$. Thus $x \equiv x' \pmod{p^3}$ and so the equation (2.16) is equivalent to

$$3hx^2+3h^2xp^3+h^3p^6 = y_1^3+y_2^3-y_2'^3-y_2'^2, \tag{2.17}$$

where we have written h for $(x'-x)p^{-3}$. Clearly h satisfies $|h| \leqslant PM^{-3} = H$ where H is as before, and the number of solutions with $x'>x$ is bounded by

$$\int_0^1 \sum_{M \leqslant p \leqslant 2M} \sum_{1 \leqslant h \leqslant H} f(\alpha;h,p)|g(\alpha)|^4\,\mathrm{d}\alpha, \tag{2.18}$$

where $g(\alpha)$ is as above and

$$f(\alpha;h,p) = \sum_{x \leqslant P} e(\alpha h(3x^2+3xhp^3+h^2p^6)). \tag{2.19}$$

Much as above it can be shown that for α on an appropriate set of minor arcs $\mathfrak{m}$ we have

$$\sum_{M<p\leqslant 2M} \sum_{1\leqslant h\leqslant H} |f(\alpha;h,p)|^2 \ll HMP^{1+\epsilon},$$

and so the contribution to the integral from these α is $\ll HMP^{\frac{1}{2}}Q^2X^{\epsilon}$. It can further be shown that, again under appropriate conditions, the $\mathfrak{M}$ make a smaller contribution to the integral. Thus we find that $\Sigma_n R(n)^2 \ll M^2(P+HP^{\frac{1}{2}})\,Q^2 X^{\epsilon}$, and once more the optimal choice for ψ is $\frac{5}{6}$ and so by (2.15) we have another proof of (2.10). However, this argument allows of two further important improvements.

First of all, the left-hand side of (2.17) is quadratic in x, and on completing the square and replacing x by $z = 2x+hp^3$ we see that it becomes

$$3hz^2+h^3p^6 = 4y_2'^3+4_2'^3-4y_1^3-4y_2^3. \tag{2.20}$$

More precisely, if we take $h = (x'-x)\,p^{-3}$ and $z = x'+x$ in (2.16) and suppose that $x' > x$, then we obtain (2.20) with

$$h \leqslant H, \quad z \leqslant 2P, \quad M < p \leqslant 2M, \quad y_j \leqslant Q \tag{2.21}$$

and the other variables as before. The number of solutions of (2.20) with (2.21) is

$$\int_0^1 \mathscr{F}(\alpha)\,|g(4\alpha)|^4\,\mathrm{d}\alpha,$$

where

$$\mathscr{F}(\alpha) = \sum_{1\leqslant h\leqslant H} F(\alpha;h)\,G(\alpha;h), \tag{2.22}$$

$$F(\alpha;h) = \sum_{z\leqslant 2P} \mathrm{e}(\alpha 3hz^2), \tag{2.23}$$

$$G(\alpha;h) = \sum_{M<p\leqslant 2M} \mathrm{e}(\alpha h^2 p^6). \tag{2.24}$$

Again, on the minor arcs we have $\Sigma_{h\leqslant H}|F(\alpha;h)|^2 \ll HPX^{\epsilon}$. Moreover, the separation of the 'x' part from the 'p' part means that there is the possibility of a further saving through a non-trivial estimate for $\Sigma_{h\leqslant H}|G(\alpha;h)|^2$. In fact, it can be shown (Vaughan 1986) under suitable conditions that this last expression is $O(HMX^{\epsilon})$ on the $\mathfrak{m}$, and so

$$\mathscr{F}(\alpha) \ll H(PM)^{\frac{1}{2}}X^{\epsilon}. \tag{2.25}$$

Thus one obtains $\Sigma_n R(n)^2 \ll M^2(P+HP^{\frac{1}{2}}M^{-\frac{1}{2}})\,Q^2 X^{\epsilon}$, and the optimal choice of ψ is $\frac{6}{7}$. Therefore, one obtains

$$\operatorname{card}\mathscr{B}_{3,3} \gg X^{\frac{19}{21}-\epsilon} \quad (X > X_0(\epsilon)). \tag{2.26}$$

Differences of the kind $((x+hp^3)^3-x^3)\,p^{-3}$ are often referred to as *efficient differences*.

The second improvement which can be introduced here stems from the observation that in the 'p-adic' method each of the cubes in a representation ranges out to P, i.e. it restores a measure of homogeneity. This can be exploited in the following way.

For a suitable large parameter L let $\mathscr{P}$ and $\mathscr{Q}$ denote the set of numbers of the form $p_1 \dots p_L$ and $p_2 \dots p_L$, respectively, with $P^{\theta(1-\theta)^{j-1}} < p_j \leqslant 2P^{\theta(1-\theta)^{j-1}}$ and $p_j \equiv 2 \pmod 3$ and then define $R(n;\mathscr{R})$ to be the number of representations of n in the form $x_1^3+x_2^3+x_3^3$ with $x_j \in \mathscr{R}$. Thus we have the possibility of comparing $\Sigma_n R(n;\mathscr{P})^2$ with $\Sigma_n R(n;\mathscr{Q})^2$ and thereby setting up an iterative process of a new kind.

