ON VINOGRADOV'S MEAN VALUE THEOREM, II

Trevor D. Wooley

1. Introduction

The main purpose of this note is to provide an improvement of Vinogradov's mean value theorem which may be of use in multiplicative number theory. Let $J_{s,k}(P)$ denote the number of solutions of the simultaneous diophantine equations

$$\sum_{i=1}^{s}(x_i^j - y_i^j) = 0 \quad (1 \le j \le k) \tag{1}$$

with $1 \le x_i, y_i \le P$ for $1 \le i \le s$. On writing

$$f(\boldsymbol{\alpha}; Q) = \sum_{x \le Q} e(\alpha_1 x + \alpha_2 x^2 + \dots + \alpha_k x^k), \tag{2}$$

in which $e(\alpha)$ denotes $e^{2\pi i\alpha}$, we observe that

$$J_{s,k}(P) = \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; P)|^{2s} d\boldsymbol{\alpha}, \tag{3}$$

where $\mathbb{T}^k$ denotes the k-dimensional unit cube, and $\boldsymbol{\alpha} = (\alpha_1, \dots, \alpha_k)$. Estimates for the mean value (3) were first investigated by Vinogradov, and are now known collectively as *Vinogradov's mean value theorem*. These estimates have found varied uses in both additive and multiplicative number theory.

Modern bounds for $J_{s,k}(P)$ take the form

$$J_{rk,k}(P) \le D(k,r)P^{2rk - \frac{1}{2}k(k+1) + \eta(r,k)} \quad (r \in \mathbb{N}), \tag{4}$$

where $D(k,r)$ is independent of P, and

$$\eta(r,k) = \tfrac{1}{2}k^2(1 - 1/k)^r. \tag{5}$$

The most general bound currently in the literature appears to be due to Stechkin [5], who showed that when $k \ge 2$ the bound (4) holds with (5) for each $P \in \mathbb{R}^+$ and $r \in \mathbb{N}$, with

$$D(k,r) = \exp(C \min\{r,k\} k^2 \log k) \tag{6}$$

and C an absolute constant. The explicit nature of the constant (6) is of importance when it comes to obtaining zero-free regions for the Riemann zeta function (see, for example, Walfisz [8]). It has since been shown that the permissible choice for $\eta(r,k)$ may be reduced provided that we are willing to accept a larger value for $D(k,r)$ (Turina [6] has obtained improvements effective for small r, and Wooley [9] for a large range of r).

In this note we will reduce the permissible size of $D(k,r)$ for a range of P of use in estimating the zero-free region for the Riemann zeta function.

Research supported in part by NSF grant DMS-8610730 at the Institute for Advanced Study.
Michigan Math. J. 40 (1993), 175-180

Theorem. *Let k and r be integers with $k \geq 2$ and $1 \leq r \leq k^2$. Then there exist absolute constants C_1 and C_2 such that for each*

$$P \geq \exp(C_1 k(1-1/k)^{-r} \log k), \tag{7}$$

we have the bound (4) *with* (5), *where*

$$D(k,r) = \exp(C_2 rk \log k). \tag{8}$$

In some limited sense, the expression for $D(k,r)$ is close to the best which one might hope to achieve. For by considering diagonal solutions of (1), and permutations thereof, we have for each $P \geq (rk)^2$ that $J_{rk,k}(P) \gg (rk)![P]^{rk} \gg D^*(k,r)P^{rk}$, with $D^*(k,r) = \exp(rk \log k)$. So $D(k,r)$ is a fixed power of $D^*(k,r)$. Unfortunately, of course, our theorem contains a condition on the size of P.

We note that in applications to the zero-free region of the Riemann zeta function, estimates of the above form are of importance with $r \leq C_3 k$ (with C_3 some absolute constant). In such circumstances, for some absolute constants A and B, we may replace (7) by $P \geq k^{Ak}$, and (8) by $D(k,r) = k^{Brk}$.

