Mathematika 64 (2018) 430–444 © 2018 University College London
doi:10.1112/S0025579318000025

SOLUTIONS TO DIAGONAL CONGRUENCES WITH VARIABLES RESTRICTED TO A BOX

TODD COCHRANE, MISTY OSTERGAARD AND CRAIG SPENCER

Abstract. We prove that for any positive integers k, n with $n > \frac{3}{2}(k^2+k+2)$, prime p, and integers c, a_i, with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution $\underline{x}$ to the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{p}$$

with $1 \leqslant x_i \ll_k p^{1/k}$, $1 \leqslant i \leqslant n$. This upper bound is best possible. Refinements are given for smaller n, and for variables restricted to intervals in more general position. In particular, for any $\varepsilon > 0$ we give an explicit constant c_ε such that if $n > c_\varepsilon k$, then there is a solution with $1 \leqslant x_i \ll_{\varepsilon,k} p^{1/k+\varepsilon}$.

§1. *Introduction.* Let p, n, k be positive integers with p a prime, a_i be integers where $p \nmid a_i$, $1 \leqslant i \leqslant n$, and c be any integer. Our interest here is in obtaining small solutions to the diagonal congruence

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_n x_n^k \equiv c \pmod{p}. \tag{1.1}$$

In general, the best one can hope for is a solution with all $|x_i| \ll p^{1/k}$; consider for example the congruence $x_1^k + \cdots + x_n^k \equiv (p-1)/2 \pmod{p}$. The best results available until now yield solutions with $|x_i| \ll_{k,\varepsilon} p^{1/k+\delta_k(n)+\varepsilon}$, for some positive constant $\delta_k(n)$ satisfying $\delta_k(n) \to 0$ as $n \to \infty$. Here we obtain the best possible result for arbitrary k, with a relatively small number of variables.

THEOREM 1.1. *For any positive integer k, positive integer $n \geqslant \frac{3}{2}(k^2+k+2)$, prime p, and integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution of (1.1) with $1 \leqslant x_i \ll_k p^{1/k}$, $1 \leqslant i \leqslant n$.*

In fact, for $n \geqslant \frac{3}{2}(k^2+k+2)$ we obtain the existence of a solution of (1.1) in any cube of the type

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : c_i + 1 \leqslant x_i \leqslant c_i + B, 1 \leqslant i \leqslant n\}, \tag{1.2}$$

$B, c_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$, $1 \leqslant B \leqslant p$, provided that $B \gg_k p^{1/k}$ and that for at least $\frac{1}{2}(k^2+k+2)$ choices of i, we have $c_i \ll_k 1$; see Remark 8.1. The constraint $n \geqslant \frac{3}{2}(k^2+k+2)$ in the theorem is certainly not best possible. In fact, it is

Received 2 June 2017, published online 3 April 2018.
MSC (2010): 11L07, 11L03 (primary).

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

reasonable to believe that the conclusion of the theorem holds for $n \geqslant Ck$, for some absolute constant C.

With fewer variables we obtain a slightly larger solution.

THEOREM 1.2. *For any positive real $\varepsilon < 1$, positive integers k, n with $n > \frac{3}{2}k\log(3e/\varepsilon) + 3$, prime p, and integers c, a_i, $1 \leqslant i \leqslant n$ with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there is a solution of (1.1) with $1 \leqslant x_i \ll_{\varepsilon,k} p^{1/k+\varepsilon}$, $1 \leqslant i \leqslant n$.*

Another problem of interest is to minimize the number of variables required to break the $\sqrt{p}$ threshold for the size of a solution. The square-root threshold is the natural one that arises when one tries to attack the problem by completing exponential sums over restricted intervals.

COROLLARY 1.1. *For $k \geqslant 2$, $n \geqslant 5k+3$, and any c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution of (1.1) with $1 \leqslant x_i \ll_k \sqrt{p}$, $1 \leqslant i \leqslant n$.*

§2. *Comparison with known results.* The problem of obtaining small solutions to diagonal congruences of the type (1.1) has received much attention over the years including the work of Schmidt [**11**–**13**], Baker [**1**, **2**], Dietmann [**8**], Cochrane [**5**] and Cochrane and Zheng [**7**]. Their results are summarized in the introduction to the authors' first paper on this topic [**6**]. The results from [**6**] stated below in (2.1), (2.2), and (2.3) are the best available estimates (prior to the current work) for the problem at hand.

In [**6**], the authors proved that for $k \geqslant 2$, $\varepsilon > 0$, and integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a non-zero solution $\underline{x}$ to (1.1) with

$$1 \leqslant x_i \ll_{k,\varepsilon} \begin{cases} p^{k(\log k+\gamma\log\log 2k)/n+\varepsilon} & \text{if } n \leqslant k(k-1)(\log k+\gamma\log\log 2k), \\ p^{1/(k-1)} & \text{if } k(k-1)(\log k+\gamma\log\log 2k) \\ & \quad < n \leqslant k(k-1)^2, \\ p^{1/k+(k-1)/n+\varepsilon} & \text{if } n > k(k-1)^2, \end{cases} \tag{2.1}$$

for $1 \leqslant i \leqslant n$. Here, γ is the implicit constant appearing in [**16**, Theorem 1.1]. Theorem 1.2 improves on this result for $n < \frac{3}{2}(k^2+k+2)$ and Theorem 1.1 improves on it for all larger values of n.

Also in [**6**], the authors established that for $k \geqslant 2$, $\varepsilon > 0$, and integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution $\underline{x}$ to (1.1) in an arbitrary cube $\mathcal{B}$ of side length B provided that

$$B \gg_{k,\varepsilon} \begin{cases} p^{k(k-1)/n+\varepsilon} & \text{if } n \leqslant k(k-1)^2, \\ p^{1/k+(k-1)/n+\varepsilon} & \text{if } n > k(k-1)^2, \end{cases} \tag{2.2}$$

and that for $2 \leqslant k \leqslant 5$, the inequalities in (2.2) may be improved to

$$B \gg_{k,\varepsilon} \begin{cases} p^{2^{k-1}/n+\varepsilon} & \text{if } n \leqslant 2^{k-1}(k-1), \\ p^{1/k+2^{k-1}/(nk)+\varepsilon} & \text{if } n > 2^{k-1}(k-1). \end{cases} \tag{2.3}$$

For $n \geqslant \frac{3}{2}(k^2+k+2)$, Theorem 1.1 improves on (2.2) and (2.3) for cubes to which it applies.