Somehow, we need to introduce the condition $(x,p) = 1$ which is made use of in the previous argument, i.e. we need to show that the dominant contribution comes from the 'non-singular solutions' to the congruence which arises. In the processes we describe below this step is usually dealt with by a suitable 'fundamental lemma'. The sum $\Sigma_n R(n;\mathscr{P})^2$ is the number of solutions of

$$x_1^3+x_2^3+x_3^3 = x_1'^3+x_2'^3+x_3'^3 \tag{2.27}$$

with each of the variables in $\mathscr{P}$. Let

$$f(\alpha) = \sum_{x\in\mathscr{P}} e(\alpha x^3), \quad g(\alpha) = \sum_{x\in\mathscr{Q}} e(\alpha x^3). \tag{2.28}$$

Then the number of solutions in which at least one pair of the variables have a common factor in $(M, 2M]$ has order of magnitude at most

$$\sum_{M<p\leqslant 2M} \int_0^1 |f(\alpha)^4 g(\alpha p^3)^2|\, d\alpha,$$

and by Hölder's inequality this does not exceed

$$M\Big(\sum_n R(n;\mathscr{P})^2\Big)^{\frac{2}{3}}\Big(\sum_n R(n;\mathscr{Q})^2\Big)^{\frac{1}{3}}.$$

Thus if the solutions of this kind account for at least one half of all solutions, then we can conclude that

$$\sum_n R(n;\mathscr{P})^2 \ll M^3 \sum_n R(n;\mathscr{Q})^2. \tag{2.29}$$

Suppose on the contrary that less than one half of all solutions to (2.27) are of this kind. Then

$$\sum_n R(n;\mathscr{P})^2 \ll \sum_{p_1}\sum_{p_2}\sum_{p_3}\sum_{p_4} \int_0^1 |f(\alpha; p_1p_2p_3p_4)^2 g(\alpha p_1^3)\, g(\alpha p_2^3)\, g(\alpha p_3^3)\, g(\alpha p_4^3)|\, d\alpha,$$

where each prime p_j satisfies $p_j \equiv 2 \pmod 3$ and $M < p_j \leqslant 2M$, and

$$f(\alpha; m) = \sum_{\substack{x\in\mathscr{P}\\ (x,m)=1}} e(\alpha x^3). \tag{2.30}$$

By Hölder's inequality the above integral does not exceed

$$\sum_{p_1}\sum_{p_2}\sum_{p_3}\sum_{p_4} \int_0^1 |f(\alpha; p_1p_2p_3p_4)|^2\, |g(\alpha p_1^3)|^4\, d\alpha.$$

This in turn does not exceed M^3 times the number of solutions of (2.16) with $x \leqslant P$, $x' \leqslant P, M < p \leqslant 2M, p \equiv 2 \pmod 3$, $y_j \in \mathscr{Q}$. The number of solutions with $x' = x$ is $O(PMQ^2X^{\epsilon})$. The remaining solutions are dealt with initially as in our original description of the 'p-adic' method above. Thus we obtain

$$\sum_n R(n;\mathscr{P})^2 \ll PM^4Q^2X^{\epsilon} + M^3 \int_0^1 \mathscr{F}(\alpha)\, |g(\alpha)|^4\, d\alpha. \tag{2.31}$$

By Hölder's inequality, the integral here is bounded by

$$\Big(\int_0^1 |\mathscr{F}(\alpha)|^3\, d\alpha\Big)^{\frac{1}{3}}\Big(\int_0^1 |g(\alpha)|^6 d\alpha\Big)^{\frac{2}{3}}. \tag{2.32}$$

Now $\int_0^1 |\mathscr{F}(\alpha)|^2\, d\alpha$ is the number of solutions of the equation $3hx^2 + h^3p^6 = 3h'x'^2 + h'^3p'^6$ and this is readily seen to be $O(HPMX^{\epsilon})$. On the minor arcs $\mathfrak{m}$ we have

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

(2.25) and it can be shown (Vaughan 1989*a*) that for an appropriate choice of parameters the contribution from the major arcs $\mathfrak{M}$ is no larger. Thus

$$\int_0^1 |\mathscr{F}(\alpha)|^3 \, d\alpha \ll H^2 (PM)^{\frac{3}{2}} x^{2\epsilon}. \tag{2.33}$$

The second integral in (2.32) is nothing other than $\Sigma_n R(n;\mathscr{Q})^2$. Thus

$$\sum_n R(n;\mathscr{P})^2 \ll X^{\epsilon}\left(PM^4 Q^2 + H^{\frac{2}{3}} P^{\frac{1}{2}} M^{\frac{7}{6}} \left(\sum_n R(n;\mathscr{Q})^2\right)^{\frac{2}{3}}\right).$$