The new ingredient in our proof is very simple, and has also been used by the author in previous work on Vinogradov's mean value theorem (see Wooley [9]). Put in the simplest terms, we note only that if $d > n \geq 0$ and $d|n$ then $n = 0$. This enables us to show that a diophantine equation having some singularity in sufficiently many p-adic fields must also have a singularity in the real field. It is this transition from local to global singularities which appears to provide such an effective handle on such problems. The skeleton of the proof is otherwise based on Section 5.1 of Vaughan [7].

The author thanks Professors A. Ghosh, D. A. Goldston, and R. C. Vaughan for useful comments. This work was supported in part by a Science and Engineering Research Council Research Studentship, and completed while the author was in receipt of NSF grant number DMS-8610730.

2. The proof of the theorem

We shall require two preliminary lemmata. The first is a well-known lemma on congruences (see Linnik [4, Lemma 1]), a very short proof of which may be found in Vaughan [7, Lemma 5.1].

Lemma 1. *Suppose that p is a prime number with $p > k$. Let S denote the number of solutions of the simultaneous congruences*

$$\sum_{r=1}^{k} x_r^j \equiv h_j \pmod{p^j} \quad (1 \leq j \leq k)$$

with $x_r \leq p^k$ and the x_r distinct (mod p). *Then $S \leq k!p^{k(k-1)/2}$.*

The second lemma we require is a result on the density of prime numbers in short intervals.

Lemma 2. *There exist positive real numbers R and $c = c(R)$ such that if $\theta > 1-1/R > 0$ and $x \geq x(\theta)$, then*

$$\pi(x) - \pi(x-y) > \frac{cy}{\log x} \tag{9}$$

for $x^\theta \leq y \leq x/2$. (Here $\pi(x)$ denotes the number of primes less than or equal to x).

A result of this form was first proved by Hoheisel [2], who showed that $R = 33000$ is permissible. A key ingredient of the proof is Littlewood's zero-free region for the Riemann zeta function. Stronger results are now known (an interesting survey on results of this type is given in Heath-Brown [1]). We note that by assuming no more than the prime number theorem (taking $\theta = 1$), it is a simple matter to modify the proof we give so as to obtain the theorem with $D(k,r) = \exp(C_2 rk^2 \log k)$, unconditionally with respect to P. This in itself is a simplification of the arguments of Karatsuba [3] and Stechkin [5], in particular making the treatment of singular solutions almost trivial.

We prove the theorem by induction on r. First note that by using Newton's formulae on the roots of polynomials, we have $J_{k,k}(X) \leq k!X^k$ for each $X \in \mathbb{R}$. Thus the theorem follows in the case $r = 1$. Next we take $R \geq 2$ and c to be real numbers for which (9) holds. Then we may take $D \geq 1$ to be an absolute constant so large that whenever $x > D$ we have $cx > 4R \log 2x$ and $\pi(x + x^{1-1/R}) - \pi(x) > cx^{1-1/R}/\log 2x$. We assume that $k > 1$, $r > 1$, and write $s = rk$.

Suppose that the theorem holds for each $r' < r$, and that $X \geq X_0$ with $X_0 = \exp(4Rk(1-1/k)^{-r}\log Dk)$. Write $M = X^{1/k}$, and let $\mathcal{P}$ denote the set consisting of the k^3 smallest primes exceeding M. Then by our choice of D we have

$$\pi(M + M^{1-1/R}) - \pi(M) > \frac{c(Dk)^4}{4R\log(2Dk)} > k^3,$$

and so each prime $p \in \mathcal{P}$ satisfies

$$M < p \leq M + M^{1-1/R}. \tag{10}$$

Let $R_1(\mathbf{h})$ denote the number of solutions of the simultaneous equations

$$\sum_{r=1}^{s} x_r^j = h_j \quad (1 \leq j \leq k) \tag{11}$$

with $0 < x_r \leq X$ and with $x_1, \ldots, x_k$ distinct, and let $R_2(\mathbf{h})$ denote the corresponding number of solutions with $x_1, \ldots, x_k$ not distinct. Then

$$J_{s,k}(X) = \sum_{\mathbf{h}} (R_1(\mathbf{h}) + R_2(\mathbf{h}))^2 \leq 2(S_1 + S_2),$$

where $S_i = \sum_{\mathbf{h}} R_i(\mathbf{h})^2$ $(i = 1, 2)$.