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

§3. *A general upper bound on the number of solutions of (1.1).* The objective of the next few sections is to establish a sharp upper bound on the number of solutions to a diagonal congruence of the type (1.1), with variables restricted to a cube $\mathcal{B}$ of the type (1.2). In fact our proof holds identically for a general modulus q and so we state it as such. In this case, we restrict our attention to congruences of the type

$$\sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{q} \tag{3.1}$$

with the a_i integers relatively prime to q. Let $N_q(\mathcal{B})$ denote the number of solutions of (3.1) with $\underline{x} \in \mathcal{B}$.

THEOREM 3.1. *Let q, n, k be positive integers with $n \geqslant k^2+k+2$, $\mathcal{B}$ be any cube of edge length $B \leqslant q$ as in (1.2), a_i be integers with $(a_i, q) = 1$, $1 \leqslant i \leqslant n$, and $c \in \mathbb{Z}$. Then*

$$N_q(\mathcal{B}) \ll_k \frac{B^n}{q} + B^{n-k}. \tag{3.2}$$

An explicit value for the constant in (3.2) is given in (6.1). Aside from the determination of this constant the upper bound is best possible. Indeed, as c runs from 0 to $q-1$, the average number of solutions of the congruence (3.1) with $\underline{x} \in \mathcal{B}$, is B^n/q. On the other hand, if $\sum_{i=1}^n |a_i|$ is fixed, and c is allowed to run from $-B^k \sum_{i=1}^n |a_i|$ to $B^k \sum_{i=1}^n |a_i|$, then the average number of solutions of the equation $\sum_{i=1}^n a_i x_i^k = c$ with $1 \leqslant x_i \leqslant B$ is of order B^{n-k}. Thus for a cube of the type $1 \leqslant x_i \leqslant B$, one can do no better than B^n/q for large B ($B > q^{1/k}$), and no better than B^{n-k} for small B, ($B < q^{1/k}$).

Theorem 3.1 yields the upper bound $N_q(\mathcal{B}) \ll_k |\mathcal{B}|/q$ for $B \gg_k q^{1/k}$. In comparison, for the case of prime moduli p, standard estimates for exponential sums over the algebraic set $\sum_{i=1}^n a_i x_i^k = c$ in $\mathbb{Z}_p$, yield the asymptotic formula [**5**, Example 4.4.19],

$$N_p(\mathcal{B}) = \frac{B^n}{p} + O_{n,k}(p^{(n-1)/2}(\log p)^n), \tag{3.3}$$

for any k, n, and $p \nmid a_1 \cdots a_n c$. This estimate, when it applies, improves on the constant in the main term of (3.2) for $B \gg_{n,k} p^{1/2+1/2n} \log p$. However, estimates of this kind fall short of breaking the $\sqrt{p}$ barrier for a solution of (1.1), no matter how many variables are used.

The upper bound in (3.2) can be generalized to a rectangular box with edges of different lengths as follows. For any positive integers k, n, q with $n \geqslant \frac{1}{2}(k^2+k+2)$,

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : c_i + 1 \leqslant x_i \leqslant c_i + B_i, 1 \leqslant i \leqslant n\}, \tag{3.4}$$

$c_i, B_i \in \mathbb{Z}$, $1 \leqslant B_i \leqslant q$, and $(a_i, q) = 1$, $1 \leqslant i \leqslant n$,

$$N_q(\mathcal{B}) \ll_k \prod_{i=1}^{n} \left(\frac{B_i^n}{q} + B_i^{n-k} \right)^{1/n}.$$

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

We begin the proof of the theorem with the following lemma. Let $\mathbb{Z}_q$ denote the residue class ring modulo q and $e_q(\cdot) := e^{2\pi i(\cdot)/q}$, an additive character on $\mathbb{Z}_q$. For any subsets $S_1, \dots, S_n$ of $\mathbb{Z}_q$, put $\mathcal{S} = S_1 \times \cdots \times S_n$, and define

$$I_{n,k}(\mathcal{S}) := \#\left\{(\underline{x}, \underline{y}) \in \mathcal{S} \times \mathcal{S} : \sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod q\right\}. \tag{3.5}$$

LEMMA 3.1. *Let q, n, k be positive integers, $S_1, \dots, S_{2n}$ be subsets of $\mathbb{Z}_q$, and $\mathcal{T} = S_1 \times \cdots \times S_{2n}$. For any integers c, a_i, $1 \leqslant i \leqslant 2n$, with $(a_i, q) = 1$, $1 \leqslant i \leqslant 2n$, we have*

$$\#\left\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} a_i x_i^k \equiv c \pmod q\right\} \leqslant \prod_{i=1}^{2n} I_{n,k}(\mathcal{S}_i^n)^{1/2n},$$

where S_i^n is the cartesian product of S_i with itself n times.

Proof. We have

$$\begin{aligned}
\#\left\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} a_i x_i^k \equiv c \pmod q\right\} &= \frac{1}{q} \sum_{\underline{x} \in \mathcal{T}} \sum_{\lambda=1}^{q} e_q\left(\lambda\left(\sum_{i=1}^{2n} a_i x_i^k - c\right)\right) \\
&\leqslant \frac{1}{q} \sum_{\lambda=1}^{q} \left| e_q(-\lambda c) \prod_{i=1}^{2n} \sum_{x_i \in S_i} e_q(\lambda a_i x_i^k) \right| \\
&\leqslant \frac{1}{q} \left[\sum_{\lambda=1}^{q} \left| \sum_{x_1 \in S_1} e_q(\lambda a_1 x_1^k) \right|^{2n}\right]^{1/2n} \\
&\quad \cdots \left[\sum_{\lambda=1}^{q} \left| \sum_{x_{2n} \in S_{2n}} e_q(\lambda a_{2n} x_{2n}^k) \right|^{2n}\right]^{1/2n},
\end{aligned}$$

by Hölder's inequality. Now, for $1 \leqslant i \leqslant n$, the sum

$$\sum_{\lambda=1}^{q} \left| \sum_{x_i \in S_i} e_q(\lambda a_i x_i^k) \right|^{2n}$$

is q times the number of solutions of the congruence

$$a_i(x_1^k + \cdots + x_n^k) \equiv a_i(y_1^k + \cdots + y_n^k) \pmod q,$$

with variables restricted to S_i. Since $(a_i, q) = 1$ this is just $q\, I_{n,k}(S_i^n)$. Therefore,

$$\begin{aligned}
\#\left\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} a_i x_i^k \equiv c \pmod q\right\} &\leqslant \frac{1}{q} \prod_{i=1}^{2n} (q\, I_{n,k}(S_i^n))^{1/2n} \\
&= \prod_{i=1}^{2n} I_{n,k}(S_i^n)^{1/2n}. \qquad \square
\end{aligned}$$