Now we wish to find the smallest real number $\lambda \geqslant 3$ such that $\Sigma_n R(n;\mathscr{Q})^2 \ll Q^{\lambda+\epsilon}$ implies

$$\sum_n R(n;\mathscr{P})^2 \ll P^{\lambda+\epsilon}. \tag{2.34}$$

If (2.29) holds, then we may expect to be able to take $\lambda = 3$. On the other hand, if (2.34) holds, then we expect that

$$P^{\lambda} \ll X^{\epsilon}(PM^4 Q^2 + H^{\frac{2}{3}} (PM)^{\frac{1}{2}} Q^{2\lambda/3}). \tag{2.35}$$

In this case, when ψ, or equivalently θ, is chosen optimally, we have

$$\lambda = 3 + 2\theta = \tfrac{2}{3}(1-3\theta) + \tfrac{1}{2}(1+7\theta) + \tfrac{2}{3}(1-\theta)(3+2\theta).$$

Thus $\theta = \frac{1}{8}$, $\psi = \frac{7}{8}$ give $\lambda = \frac{13}{4}$, and so

$$\operatorname{card} \mathscr{B}_{3,3} \gg X^{\frac{11}{12}-\epsilon} \quad (X > X_0(\epsilon)). \tag{2.36}$$

An appropriate inductive argument to establish this is constructed along these lines in the proof of Theorem 1.3 of Vaughan (1989*a*).

3. The introduction of numbers without large prime factors

Although the case of three cubes discussed above illustrates many of the salient features of the modern theory, in one important respect it obscures an issue. It is clear that the techniques described above are essentially iterative, i.e. generally we bound the number of solutions of (1.2) in terms of the number of solutions of (1.2) with the variables lying in a smaller set and with s replaced by various values of t not exceeding s. When $s = 3$ the values of t which arise are $t = 3$ and $t = 2$. Bounding the number of solutions when $t = 2$ is essentially trivial.

When $s > 3$, the case in which $t = s-1$ is no longer trivial, and we may wish to apply our iterative procedure to the new equation. But then the optimal value of θ may well be different from the optimal value which arises in the case $t = s$. Thus we need to find a substitute for the set $\mathscr{P}$ in which most elements have a plentiful supply of suitable divisors.

Let $\mathscr{A}(P,R)$ denote the set of natural numbers not exceeding P which have no prime factor exceeding R. This set has the remarkable property that, given any M with $M < P$, then any $a \in \mathscr{A}(P,R)$ with $M < a$ has a divisor m with $M < m \leqslant MR$. In practice we usually take $R = P^{\eta}$ where η is a small but fixed positive number.

The set $\mathscr{A}(P,R)$ has great flexibility in this regard. However, we now have to concern ourselves with two new problems. Firstly, there is the problem of dealing

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

with the 'singular solutions' of the congruence which arises. Secondly, there is the analogue of the condition $p \equiv 2 \pmod 3$ which occurs in the 'p-adic' method described above.

The first problem is more central and usually is overcome by a 'fundamental lemma'. We describe below the various fundamental lemmas which have been devised to deal with this situation. The second of the problems is something of a red herring, and is easily overcome by a technical device, introduced in Vaughan (1986), which is simply described.

We have to bound the number N of solutions of an equation of the form

$$x^k + m^k u = x'^k + m^k u' \tag{3.1}$$

where $x \in \mathscr{A}$, $x' \in \mathscr{A}$ with $\mathscr{A} \subset [1, P] \cap \mathbb{N}, M < m \leqslant 2M$, $(xx', m) = 1, u \in \mathscr{B}$, $u' \in \mathscr{B}$ with $\mathscr{B}$ a finite subset of $\mathbb{N}$, and each element u of $\mathscr{B}$ is counted with weight $\sigma(u)$, say. Thus

$$N = \sum_{m} \sum_{\substack{y \,(\mathrm{mod}\, m^k) \\ (y,m)=1}} \sum_{\substack{y' \,(\mathrm{mod}\, m^k) \\ y'^k \equiv y^k \,(\mathrm{mod}\, m^k)}} \int_0^1 f(\alpha; m, y) f(-\alpha; m, y') \, |S(\alpha m^k)|^2 \, \mathrm{d}\alpha,$$

where

$$f(\alpha; m, y) = \sum_{\substack{x \in \mathscr{A} \\ x \equiv y \,(\mathrm{mod}\, m^k)}} e(\alpha x^k), \tag{3.2}$$

$$S(\alpha) = \sum_{u \in \mathscr{B}} \sigma(u) \, e(\alpha u). \tag{3.3}$$

Hence, by Cauchy's inequality,

$$N \leqslant \sum_{m} \sum_{\substack{y \,(\mathrm{mod}\, m^k) \\ (y,m)=1}} \rho(y) \int_0^1 |f(\alpha; m, y) S(\alpha m^k)|^2 \, \mathrm{d}\alpha,$$

where $\rho(y)$ is the number of solutions of the congruence $z^k \equiv y^k \pmod{m^k}$. Since $(y, m) = 1$ we have $\rho(y) \ll m^{\epsilon}$. Thus

$$N \ll N' M^{\epsilon}, \tag{3.4}$$

where N' is the number of solutions of (3.1) with $x \equiv x' \pmod{m^k}$ in addition to the previous conditions. Thus N' is the precise analogue of the situation which occurred in the p-adic method described above.