We divide into two cases.

(a) Suppose that $S_2 \geq S_1$. Then we have $J_{s,k}(X) \leq 4S_2$. Now $R_2(\mathbf{h})$ is at most $\binom{k}{2}$ times the number of solutions of the simultaneous equations (11) with $x_1 = x_2$. By considering the underlying diophantine equations, we therefore have

$$S_2 \leq k^4 \int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; X)^{2s-4} f(2\boldsymbol{\alpha}; X)^2| d\boldsymbol{\alpha}.$$

Then by Hölder's inequality,

$$S_2 \leq k^4 \left(\int_{\mathbb{T}^k} |f(\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \right)^{1-2/s} \left(\int_{\mathbb{T}^k} |f(2\boldsymbol{\alpha}; X)|^{2s} d\boldsymbol{\alpha} \right)^{1/s} \leq k^4 (J_{s,k}(X))^{1-1/s},$$

and the result now follows in the first case.

(b) Suppose that $S_1 \geq S_2$. Then we have $J_{s,k}(X) \leq 4S_1$. For a solution $\mathbf{x}$ counted by $R_1(\mathbf{h})$, let $\mathcal{I} = \prod_{1 \leq i < j \leq k} (x_i - x_j)$. Then we have $0 < |\mathcal{I}| \leq X^{k(k-1)/2}$. On noting (10) we find that the number, N^*, of prime divisors $p \in \mathcal{P}$ of $\mathcal{I}$ is at most $\frac{1}{2}k^2(k-1)$. Then $\mathrm{card}(\mathcal{P}) > N^*$, and hence there is a $p \in \mathcal{P}$ with $p \nmid \mathcal{I}$, so that $x_1, \ldots, x_k$ are distinct $\pmod p$. Then $R_1(\mathbf{h}) \leq \sum_{p \in \mathcal{P}} R_3(\mathbf{h}, p)$, where $R_3(\mathbf{h}, p)$ denotes the number of solutions of the equations (11) with $0 < x_r \leq X$ and with $x_1, \ldots, x_k$ distinct $\pmod p$. (The right-hand side of this last inequality counts too many solutions, but does not explicitly depend on a fixed prime p.)

Let $I_1(p) = \sum_{\mathbf{h}} R_3(\mathbf{h}, p)^2$. Then $I_1(p)$ is the number of solutions of the simultaneous equations (1) with $0 < x_r, y_r \leq X$, with $x_1, \ldots, x_k$ distinct $\pmod p$, and likewise $y_1, \ldots, y_k$. Further, in this case we have

$$J_{s,k}(X) \leq 4(\mathrm{card}\mathcal{P})^2 \max_{p \in \mathcal{P}} I_1(p). \tag{12}$$

For a fixed prime p, let

$$f(\boldsymbol{\alpha}, y) = \sum_{\substack{0 < x \leq X \\ x \equiv y \pmod p}} e(\alpha_1 x + \cdots + \alpha_k x^k),$$

and let $\mathcal{A}$ denote the set of $k-$tuples $\mathbf{a} = (a_1, \ldots, a_k)$ with $0 < a_r \leq p$ and the a_r distinct. Then by considering the underlying diophantine equations, we have

$$I_1(p) = \int_{\mathbb{T}^k} \left| \sum_{0 \leq x < p} f(\boldsymbol{\alpha}, x) \right|^{2s-2k} \left| \sum_{\mathbf{a} \in \mathcal{A}} f(\boldsymbol{\alpha}, a_1) \ldots f(\boldsymbol{\alpha}, a_k) \right|^2 d\boldsymbol{\alpha}.$$