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

§4. *Relating $I_{n,k}(\mathcal{B})$ to $J_{n,k}(B)$ and $J^*_{n,k}(B)$.* In this section we obtain an estimate for $I_{n,k}(\mathcal{B})$, the number of solutions of

$$\sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod{q}, \tag{4.1}$$

with $\underline{x}$, $\underline{y}$ in a cube of the type

$$\mathcal{B} = \mathcal{B}(c, B) := \{\underline{x} \in \mathbb{Z}^n : c+1 \leqslant x_i \leqslant c+B,\ 1 \leqslant i \leqslant n\}, \tag{4.2}$$

by first relating it to the number of solutions $J_{n,k}(B)$ to the system of congruences

$$\begin{aligned} x_1 + \cdots + x_n &\equiv y_1 + \cdots + y_n \pmod{q}, \\ x_1^2 + \cdots + x_n^2 &\equiv y_1^2 + \cdots + y_n^2 \pmod{q}, \\ &\vdots \\ x_1^k + \cdots + x_n^k &\equiv y_1^k + \cdots + y_n^k \pmod{q} \end{aligned} \tag{4.3}$$

with $1 \leqslant x_i, y_i \leqslant B$, $1 \leqslant i \leqslant n$, and then relating it to the number of solutions of the corresponding system of equations (4.7).

LEMMA 4.1. *For any positive integers B, n, k, q with $B \leqslant q$, integer c, and cube $\mathcal{B}(c, B)$ as in (4.2) we have*

$$I_{n,k}(\mathcal{B}) \leqslant (2n)^{k-1} B^{k(k-1)/2} J_{n,k}(B). \tag{4.4}$$

Moreover, if for some j with $1 \leqslant j < k$ we have $n(B^{j-1} - 1) < (q-1)/2 \leqslant n(B^j - 1)$, then

$$I_{n,k}(\mathcal{B}) \leqslant (2n)^{j-1} B^{j(j-1)/2} q^{k-j} J_{n,k}(B). \tag{4.5}$$

Proof. First we observe that for any integers h_i, $1 \leqslant i \leqslant k-1$, the number $N(h_1, \ldots, h_{k-1})$ of integer solutions of the system

$$\begin{aligned} (x_1 - c) + \cdots + (x_n - c) &\equiv (y_1 - c) + \cdots \\ &\quad + (y_n - c) + h_1 \pmod{q} \\ &\vdots \\ (x_1 - c)^{k-1} + \cdots + (x_n - c)^{k-1} &\equiv (y_1 - c)^{k-1} + \cdots \\ &\quad + (y_n - c)^{k-1} + h_{k-1} \pmod{q} \\ x_1^k + \cdots + x_n^k &\equiv y_1^k + \cdots + y_n^k \pmod{q} \end{aligned} \tag{4.6}$$

with $c+1 \leqslant x_i, y_i \leqslant c+B$, is less than or equal to the number of solutions with all $h_i = 0$. This follows by applying the triangle inequality to the exponential sum representation for the number of solutions of the system,

$$\frac{1}{q^k} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} e_q(-\lambda_1 h_1 - \cdots - \lambda_{k-1} h_{k-1}) \sum_{\underline{x} \in \mathcal{B}} \sum_{\underline{y} \in \mathcal{B}}$$
$$e_q\left[\lambda_k \left(\sum_{i=1}^{n} x_i^k - \sum_{i=1}^{n} y_i^k\right) + \sum_{j=1}^{k-1} \lambda_j \left(\sum_{i=1}^{n} (x_i - c)^j - \sum_{i=1}^{n} (y_i - c)^j\right)\right].$$

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

But with all $h_i = 0$ the system of congruences above is equivalent to the defining system (4.3) for $J_{n,k}(B)$, and this system is invariant under the translation $x_i \to x_i + c$, $y_i \to y_i + c$. Thus we have $N(h_1, \dots, h_{k-1}) \leqslant J_{n,k}(B)$ uniformly. Also, any solution of the diagonal congruence (4.1) with $\underline{x}, \underline{y} \in \mathcal{B}$, is a solution of a system of the type (4.6) for some h_i satisfying $|h_i| \leqslant n(B^i - 1)$, $1 \leqslant i \leqslant k-1$. Thus we obtain

$$\begin{aligned} I_{n,k}(\mathcal{B}) &= \sum_{|h_1| \leqslant n(B-1)} \cdots \sum_{|h_{k-1}| \leqslant n(B^{k-1}-1)} N(h_1, \dots, h_{k-1}) \\ &\leqslant J_{n,k}(B) \prod_{i=1}^{k-1} (2n(B^i - 1) + 1), \end{aligned}$$

yielding the inequality in (4.4).

Suppose now that for some j with $1 \leqslant j < k$ we have $n(B^{j-1} - 1) < (q-1)/2 \leqslant n(B^j - 1)$. Then the upper bound can be improved by simply allowing $h_j, \dots, h_{k-1}$ to each run through a complete residue system modulo q. In this case, we see that there are at most $(2n)^{j-1} B^{1+2+\cdots+(j-1)} q^{k-j}$ choices for the h_i, yielding the second inequality in the lemma. □

Next we relate $J_{n,k}(B)$ to $J^*_{n,k}(B)$, the number of integer solutions to the system of equations

$$\begin{aligned} x_1 + \cdots + x_n &= y_1 + \cdots + y_n, \\ x_1^2 + \cdots + x_n^2 &= y_1^2 + \cdots + y_n^2, \\ &\vdots \\ x_1^k + \cdots + x_n^k &= y_1^k + \cdots + y_n^k, \end{aligned} \tag{4.7}$$

with $1 \leqslant x_i, y_i \leqslant B$, $1 \leqslant i \leqslant n$.