4. Fundamental lemmas

Let $S_s(P, R)$ denote the number of solutions of

$$x_1^k + \ldots + x_s^k = y_1^k + \ldots + y_s^k, \tag{4.1}$$

with

$$x_i \in \mathscr{A}(P, R), \quad y_i \in \mathscr{A}(P, R), \tag{4.2}$$

and for a given real number θ with $0 < \theta < 1$ let $T_s(P, R, \theta)$ denote the number of solutions of

$$x^k + m^k(x_1^k + \ldots + x_{s-1}^k) = y^k + m^k(y_1^k + \ldots + y_{s-1}^k), \tag{4.3}$$

with

$$x, y \leqslant P, \quad x \equiv y \,(\mathrm{mod}\, m^k), \quad P^{\theta} < m \leqslant \min(P, P^{\theta} R), \quad x_i, y_i \in \mathscr{A}(P^{1-\theta}, R). \tag{4.4}$$

Then the following lemma is established in Vaughan (1989a, Lemma 2.1).

Lemma 1. *Let $\theta = \theta(s,k)$ satisfy $0 < \theta < 1$ and suppose that $1 \leqslant D \leqslant P$. Then*

$$S_s(P,R) \ll \left(\sum_{d>D} S_s(P/d,R)^{1/s}\right)^s + S_s(D^{1-\theta}P^{\theta},R) + P^{\epsilon}\left(\sum_{d\leqslant D}((P/d)^{\theta}R)^{2-3/s}\,T_s(P/d,R,\theta)^{1/s}\right)^s.$$

When $s > k$ and R is not too small by comparison with P we expect that $S_s(P,R) \approx P^{\sigma}$ and $T_s(P,R,\theta) \approx P^{\tau}$ with $\sigma > s$, $\tau > s$. Thus for a suitable choice of D the first two terms on the right of the above inequality can be expected to be small compared with the left-hand side and the third term will be dominated by the term in the sum with $d = 1$. Thus in principle the lemma says that either $S_s(P,R) \ll P^s$or $S_s(P,R) \ll (P^{\theta}R)^{2s-3}T_s(P,R,\theta)$, and so is eminently suitable for solving the first problem described above.

Let

$$M = P^{\theta}, \quad Q = P/M. \tag{4.5}$$

Then
$$T_s(P,R,\theta) \leqslant PMRS_{s-1}(Q,R) + 2U_s(P,R,M),$$

where $U_s(P,R,M)$ is the number of solutions of (4.3) with (4.4) and $x > y$. Moreover

$$U_s(P,R,M) \leqslant \int_0^1 F(\alpha)\,|g(\alpha)|^{2s-2}\,\mathrm{d}\alpha,$$

where
$$F(\alpha) = \sum_{h,m,x} e(\alpha((x+hm^k)^k - x^k)\,m^{-k})$$

with $h \leqslant H = PM^{-k}, M < m \leqslant MR, x \leqslant P$, and

$$g(\alpha) = \sum_{x\in\mathscr{A}(Q,R)} e(\alpha x^k).$$

We may proceed now by making various estimates for the exponential sum F and combine these with various forms of Hölder's inequality to set up an iterative procedure between $S_s(P,R)$ and $S_t(Q,R)$ with various choices of t and Q. This was done in Vaughan (1989*a*, *b*) and Vaughan & Wooley (1991).

The methods described so far use one efficient difference, but then to deal with the exponential sum F advert to ordinary subsequent differences. The question naturally arises as to whether it is possible to make use of repeated efficient differences. The fundamental lemma described above is not well suited to this end, at least in the form given, as apparently it makes special use of the properties of kth powers.

Wooley (1992*a*) has shown how by use of a refined fundamental lemma repeated efficient differences may be introduced. Let $\Psi(z,\boldsymbol{c})$ denote a polynomial in the variables $z, c_1, \ldots, c_t$ with integer coefficients and having degree at least one in z, and let $S_s(P,Q,R)$ denote the number of solutions of

$$\Psi(z,\boldsymbol{c}) + x_1^k + \ldots + x_s^k = \Psi(z',\boldsymbol{c}') + y_1^k + \ldots + y_s^k \tag{4.6}$$

with $x_j \in \mathscr{A}(Q,R)$, $y_j \in \mathscr{A}(Q,R)$, $1 \leqslant z \leqslant P$, $1 \leqslant z' \leqslant P$, $C_j' < c_j \leqslant C_j$, $C_j' < c_j' \leqslant C_j$. In particular, when $\Psi = z^k$, $t = 0$, $Q = P$, we have $S_s(P,Q,R) = S_{s+1}(P,R)$. Further, let $T_s(P,Q,R;\theta)$ denote the number of solutions of

$$\Psi(z,\boldsymbol{c}) + w^k(u_1^k + \ldots + u_s^k) = \Psi(z',\boldsymbol{c}) + w^k(v_1^k + \ldots + v_s^k) \tag{4.7}$$

with $z, z', \boldsymbol{c}$ as above and $P^\theta < w \leqslant \min(Q, P^\theta R)$, $u_j \in \mathscr{A}(QP^{-\theta}, R), v_j \in \mathscr{A}(QP^{-\theta}, R)$, $z \equiv z' \pmod{w^k}$. Finally take $N_s(P, Q, R)$ denote the number of solutions of (4.6) with

$$\frac{\partial \Psi}{\partial z}(z, \boldsymbol{c}) = \frac{\partial \Psi}{\partial z'}(z', \boldsymbol{c}') = 0.$$