By Hölder's inequality, we deduce that

$$\left|\sum_{0\le x<p} f(\boldsymbol{\alpha},x)\right|^{2s-2k} \le p^{2s-2k-1}\sum_{0\le x<p}|f(\boldsymbol{\alpha},x)|^{2s-2k},$$

and hence $I_1(p) \le p^{2s-2k}\max_{0\le x<p} I_2(x,p)$, where $I_2(x,p)$ denotes the number of solutions of the simultaneous equations

$$\sum_{i=1}^{k}(m_i^j-n_i^j)=\sum_{r=1}^{s-k}((py_r+x)^j-(pz_r+x)^j)\quad (1\le j\le k)$$

with $0<m_i,n_i\le X$, $-x/p<y_r,z_r\le (X-x)/p$, the m_i distinct $\pmod p$, and likewise the n_i. An application of the binomial theorem shows that $I_2(x,p)$ is the number of solutions of the simultaneous equations

$$\sum_{i=1}^{k}((m_i-x)^j-(n_i-x)^j)=\sum_{r=1}^{s-k}p^j(y_r^j-z_r^j)\quad (1\le j\le k), \tag{13}$$

under the same conditions.

We have $p^k>X$ and $p>k$, so by applying Lemma 1 to the congruences implicit in (13) we have

$$I_2(x,p)\le X^k k! p^{\frac12 k(k-1)}\max_{\mathbf{h}} J_{s-k,k}(X/p,-x/p,\mathbf{h}),$$

where $J_{s,k}(X,Y,\mathbf{h})$ denotes the number of solutions to the simultaneous equations

$$\sum_{i=1}^{s}(x_i^j-y_i^j)=h_j\quad (1\le j\le k)$$

with $Y<x_i,y_i\le Y+X$ $(1\le i\le s)$. But by appealing to the integral representation of the form (3) and using the binomial theorem, we deduce that $J_{s-k,k}(X/p,-x/p,\mathbf{h})\le J_{s-k,k}(1+X/p)$, and hence that

$$I_2(x,p)\le X^k k! p^{\frac12 k(k-1)} J_{s-k,k}(1+X/p). \tag{14}$$

Then by (10), (12), and (14) we have

$$J_{s,k}(X)\le 4k^6 k!(M+M^{1-1/R})^{2s+\frac12 k(k-5)}X^k J_{s-k,k}(1+X/M).$$

On recalling our choice of X_0, we have

$$(1+M^{-1/R})^{2s+\frac12 k(k-5)}(1+M/X)^{2s}<(1+(Dk)^{-3})^{8k^3}<\exp(8D^{-3}).$$

Then on the inductive hypothesis, we have

$$J_{s,k}(X)\le D'D(k,r-1)\exp(6\log k+k\log k)X^{2rk-\frac12 k(k+1)+\eta(r,k)},$$

where D' is a sufficiently large (but fixed) absolute constant. The inductive hypothesis then follows with r replacing $r-1$, on using the definition of $D(k,r)$.

This completes the proof of the theorem.

References

1. D. R. Heath-Brown, *Differences between consecutive primes*, Jahresber. Deutsch Math.-Verein. **90** (1988), 71–89.
2. G. Hoheisel, *Primzahlprobleme in der Analysis*, Sitzungsber. Preß. Akad. Wiss. Phys.-Math. Kl. (1930), 580–588.
3. A. A. Karatsuba, *The mean value of the modulus of a trigonometric sum*, Izv. Akad. Nauk SSSR Ser. Mat. **37** (1973), 1203–1227.
4. Ju. V. Linnik, *On Weyl's sums*, Mat. Sb. (Rec. Math.) **12** (1943), 28–39.
5. S. B. Stechkin, *On mean values of the modulus of a trigonometric sum*, Trudy Mat. Inst. Steklov. **134** (1975), 283–309. (Russian)
6. O. V. Turina, *A new estimate for a trigonometric integral of I. M. Vinogradov*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 2; translation in Math. USSR-Izv. **30** (1988), 337–351.
7. R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge Univ. Press, Cambridge, 1981.
8. A. Z. Walfisz, *Weylsche Exponentialsummen in der neueren Zahlentheorie*, Deutscher Verlag der Wissenschaften, Berlin, 1963.
9. T. D. Wooley, *On Vinogradov's mean value theorem*, Mathematika **39** (1992), 379–399.

Department of Mathematics, University of Michigan, Ann Arbor, MI48109-1003
E-mail address: `wooley@math.lsa.umich.edu`