LEMMA 4.2. *Let B, k, n, q be positive integers with $1 \leqslant B \leqslant q$.*

(i) *If $n(B^k - 1) < q$ then $J_{n,k}(B) = J^*_{n,k}(B)$.*

(ii) *If $n(B^{k-1} - 1) < (q-1)/2 \leqslant n(B^k - 1)$ then*

$$J_{n,k}(B) \leqslant (2nB^k/q + 1) J^*_{n,k}(B).$$

(iii) *If for some j with $1 \leqslant j \leqslant k-1$ we have $n(B^{j-1} - 1) < (q-1)/2 \leqslant n(B^j - 1)$, then*

$$J_{n,k}(B) < 5(2n/q)^{k-j+1} B^{k(k+1)/2 - j(j-1)/2} J^*_{n,k}(B).$$

Proof. Any solution of (4.3) with $1 \leqslant x_i, y_i \leqslant B$, $1 \leqslant i \leqslant n$, satisfies a system of equations of the form

$$\begin{aligned} x_1 + \cdots + x_n &= y_1 + \cdots + y_n + l_1 q, \\ x_1^2 + \cdots + x_n^2 &= y_1^2 + \cdots + y_n^2 + l_2 q, \\ &\vdots \\ x_1^k + \cdots + x_n^k &= y_1^k + \cdots + y_n^k + l_k q \end{aligned} \tag{4.8}$$

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

for some integers l_i with $|l_i| \leqslant n/q(B^i - 1)$, $1 \leqslant i \leqslant k$. For fixed l_i the number of solutions of (4.8) with $1 \leqslant x_i, y_i \leqslant B$ is at most $J^*_{n,k}(B)$, as one can see by applying the triangle inequality to the integral representation for the number of solutions.

If $n(B^k - 1) < q$, then for $1 \leqslant i \leqslant k$ we have $(n/q)(B^i - 1) < 1$ and so there is only one choice for l_i, namely $l_i = 0$. Thus $J_{n,k}(B) = J^*_{n,k}(B)$, completing the proof of part (i). If for some j with $1 \leqslant j \leqslant k$ we have $n(B^{j-1} - 1) < (q-1)/2 \leqslant n(B^j - 1)$, then for $1 \leqslant i \leqslant j-1$, we again have $l_i = 0$. Thus

$$J_{n,k}(B) \leqslant J^*_{n,k}(B) \prod_{i=j}^{k} \left(2\left\lfloor \frac{n}{q}(B^i - 1)\right\rfloor + 1\right) \leqslant J^*_{n,k}(B) \prod_{i=j}^{k} \left(2\frac{n}{q}B^i + 1\right).$$

If $j = k$ this is the inequality in (ii). Suppose now that $j \leqslant k-1$. Then,

$$J_{n,k}(B) \leqslant J^*_{n,k}(B) B^{j+(j+1)+\cdots+k} \left(\frac{2n}{q}\right)^{k-j+1} \prod_{i=j}^{k} \left(1 + \frac{q/2n}{B^i}\right).$$

Using $(q-1)/2 \leqslant n(B^j - 1)$, whence $q/2n < B^j$, we see that (since $B \geqslant 2$),

$$\prod_{i=j}^{k} \left(1 + \frac{q/2n}{B^i}\right) < \prod_{i=j}^{k} \left(1 + \frac{1}{B^{i-j}}\right) \leqslant \prod_{i=j}^{\infty} \left(1 + \frac{1}{2^{i-j}}\right) < 4.77,$$

completing the proof of part (iii). □

Putting together the results of Lemmas 4.1 and 4.2, we obtain a uniform upper bound for $I_{n,k}(\mathcal{B})$ in terms of $J^*_{n,k}(B)$.

LEMMA 4.3. *For any integer c, positive integers B, k, n, q with $1 \leqslant B \leqslant q$, and cube $\mathcal{B} = \mathcal{B}(c, B)$ as in (4.2) we have*

$$I_{n,k}(\mathcal{B}) \leqslant 5(2n)^k B^{\frac{1}{2}k(k-1)} \left(\frac{B^k}{q} + \frac{1}{2n}\right) J^*_{n,k}(B).$$

§5. *Estimation of $J^*_{n,k}(B)$.* The task of estimating $J^*_{n,k}(B)$ has been a central problem in additive number theory since Vinogradov's seminal work [**15**] on Waring's problem. Recall that a non-negative real number $\Delta^*_{n,k}$ is called an admissible exponent for the system (4.7) if

$$J^*_{n,k}(B) \leqslant c_1(n,k) B^{2n - \frac{1}{2}k(k+1) + \Delta^*_{n,k}} \tag{5.1}$$

for some constant $c_1(n,k)$. Wooley [**17**, Theorems 1.1, 1.2] established that for $k \geqslant 2$ and $n \geqslant k(k+1)$ one can take $\Delta^*_{n,k} = \varepsilon$ for any $\varepsilon > 0$, and that for $k \geqslant 3$ and $n \geqslant k^2 + k + 1$ one can take $\Delta^*_{n,k} = 0$. He [**18**, Theorem 1.1] then obtained $\Delta^*_{n,k} = \varepsilon$ for $k \geqslant 3$, $n \geqslant k^2 - 1$, and any $\varepsilon > 0$. Recently, Bourgain, Demeter,