Lemma 2. *Suppose that* $\theta = \theta(s,k)$ *satisfies* $1 < P^\theta < Q$. *Then*

$$S_s(P,Q,R) \ll P^\epsilon \left(\prod_{i=1}^{t} C_i\right)(P^\theta R)^{2s-1} T_s(P,Q,R;\theta) + QP^{\theta+\epsilon} S_{s-1}(P,Q,R) + S_s(P,P^\theta,R) + N_s(P,Q,R).$$

5. Repeated efficient differences

The introduction of repeated efficient differences leads to more complex iterative processes than have been used hitherto.

For each $s \in \mathbb{N}$ we take $\phi_i = \phi_{i,s}$ $(i = 1, \ldots, k)$ to be real numbers, with $0 \leqslant \phi_i \leqslant 1/k$, to be chosen later. We then take

$$P_j = 2^j P, \quad M_j = P^{\phi_j}, \quad H_j = P_j M_j^{-k}, \quad Q_j = P_j(M_1 \ldots M_j)^{-1} \quad (1 \leqslant j \leqslant k).$$

For the sake of concision, we shall also adopt the convention of writing

$$\tilde{H}_j = \prod_{i=1}^{j} H_i \quad \text{and} \quad \tilde{M}_j = \prod_{i=1}^{j} M_i R.$$

We define the modified forward difference operator, Δ_1^*, by

$$\Delta_1^*(f(x); h; m) = m^{-k}(f(x + hm^k) - f(x)),$$

and define Δ_j^* recursively by

$$\Delta_{j+1}^*(f(x); h_1, \ldots, h_{j+1}; m_1, \ldots, m_{j+1}) = \Delta_1^*(\Delta_j^*(f(x); h_1, \ldots, h_j; m_1, \ldots, m_j); h_{j+1}; m_{j+1}).$$

We also adopt the convention that $\Delta_0^*(f(x); h; m) = f(x)$.

For $0 \leqslant j \leqslant k$ let

$$\Psi_j = \Psi_j(z; h_1, \ldots, h_j; m_1, \ldots, m_j) = \Delta_j^*(f(z); 2h_1, \ldots, 2h_j; m_1, \ldots, m_j),$$

where $f(z) = (z - h_1 m_1^k - \ldots - h_j m_j^k)^k$.

Write

$$f_j(\alpha) = \sum_{z \in \mathscr{A}(Q_j, R)} e(\alpha x^k).$$

Also, write
$$F_j(\alpha) = \sum_{z, \boldsymbol{h}, \boldsymbol{m}} e(\alpha \Psi_j(z; \boldsymbol{h}; \boldsymbol{m})),$$

where the summation is over z, $\boldsymbol{h}, \boldsymbol{m}$ with

$$1 \leqslant z \leqslant P_j, \quad M_i < m_i \leqslant M_i R, \quad m_i \in \mathscr{A}(P, R), \quad 1 \leqslant h_i \leqslant 2^{j-i} H_i \quad (1 \leqslant i \leqslant j). \tag{5.1}$$

Suppose that the real numbers λ_s have the property that

$$S_s(P, R) \ll P^{\lambda_s + \epsilon}. \tag{5.2}$$

Such numbers certainly exist, since we may trivially take $\lambda_s = 2s$.

We list below some useful lemmata taken from Vaughan & Wooley (1993*a*). They are fairly immediate consequences of Wooley's fundamental lemma and Schwarz's inequality.

Lemma 3. *We have*

$$\int_0^1 |F_0(\alpha)^2 f_0(\alpha)^{2s}|\,\mathrm{d}\alpha \ll P^{\epsilon} M_1^{2s-1}\left(PM_1\,Q_1^{\lambda_s+\epsilon} + \int_0^1 |F_1(\alpha) f_1(\alpha)^{2s}|\,\mathrm{d}\alpha\right). \tag{5.3}$$

Lemma 4. *Whenever* $0 < t < s$ *and* $1 \leqslant j \leqslant k-1$, *we have*

$$\int_0^1 |F_j(\alpha) f_j(\alpha)^{2s}|\,\mathrm{d}\alpha \ll P^{\epsilon}(Q_j^{\lambda_t})^{\frac{1}{2}}(\tilde{H}_j \tilde{M}_j M_{j+1}^{4s-2t-1}\,T_{j+1})^{\frac{1}{2}}, \tag{5.4}$$

where

$$T_{j+1} = T_{j+1}(P;\boldsymbol{\lambda};\boldsymbol{\varphi}) = P\tilde{H}_j \tilde{M}_{j+1}\,Q_{j+1}^{\lambda_{2s-t}} + \int_0^1 |F_{j+1}(\alpha) f_{j+1}(\alpha)^{4s-2t}|\,\mathrm{d}\alpha. \tag{5.5}$$

There are two other ways of estimating the integral on the left-hand side of equation (5.4).