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

and Guth [3] established that for $k \geqslant 2$, one can take $\Delta^*_{n,k} = \varepsilon$ for $n \geqslant \frac{1}{2}k(k+1)$ and $\Delta^*_{n,k} = 0$ for $n > \frac{1}{2}k(k+1)$. In fact, for $n > \frac{1}{2}k(k+1)$, it follows from the work of [3] that one has the asymptotic formula

$$J^*_{n,k}(B) \sim c(n,k)B^{2n-(1/2)k(k+1)}, \tag{5.2}$$

where $c(n,k)$ is a constant given by

$$c(n,k) = \mathfrak{S}(n,k)\mathfrak{J}(n,k), \tag{5.3}$$

with

$$\mathfrak{S}(n,k) := \sum_{q=1}^{\infty} \sum_{\substack{\lambda_1=1 \\ (\lambda_1,\dots,\lambda_k,q)=1}}^{q} \cdots \sum_{\lambda_k=1}^{q} \left| q^{-1} \sum_{x=1}^{q} e_q(\lambda_1 x + \cdots + \lambda_k x^k) \right|^{2n},$$

and

$$\mathfrak{J}(n,k) := \int_{\mathbb{R}^k} \left| \int_0^1 e(\beta_1 x + \cdots + \beta_k x^k)\, dx \right|^{2n} d\underline{\beta}.$$

For B sufficiently large, it follows in this case that the constant in (5.1) can be taken to be $c(n,k) + \varepsilon$, for any $\varepsilon > 0$. Using the result of [3] we obtain from Lemma 4.3 the following upper bound on $I_{n,k}(\mathcal{B})$.

PROPOSITION 5.1. *For any positive integers n, k with $n > \frac{1}{2}k(k+1)$ and cube $\mathcal{B}$ as in (4.2), we have*

$$I_{n,k}(\mathcal{B}) \leqslant 5c_1(n,k)(2n)^k \left(\frac{B^{2n}}{q} + \frac{1}{2n} B^{2n-k} \right), \tag{5.4}$$

where $c_1(n,k)$ is the constant appearing in (5.1) with $\Delta^*_{n,k} = 0$.

§6. *Proof of Theorem 3.1.*

Proof. We may assume that $n = k^2 + k + 2$, by setting $n - (k^2 + k + 2)$ variables equal to arbitrary values in their specified intervals if $n > k^2 + k + 2$. Put $m = n/2$. For $1 \leqslant i \leqslant n$, let $S_i = \{x \in \mathbb{Z} : c_i + 1 \leqslant x \leqslant c_i + B\}$, and S_i^m be the cartesian product of S_i with itself m times, so that S_i^m is a cube of type (4.2). By Proposition 5.1, we have

$$I_{m,k}(S_i^m) \leqslant 5c_1(m,k)n^k \left(\frac{B^n}{q} + \frac{1}{n} B^{n-k} \right),$$

for each of the cubes S_i^m, and thus the theorem follows immediately from Lemma 3.1 (with n replaced by m). We observe that the constant in the upper bound of Theorem 3.1 may be taken to be

$$5c_1((k^2 + k + 2)/2, k)(k^2 + k + 2)^k. \tag{6.1}$$

□

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

Remark 6.1. Cilleruelo *et al* [**4**] employed a similar strategy to our proof of Theorem 3.1 for estimating the number of solutions of a congruence $f(x) \equiv y \pmod p$. Shparlinski and Zumalacárregui [**14**, (unpublished)] recently obtained a variation of Proposition 5.1. They also note that a non-trivial estimate of this kind is available with n slightly smaller than $\frac{1}{2}k(k+1)$, using $J^*_{n,k}(B) \ll B^{\varepsilon}(B^{2n-(1/2)k(k+1)} + B^n)$. However, for our purposes, this yields no benefits.

§7. *The value set of a diagonal form over a cube.* For any cube $\mathcal{B}$ as in (1.2), we define $S_{\mathcal{B}}$ to be the set of values the diagonal form $\sum_{i=1}^n a_i x_i^k$ takes on modulo q as $\underline{x}$ runs through $\mathcal{B}$,

$$S_{\mathcal{B}} := \Big\{ \sum_{i=1}^n a_i x_i^k \in \mathbb{Z}_q : \underline{x} \in \mathcal{B} \Big\}, \tag{7.1}$$

and put

$$N_{\mathcal{B}} := \#\Big\{ (\underline{x}, \underline{y}) \in \mathcal{B} \times \mathcal{B} : \sum_{i=1}^n a_i x_i^k \equiv \sum_{i=1}^n a_i y_i^k \pmod q \Big\}. \tag{7.2}$$

By Theorem 3.1, we have for $n \geqslant \frac{1}{2}(k^2+k+2)$ and $(a_i, q) = 1$, $1 \leqslant i \leqslant n$, that

$$N_{\mathcal{B}} \ll_k \frac{B^{2n}}{q} + B^{2n-k},$$

and thus using the elementary relationship $|S_{\mathcal{B}}| \geqslant B^{2n}/N_{\mathcal{B}}$, we deduce Lemma 7.1 as follows.

LEMMA 7.1. *For any positive integers k, n, B, q with $n \geqslant \frac{1}{2}(k^2+k+2)$, cube $\mathcal{B}$ as in (1.2) with $B \gg q^{1/k}$, and integers a_i with $(a_i, q) = 1$, $1 \leqslant i \leqslant n$, we have $|S_{\mathcal{B}}| \gg_k q$.*

If $n(B^k - 1) < q$, so that $J_{n,k}(B) = J^*_{n,k}(B)$, we obtain in the same manner from (4.4) and (5.1) the following explicit estimates when $n \geqslant \frac{1}{2}(k^2+k+2)$:

$$N_{\mathcal{B}} \leqslant c_1(n,k)(2n)^{k-1} B^{2n-k}, \tag{7.3}$$

and

$$|S_{\mathcal{B}}| \geqslant c_1(n,k)^{-1}(2n)^{1-k} B^k, \tag{7.4}$$

with $c_1(n,k)$ the constant in (5.1) with $\Delta^*_k = 0$.

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

§8. *Proof of Theorem 1.1.* Before proving the theorem we need a few lemmas. For prime p and positive integer k, let $\Gamma(k, p)$ be the minimal n such that for any integers a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, and any integer c, the congruence (1.1) is solvable.

LEMMA 8.1. *For any prime p and positive integer k we have $\Gamma(k, p) \leqslant k$.*

Proof. Let $\mathbb{Z}_p$ be the residue class ring modulo p. For $1 \leqslant i \leqslant n$ let a_i be a non-zero element of $\mathbb{Z}_p$ and $T_i = \{a_i x^k : x \in \mathbb{Z}_p\}$. Then $|T_i| \geqslant (p-1)/k + 1$ and by the Cauchy–Davenport theorem

$$|T_1 + T_2 + \cdots + T_n| \geqslant \min\left\{p, n\frac{p-1}{k} + 1\right\}.$$

Thus, if $n \geqslant k$ the sum set is all of $\mathbb{Z}_p$. □

The following lemma is due to Sárközy [**10**].

LEMMA 8.2 [**10**, Corollary A]. *If A, B, C, D are subsets of $\mathbb{Z}_p$ with $|A||B||C||D| > p^3$, then there is a solution of $a + b = cd$ with $a \in A$, $b \in B$, $c \in C$, $d \in D$.*

An immediate consequence that we will use is the following lemma.

LEMMA 8.3. *If A_1, A_2, A_3, and B_1 are subsets of $\mathbb{Z}_p$ with $|A_1||A_2||A_3||B_1| > p^3$, then $A_1B_1 + A_2 + A_3 = \mathbb{Z}_p$.*

Proof. For any $x \in \mathbb{Z}_p$, apply Sárközy's Lemma with $A = A_2 - x$, $B = A_3$, $C = -A_1$, and $D = B_1$. □

Proof of Theorem 1.1. Suppose that p is a prime, k, n are positive integers with $n \geqslant \frac{3}{2}(k^2 + k + 2)$, and that c, a_i are integers with $p \nmid a_i$, $1 \leqslant i \leqslant n$. Our goal is to produce a solution of the diagonal congruence (1.1) with

$$1 \leqslant x_i \leqslant \kappa(k)p^{1/k},$$

for some constant $\kappa(k)$. Set $n_1 = (k^2 + k + 2)/2$. By specifying variables if needed we may assume that $n = 3n_1$. We claim that we may take $\kappa(k)$ to be

$$\kappa(k) := \max\{2^k, \lceil k/c_2(k)^3 \rceil\}$$

with $c_2(k)$ the constant occurring in (8.1). If $p \leqslant \kappa(k)$, the result is trivial. In this case the x_i are allowed to run through a complete residue system modulo p. Since $\Gamma(k, p) \leqslant k$ by Lemma 8.1, it suffices to have $n \geqslant k$. Thus we may assume that $p > \max\{2^k, \lceil k/c_2(k)^3 \rceil\}$.

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

Let $\mathcal{B}$ be the cube $1 \leqslant x_i \leqslant B$, $1 \leqslant i \leqslant n$, in n variables with edge length B satisfying $\frac{1}{2}p^{1/k} \leqslant B < p^{1/k}$. Such an integer B exists since $p > 2^k$. Divide the n variables into three disjoint sets, F_1, F_2, F_3, with $|F_i| = n_1$, $1 \leqslant i \leqslant 3$. Let $\mathcal{B}_i$ be the cube corresponding to the ith set of variables, and let A_1, A_2, A_3 be the value sets of the diagonal sums over each of these sets of variables. Thus, for the first set of variables, $F_1 = \{x_1, \dots, x_{n_1}\}$ say,

$$A_1 = \{a_1x_1^k + \cdots + a_{n_1}x_{n_1}^k \pmod p : 1 \leqslant x_i \leqslant B, 1 \leqslant i \leqslant n_1\},$$

and similarly for A_2 and A_3. Set $D := \{1^k, 2^k, \dots, L^k\} \subseteq \mathbb{Z}_p$ (with L a parameter to be chosen later), a set with at least L/k distinct values modulo p assuming that $L \leqslant p$. Since $B \geqslant \frac{1}{2}p^{1/k}$ we have from Lemma 7.1 that

$$|A_1|, |A_2|, |A_3| \geqslant c_2(k)p \tag{8.1}$$

for some constant $c_2(k)$. Thus, if $L \leqslant p$ and $c_2(k)^3p^3L/k > p^3$, we can apply Lemma 8.3 to obtain $A_1D + A_2 + A_3 = \mathbb{Z}_p$. It suffices to take $L = \lceil k/c_2(k)^3 \rceil$, a value that is at most p by our assumption that $p > \lceil k/c_2(k)^3 \rceil$. We have

$$A_1D = \left\{ \sum_{i=1}^{n_1} a_i(yx_i)^k \pmod p : 1 \leqslant y \leqslant L, 1 \leqslant x_i \leqslant B, 1 \leqslant i \leqslant n_1 \right\}.$$

Observing that $1 \leqslant yx_i \leqslant LB < Lp^{1/k} \leqslant \kappa(k)p^{1/k}$, we obtain a solution of (1.1) with the first n_1 variables bounded by $\kappa(k)p^{1/k}$ and the remaining ones by $p^{1/k}$. □

Remark 8.1. It is plain from the proof above that the cubes corresponding to the second and third sets of variables may be taken in arbitrary position since Lemma 7.1 applies to a general cube. In this way we can obtain a solution of (1.1) with n_1 variables restricted to the interval $[1, \kappa(k)p^{1/k}]$, and the other $2n_1$ variables in arbitrary intervals of length $B \geqslant p^{1/k}$.

Remark 8.2. The constant $\kappa(k)$ in Theorem 1.1 may be taken to be

$$\kappa(k) = 2^{3k}kc_1(n_1, k)^3n_1^{3k},$$

for $p \gg_k 1$, where $n_1 = \frac{1}{2}(k^2+k+2)$, and $c_1(n_1, k)$ is the constant in (5.1) with $\Delta_k^* = 0$.