(H) We may apply Hölder's inequality in the form

$$\int_0^1 |F_j(\alpha) f_j(\alpha)^{2s}|\,\mathrm{d}\alpha \ll I_1^{\alpha} I_2^{\beta}\,U_v^{\gamma}\,U_w^{\delta},$$

where

$$I_m = \int_0^1 |F_j(\alpha)|^{2m}\,\mathrm{d}\alpha \quad (m=1,2) \quad U_u = \int_0^1 |f_j(\alpha)|^{2u}\,\mathrm{d}\alpha \quad (u = v, w),$$

in which v and w are non-negative integers and $\alpha, \beta, \gamma, \delta$ are non-negative real numbers with

$$\alpha+\beta+\gamma+\delta = 1, \quad 2\alpha+4\beta = 1, \quad v\gamma+w\delta = s.$$

The second and fourth power mean values of F_j may be estimated in terms of the number of solutions of certain diophantine equations. Also, we have $U_v \ll Q_j^{\lambda_v+\epsilon}$ and $U_w \ll Q_j^{\lambda_w+\epsilon}$. There is, of course, the possibility of using higher moments of $F_j(\alpha)$. However, estimates for such moments are too weak to be of value in the current state of knowledge.

(M) We may apply the Hardy–Littlewood method along the lines of §3 of Vaughan (1989*a*).

By considering the underlying diophantine equations, we have

$$S_{s+1}(P,R) \ll \int_0^1 |F_0(\alpha)^2 f_0(\alpha)^{2s}|\,\mathrm{d}\alpha,$$

and hence we may use a sequence Σ_s of connected inequalities (in the obvious sense) to bound $S_s(Q,R)$ in terms of $S_t(Q',R)$ $(t = 1,2,\ldots)$. Such a sequence is called an *iterative procedure*. A finite subsequence of a sequence $(\Sigma_s)_1^{\infty}$ of iterative procedures is called an *iterative scheme*.

We now outline the main strategy. Suppose that we have taken $j+1$ differences, and so are left to bound an expression of the form T_{j+1}, as defined by equation (5.5). By applying a process of the type (H) or (M), we may obtain a bound of the form

$$T_{j+1} \ll P\tilde{H}_j \tilde{M}_{j+1}\,Q_{j+1}^{\lambda_{2s-t}} + V(P;\boldsymbol{\lambda};\boldsymbol{\varphi}), \tag{5.6}$$

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

for some expression $V(P;\boldsymbol{\lambda};\boldsymbol{\varphi})$ depending explicitly only on P, $\boldsymbol{\lambda}$, and $\boldsymbol{\varphi}=(\phi_1,\ldots,\phi_{j+1})$. We may then obtain a bound for T_{j+1} by minimizing the expression on the right-hand side of (5.6). In our applications, a close approximations to the minimum occurs when a choice of $\boldsymbol{\varphi}$ is taken so that $P\tilde{H}_j\tilde{M}_{j+1}Q_{j+1}^{\lambda_{2s-t}}\approx V(P;\boldsymbol{\lambda};\boldsymbol{\varphi})$, where we use the symbol to mean that we have ignored constants and powers of R and P^{ϵ}.

This relation determines some equation,

$$\Lambda_{j+1}(\boldsymbol{\lambda};\boldsymbol{\varphi})=0, \tag{5.7}$$

connecting the ϕ_i $(1\leqslant i\leqslant j+1)$ in an obvious manner. With the optimal choice of $\boldsymbol{\varphi}$ given by (5.7), the bound (5.4) now becomes

$$\int_0^1|F_j(\alpha)f_j(\alpha)^{2s}|\,\mathrm{d}\alpha\ll P^{\epsilon}(P\tilde{H}_j^2\tilde{M}_j^2M_{j+1}^{4s-2t}Q_j^{\lambda_t}Q_{j+1}^{\lambda_{2s-t}})^{\frac{1}{2}}.$$

This bound may now be used to bound an expression of the form T_j via Lemma 4, and we obtain an inequality of the form

$$T_j\ll P^{\epsilon}(P\tilde{H}_{j-1}\tilde{M}_jQ_j^{\lambda_s}+(P\tilde{H}_j^2\tilde{M}_j^2M_{j+1}^{4s-2t}Q_j^{\lambda_t}Q_{j+1}^{\lambda_{2s-t}})^{\frac{1}{2}}).$$

Optimizing the right-hand side gives rise to a further equation connecting the $\boldsymbol{\varphi}$, say $\Lambda_j(\boldsymbol{\lambda};\boldsymbol{\varphi})=0$. We may continue this process, next bounding an expression of the form

$$\int_0^1|F_{j-1}(\alpha)f_{j-1}(\alpha)^{2u}|\,\mathrm{d}\alpha$$

in like manner, and so on.