§9. *Smooth solutions* (mod q). In order to prove Theorem 1.2, we seek smooth solutions of the diagonal congruence (1.1). Let k, q, n, ℓ, and B be positive integers and $\mathcal{A} = \mathcal{A}(B, B^{1/\ell})$ be the set of $B^{1/\ell}$-smooth numbers defined by

$$\mathcal{A} := \{x \in [1, B] \cap \mathbb{Z} : p \text{ prime}, p|x \Rightarrow p \leqslant B^{1/\ell}\}. \tag{9.1}$$

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

By the work of Ramaswami [9], we have

$$|\mathcal{A}| = |\mathcal{A}(B, B^{1/\ell})| = B\rho(\ell) + \mathrm{O}\left(\frac{B}{\log B}\right), \tag{9.2}$$

where $\rho(\ell)$ is the Dickman function. Let $\mathcal{A}^n$ denote the cartesian product of $\mathcal{A}$ with itself n times and put

$$I^*_{n,k}(\mathcal{A}^n) = \#\left\{(\underline{x}, \underline{y}) \in \mathcal{A}^n \times \mathcal{A}^n : \sum_{i=1}^{n}(x_i^k - y_i^k) = 0\right\}.$$

Following Wooley, [16, §2, p. 4], we call an exponent $\Delta_{n,k}$ permissible when for ℓ sufficiently large, $\ell \geqslant \ell_0(k, n)$, and for any $\varepsilon > 0$, we have

$$I^*_{n,k}(\mathcal{A}^n) \leqslant c(\varepsilon, k, \ell, n)B^{2n-k+\varepsilon+\Delta_{n,k}},$$

for some constant $c(\varepsilon, k, \ell, n)$. The following lemma of Wooley provides a value for $\Delta_{n,k}$.

LEMMA 9.1 [16, Lemma 2.1]. *For $k \geqslant 4$, $n \geqslant 2$, let $\Delta_{n,k}$ be the unique positive solution of the equation $\Delta_{n,k}\mathrm{e}^{\Delta_{n,k}/k} = k\mathrm{e}^{1-2n/k}$. Then $\Delta_{n,k}$ is permissible. In particular, the exponent $\Delta^*_{n,k} = k\mathrm{e}^{1-2n/k}$ is permissible.*

For any positive integers $k \geqslant 4$, $n \geqslant 2$ and positive real $\delta < k$ with $n > \frac{1}{2}k\log(ek/\delta)$, we obtain from the lemma the permissible exponent

$$\Delta^*_{n,k} := k\mathrm{e}^{1-2n/k} < k\mathrm{e}^{1-\log(ek/\delta)} = \delta. \tag{9.3}$$

For any integers a_i with $(a_i, q) = 1$, $1 \leqslant i \leqslant n$, let $N_{\mathcal{A}^n}$ denote the value

$$N_{\mathcal{A}^n} := \#\left\{(\underline{x}, \underline{y}) \in \mathcal{A}^n \times \mathcal{A}^n : \sum_{i=1}^{n} a_i x_i^k \equiv \sum_{i=1}^{n} a_i y_i^k \pmod q\right\}.$$

Following the proof of Lemma 3.1, we obtain

$$N_{\mathcal{A}^n} \leqslant \#\left\{(\underline{x}, \underline{y}) \in \mathcal{A}^n \times \mathcal{A}^n : \sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod q\right\}.$$

If $n(B^k - 1) < q$, so that any solution of the congruence $\sum_{i=1}^n x_i^k \equiv \sum_{i=1}^n y_i^k \pmod q$ is a solution of the corresponding equation, we then obtain

$$N_{\mathcal{A}^n} \leqslant I^*_{n,k}(\mathcal{A}^n) \leqslant c(\varepsilon, k, \ell, n)B^{2n-k+\varepsilon+\Delta_{n,k}},$$

for any permissible exponent $\Delta_{n,k}$.

Letting $S_{\mathcal{A}^n}$, denote the value set

$$S_{\mathcal{A}^n} := \left\{\sum_{i=1}^{n} a_i x_i^k \in \mathbb{Z}_q : \underline{x} \in \mathcal{A}^n\right\},$$

and using $|S_{\mathcal{A}^n}| \geqslant |\mathcal{A}^n|^2/N_{\mathcal{A}^n}$, together with the lower bound $|\mathcal{A}^n| > \frac{1}{2}\rho(\ell)^n B^n$ available from (9.2) for B sufficiently large, we obtain the following lower bound on $|S_{\mathcal{A}^n}|$.

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

LEMMA 9.2. *For any positive integers k, ℓ, n, q, B and $\varepsilon > 0$ with $B^k < q/n$, and integers a_i with $(a_i, q) = 1$, $1 \leqslant i \leqslant n$, we have*

$$|S_{\mathcal{A}^n}| \gg_{k,\ell,n,\varepsilon} B^{k-\varepsilon-\Delta_{n,k}},$$

for any permissible exponent $\Delta_{n,k}$.

§10. *Proofs of Theorem 1.2 and Corollary 1.1.*

Proof of Theorem 1.2. Let k, n be positive integers with $n > \frac{3}{2}k\log(3e/\varepsilon)+3$, p a prime, a_i be integers with $p \nmid a_i$, $1 \leqslant i \leqslant n$ and c be any integer. Our goal is to obtain a solution of the diagonal congruence (1.1) with

$$1 \leqslant x_i \ll_{\varepsilon,k} p^{1/k+\varepsilon}, \quad 1 \leqslant i \leqslant n. \tag{10.1}$$

If $k = 1$ the result is trivial. For $k = 2$, it is already known [7] that for $n \geqslant 4$ (1.1) has a solution with $1 \leqslant x_i \ll \sqrt{p}\log p$. For $k = 3$ the result follows from Theorem 1.1 for $\varepsilon \leqslant 0.18$ and from (2.3) for $\varepsilon \geqslant 0.18$. Thus, we may assume that $k \geqslant 4$.

Set $m = \lfloor n/3 \rfloor$ and $B = \lfloor (3p/n)^{1/k} \rfloor$. Since $n > k$, we know by Lemma 8.1 that (1.1) is solvable. Thus by taking the implied constant in (10.1) sufficiently large we may assume that p is greater than any constant we may need depending only on ε, n and k. In particular, we may assume that $3p > n$, whence $B \geqslant 1$. Let $\mathcal{A}$ be the set of $B^{1/\ell}$-smooth numbers as in (9.1), with ℓ sufficiently large. We divide the n variables into three sets, each with at least m variables. Assuming the first set of variables is $x_1, \ldots, x_m$, let

$$A_1 = \left\{ \sum_{i=1}^{m} a_i x_i^k \in \mathbb{Z}_p : x_i \in \mathcal{A}, 1 \leqslant i \leqslant m \right\},$$

and define A_2 and A_3 similarly for the second and third sets of variables.

Note that $m > n/3 - 1 > \frac{1}{2}k\log(3e/\varepsilon)$, and so by (9.3) with $\delta = \varepsilon k/3$, there exists a permissible exponent $\Delta^*_{m,k} < \varepsilon k/3$. Let $\varepsilon' > 0$ satisfy $\varepsilon' + \Delta^*_{m,k} = \varepsilon k/3$. We have $B^k < 3p/n \leqslant p/m$, and so by Lemma 9.2 (with ε taken to be ε') we obtain

$$|A_1|, |A_2|, |A_3| \gg_k B^{k-k\varepsilon/3} \gg_k p^{1-\varepsilon/3}.$$

Let $D = \{1^k, 2^k, 3^k, \ldots, L^k\} \subseteq \mathbb{Z}_p$, a set with at least L/k distinct values (mod p), assuming that $L \leqslant p$. Thus, for $L \gg_{k,n} p^{\varepsilon}$,

$$|A_1||A_2||A_3||D| \geqslant p^3,$$

and applying Lemma 8.3, we obtain a solution of (1.1) with

$$1 \leqslant x_i \leqslant LB \ll_k p^{1/k+\varepsilon},$$

for $1 \leqslant i \leqslant n$. □

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

Remark 10.1. An alternate way of stating Theorem 1.2 is as follows: for any positive integers k, n, prime p, $\tau > 3e^{1-2(n-3)/3k}$ and integers a_i, c with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there is a solution of (1.1) with $1 \leqslant x_i \ll_{k,\tau} p^{1/k+\tau}$.

Proof of Corollary 1.1. For convenience, we call a solution of (1.1) a small solution if $1 \leqslant x_i \ll_k \sqrt{p}$, $1 \leqslant i \leqslant n$. For $k = 2$, Theorem 1.1 gives a small solution for $n \geqslant 12$. For $k = 3$, the inequality in (2.3) gives a small solution for $n \geqslant 9$, while for $k = 4$ it yields a small solution for $n \geqslant 17$. Thus for $k \leqslant 4$ and $n \geqslant 5k+3$, there is small solution. Suppose now that $k \geqslant 5$. Letting $\varepsilon = \frac{1}{2} - 1/k$ in Theorem 1.2, we see that if $n > \frac{3}{2}k \log(6ek/(k-2)) + 3$ then there exists a small solution. For $k \geqslant 5$, $\frac{3}{2}\log(6ek/(k-2)) \leqslant 4.96$, and thus for $n \geqslant 5k+3$ there is a small solution. □

Remark 10.2. An alternate way of stating the corollary with a smaller constant on k is the following: for $k \geqslant 3$ and $n \geqslant 4.19k + 6 + 6/(k-2)$, there is a solution of (1.1) with $1 \leqslant x_i \ll_k \sqrt{p}$.

Acknowledgement. The research of the third author was supported in part by NSA Young Investigator Grant #H98230-14-1-0164.

References

1. R. C. Baker, Small solutions of congruences. *Mathematika* **30** (1983), 164–188.
2. R. C. Baker, *Diophantine Inequalities* (*London Mathematical Society Monographs*), Clarendon Press (Oxford, 1986).
3. J. Bourgain, C. Demeter and L. Guth, Proof of the main conjecture in Vinogradov's mean value theorem for degrees higher than three. *Ann. of Math.* (2) **184**(2) (2016), 633–682.
4. J. Cilleruelo, M. Z. Garaev, A. Ostafe and I. E. Shparlinski, On the concentration of points of polynomial maps and applications. *Math. Z.* **272** (2012), 825–837.
5. T. Cochrane, *Exponential Sums and the Distributions of Solutions of Congruences* (*Institute of Mathematics*), Academia Sinica (Taipei, Taiwan, 1994), 1–84.
6. T. Cochrane, M. Ostergaard and C. Spencer, Small solutions of diagonal congruences. *Funct. Approx. Comment. Math.* **56**(1) (2017), 39–48.
7. T. Cochrane and Z. Zheng, Small solutions of the congruence $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \equiv c \pmod p$. *Acta Math. Sinica (N.S.)* **14**(2) (1998), 175–182.
8. R. Dietmann, Small solutions of additive cubic congruences. *Arch. Math.* **75** (2000), 195–197.
9. V. Ramaswami, On the number of positive integers less than x and free of prime divisors greater than x^c. *Bull. Amer. Math. Soc.* **55** (1949), 1122–1127.
10. A. Sárközy, On products and shifted products of residues modulo p. *Integers* **8**(2) (2008), A9, 8 pp.
11. W. M. Schmidt, Small zeros of additive forms in many variables, II. *Acta Math.* **143**(3–4) (1979), 219–232.
12. W. M. Schmidt, Bounds on exponential sums. *Acta Arith.* **94**(3) (1984), 281–297.
13. W. M. Schmidt, Small solutions of congruences with prime modulus. In *Diophantine Analysis, Proc. Number Theory Sect. Aust. Math. Soc. Conv. 1985* (*London Mathematical Society Lecture Notes Series* **109**), Cambridge University Press (Cambridge, 1986), 37–66.
14. I. E. Shparlinski and A. Zumalacárregui, On the density of zeros of diagonal forms modulo a prime. *Preprint*, 2017.
15. I. M. Vinogradov, New estimates for Weyl sums. *Dokl. Akad. Nauk SSSR* **8** (1935), 195–198.
16. T. D. Wooley, New estimates for smooth Weyl sums. *J. Lond. Math. Soc.* **51** (1995), 1–13.
17. T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing. *Ann. of Math.* (2) **175** (2012), 1575–1627.
18. T. D. Wooley, Vinogradov's mean value theorem via efficient congruencing, II. *Duke Math. J.* **162** (2013), 673–730.

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press

Todd Cochrane,
Department of Mathematics,
Kansas State University,
Manhattan, KS 66506,
U.S.A.
E-mail: cochrane@math.ksu.edu

Craig Spencer,
Department of Mathematics,
Kansas State University,
Manhattan, KS 66506,
U.S.A.
E-mail: cvs@math.ksu.edu

Misty Ostergaard,
Department of Mathematics,
University of Southern Indiana,
Evansville, IN 47712,
U.S.A.
E-mail: m.ostergaard@usi.edu

https://doi.org/10.1112/S0025579318000025 Published online by Cambridge University Press