In this way, for each s we obtain $j+1$ equations $\Lambda_i^{(s)}(\boldsymbol{\lambda};\boldsymbol{\varphi})=0$ $(1\leqslant i\leqslant j+1)$, in $j+1$ variables ϕ_i $(1\leqslant i\leqslant j+1)$. These permit us to solve for $\boldsymbol{\varphi}$ in terms of $\boldsymbol{\lambda}$, and, provided that a solution is found with $0\leqslant\phi_i\leqslant 1/k$ for each $1\leqslant i\leqslant j+1$, it follows that

$$\int_0^1|F_0(\alpha)^2f_0(\alpha)^{2s}|\,\mathrm{d}\alpha\ll P^{1+\epsilon}M_1^{2s}Q_1^{\lambda_s},$$

with ϕ_1 given by the solution $\boldsymbol{\varphi}$ of the simultaneous equations $\boldsymbol{\Lambda}^{(s)}(\boldsymbol{\lambda};\boldsymbol{\varphi})=0$. It therefore follows that

$$S_{s+1}(P,R)\ll P^{\lambda'_{s+1}+\epsilon},$$

with $\lambda'_{s+1}=\lambda_s(1-\phi_1)+1+2s\phi_1$.

By adopting this entire process for $s=1,2,\ldots,$ we may define a new sequence of exponents, $\boldsymbol{\lambda}^+$, by taking $\lambda_s^+=\min\{\lambda'_s,\lambda_s\}$ $(s=1,2,\ldots)$. Thus, we have the sequence of bounds

$$S_s(P,R)\ll P^{\lambda_s^++\epsilon}.$$

In principle we may obtain the optimal $\boldsymbol{\lambda}$ by solving the equations $\boldsymbol{\lambda}=\boldsymbol{\lambda}^+$. Indeed, for smaller values of s, and in particular when the λ_t with $t>s$ do not occur explicitly in the formulae involving λ_s, this may be the easiest way to proceed. In practice, however, we proceed to calculate values for $\boldsymbol{\lambda}$ as follows. Starting from a known sequence $\boldsymbol{\lambda}$ we calculate $\boldsymbol{\lambda}^+$ as described above. Then we use the λ_s^+ in place of the λ_s in the equations $\boldsymbol{\Lambda}^{(r)}(\boldsymbol{\lambda};\boldsymbol{\varphi})=0$. Thus, by applying this iterative scheme repeatedly, we obtain a sequence of sequences $(\lambda_s^{(r)})$ with $\lambda_s^{(r+1)}\leqslant\lambda_s^{(r)}$ for each r and s. Since diagonal solutions provide us with the lower bound $\lambda_s^{(r)}\geqslant s$, the sequence must converge to some limit (λ_s^*). Moreover, $\boldsymbol{\lambda}^*$ has the property that

$$S_s(P,R)\ll P^{\lambda_s^*+\epsilon}. \tag{5.8}$$

The method outlined above involves an iteration process in which each $\lambda_s^{(r+1)}$ ($1 \leqslant s < \infty$) depends on each $\lambda_s^{(r)}$ ($1 \leqslant s < \infty$). Sometimes economies may be made in this procedure. Thus, for example, for s exceeding some s_0 we have $\lambda_s^* = 2s-k$. Further, for certain values of s the iterative procedure for λ_s may be independent of λ_t for $t > s$. In this latter case it may then be possible to obtain λ_s^* independently of λ_t^* ($t > s$). The detailed analyses and calculations are extremely complicated. They and various applications of the mean values (5.8) are given in Harman (this volume), Vaughan & Wooley (this volume, 1993*a*, *b*, *c*) and Wooley (1992*a*, 1993*a*). In Waring's problem, where as usual $G(k)$ is the smallest s such that every sufficiently large natural number n is the sum of at most s non-negative kth powers, they lead to the upper bounds $G(k) \leqslant k \log k + k \log\log k + o(k)$ for large k and to $G(5) \leqslant 17$, $G(6) \leqslant 24$, $G(7) \leqslant 33$, $G(8) \leqslant 42$, $G(9) \leqslant 51$. Wooley (1993*b*, Theorem 2.1) has recently obtained (5.8) with $\lambda_s = 2s - k + k\,e^{1-2s/k}$ and this leads to the refined upper bound

$$G(k) \leqslant k\left(\log k + \log\log k + 2 + \log 2 + \frac{\log\log k}{\log k}(1+o(1))\right).$$

Also, the recent work by Wooley on Vinogradov's mean value theorem (1992*b*, 1993*b*) is motivated in spirit, at least, by the ideas described here.

6. Exponential sums

We may view (5.8) as giving a bound for the $2s$th mean of the exponential sum

$$g(\alpha) = \sum_{x \in \mathscr{A}(P,R)} e(\alpha x^k). \tag{6.1}$$

In applications it is often essential to have estimates for the individual sum also. When α is close to a rational number with a relatively small denominator there may well be a technical requirement for an asymptotic formula for $g(\alpha)$, see Lemma 5.4 of Vaughan (1989*a*). Such results are usually poor compared with the case when the sum is over all x in an interval, in spite of various estimates (Vaughan & Wooley 1991, Lemmas 7.2 and 8.5) which have the effect in essence of extending the range of validity of the asymptotic formula. Thus normally this would not be the reason for the introduction of numbers without large prime factors to a problem.

When α is close to a rational number with a relatively large denominator, however, the situation is reversed. For large k the best general bound for the complete sum

$$f(\alpha) = \sum_{x \leqslant P} e(\alpha x^k) \tag{6.2}$$

is that of Corollary 1.1 of Wooley (1992*b*) which, in particular, tells us that when $|q\alpha - a| \leqslant P^{1-k}$, $(a,q)=1, P < q \leqslant P^{k-1}$ we have

$$f(\alpha) \ll P^{1-\sigma+\epsilon},$$

where $1/\sigma \sim 2k^2 \log k$. On the other hand the methods of Vaughan (1989*a*, §10) and Wooley (1992*a*) in the same circumstances give

$$g(\alpha) \ll P^{1-\rho+\epsilon},$$

where $1/\rho \sim 2k \log k$. Again an important ingredient is that the bulk of the elements

PHILOSOPHICAL TRANSACTIONS OF THE ROYAL SOCIETY A MATHEMATICAL, PHYSICAL & ENGINEERING SCIENCES

of $\mathscr{A}(P,R)$ have convenient factoring properties. In this instance the following lemma, Lemma 10.1 of Vaughan (1989*a*), is most useful.

Lemma 5. *Suppose that* $2 \leqslant R \leqslant M < y \leqslant P$ *and* $y \in \mathscr{A}(P,R)$. *Then there is a unique triple* (p,u,v) *with*

(i) $y = uv$,

(ii) $u \in \mathscr{A}(Q/v, p)$,

(iii) $M < v \leqslant Mp$,

(iv) $p \mid v$,

(v) $p' \mid v \Rightarrow p \leqslant p' \leqslant R$.

This lemma enables us to write $g(\alpha)$ as a combination of bilinear forms which then may be bounded *via* the large sieve and the mean value estimates (5.8).

References

Davenport, H. 1938 Sur les sommes de puissances entières. *C.r. hebd. Séanc. Acad. Sci. Paris* **207**, 1366–1368.

Davenport, H. 1939*a* On Waring's problem for cubes. *Acta Math.* **71**, 123–143.

Davenport, H. 1939*b* On sums of positive integral *k*th powers. *Proc. R. Soc. Lond.* A **170**, 293–299.

Davenport, H. 1939*c* On Waring's problem for fourth powers. *Ann. Math.* **40**, 731–747.

Davenport, H. 1942*a* On sums of positive integral *k*th powers. *Am. J. Math.* **64**, 189–198.

Davenport, H. 1942*b* On Waring's problem for fifth and sixth powers. *Am. J. Math.* **64**, 199–207.

Davenport, H. 1950 Sums of three positive cubes. *J. Lond. math. Soc.* **25**, 339–343.

Davenport, H. 1977 *The collected works of Harold Davenport*, vol. III (ed. B. J. Birch, H. Halberstam & C. A. Rogers). London: Academic Press.

Davenport, H. & Erdös, P. 1939 On sums of positive integral *k*th powers. *Ann. Math.* **40**, 533–536.

Hardy, G. H. & Littlewood, J. E. 1925 Some problems of 'partitio numerorum'. VI. Further researches in Waring's problem. *Math. Z.* **23**, 1–37.

Vaughan, R. C. 1981 *The Hardy–Littlewood method*. Cambridge University Press.

Vaughan, R. C. 1985 Sums of three cubes. *Bull. Lond. math. Soc.* **17**, 17–20.

Vaughan, R. C. 1986 On Waring's problem for cubes. *J. Math.* **385**, 122–170.

Vaughan, R. C. 1989*a* A new iterative method in Waring's problem. *Acta Math.* **162**, 1–70.

Vaughan, R. C. 1989*b* A new iterative method in Waring's problem. II. *J. Lond. math. Soc.* **39**, 219–230.

Vaughan, R. C. & Wooley, T. D. 1991 On Waring's problem: some refinements. *Proc. Lond. math. Soc.* **63**, 35–68.

Vaughan, R. C. & Wooley, T. D. 1993*a* Further improvements in Waring's problem. (Submitted.)

Vaughan, R. C. & Wooley, T. D. 1993*b* Further improvements in Waring's problem. II. Sixth powers. (Submitted.)

Vaughan, R. C. & Wooley, T. D. 1993*c* Further improvements in Waring's problem. IV. Higher powers. (In preparation.)

Vinogradov, I. M. 1984 *Selected works*. (Translated from the Russian by N. Psv.) Berlin: Springer-Verlag.

Wooley, T. D. 1992*a* Large improvements in Waring's problem. *Ann. Math.* **135**, 131–164.

Wooley, T. D. 1992*b* On Vinogradov's mean value theorem. *Mathematika* **39**, 379–399.

Wooley, T. D. 1993*a* Quasi-diagonal behaviour in certain mean value theorems of additive number theory. (Submitted.)

Wooley, T. D. 1993*b* The application of a new mean value theorem to the fractional parts of polynomials. *Acta Arithmetica*. (In the press.)