Functiones et Approximatio
56.1 (2017), 39–48
doi: 10.7169/facm/1587

SMALL SOLUTIONS OF DIAGONAL CONGRUENCES

Todd Cochrane, Misty Ostergaard, Craig Spencer

Abstract: We prove that for $k \geqslant 2$, $0 < \varepsilon < \frac{1}{k(k-1)}$, $n > \frac{k-1}{\varepsilon}$, prime $p > P(\varepsilon, k)$, and integers c, a_i, with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution $\underline{x}$ to the congruence

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

in any cube $\mathcal{B}$ of side length $b \geqslant p^{\frac{1}{k}+\varepsilon}$. Various refinements are given for smaller n and for cubes centered at the origin.

Keywords: diagonal congruences in many variables, exponential sums.

1. Introduction

Our goal is to find small integer solutions to the congruence

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

with p prime, $k \in \mathbb{N}$, and $a_i, c \in \mathbb{Z}$, $1 \leqslant i \leqslant n$. By small we mean $\|\underline{x}\| := \max|x_i| \leqslant \xi p^{\lambda}$ with $\lambda < 1$ and ξ a constant possibly dependent upon λ, k, or n. We hope, in particular, to find the smallest possible value of λ for a given k and n. We also find solutions within a small box that is not centered at the origin. In this case, we seek the minimal b such that any cube $\mathcal{B} := \{\underline{x} : d_i + 1 \leqslant x_i \leqslant d_i + b, 1 \leqslant i \leqslant n\}$ with $d_i \in \mathbb{Z}$ for $1 \leqslant i \leqslant n$, contains a solution of (1).

The optimal choice of λ is $\lambda = \frac{1}{k}$. We reach this conclusion after considering the congruence $\sum_{i=1}^{n} x_i^k \equiv \frac{p-1}{2} \mod p$. Any solution $\underline{x}$ must satisfy $n\|\underline{x}\|^k \geqslant |\sum_{i=1}^{n} x_i^k| \geqslant \frac{p-1}{2}$ and so $\|\underline{x}\| \geqslant \left(\frac{p-1}{2n}\right)^{\frac{1}{k}}$.

A similar problem may be posed with a composite modulus or a homogeneous congruence (restricting c in (1) to be 0). There is also the option of making some restrictions on k or n. For instance, Schmidt in [11, Equation (4.1)] proved that

2010 Mathematics Subject Classification: primary: 11D79, 11D72; secondary: 11L03

for k odd, $\varepsilon > 0$, and n sufficiently large, there exists a nonzero solution to the homogeneous congruence with $\|\underline{x}\| \ll p^{\varepsilon}$. Thus, one can surpass the $p^{\frac{1}{k}}$ barrier for a homogeneous congruence of odd degree. For a homogeneous congruence of even degree, $p^{\frac{1}{k}}$ is still optimal.

Baker [1] and Dietmann [6] proved results in the homogeneous case for a composite modulus. In particular, Baker proved in [1, Theorem 1] that for any $\varepsilon > 0$, $m \in \mathbb{N}$, and integers $a_1, a_2, \ldots, a_n$, there is a nonzero solution of

$$a_1x_1^k + \cdots + a_nx_n^k \equiv 0 \mod m$$

with

$$\|\underline{x}\| < \begin{cases} m^{\frac{1}{2}+\frac{1}{2(n-1)}+\varepsilon}, & n \geqslant 4; \\ m^{\frac{2}{3}+\varepsilon}, & n = 3. \end{cases}$$

Dietmann [6] made an improvement for cubic congruences. He proved that for $a_1, \ldots, a_n \in \mathbb{Z}$, $n \geqslant 3$, and $m \in \mathbb{N}$, there is a nonzero solution of the congruence

$$a_1x_1^3 + \cdots + a_nx_n^3 \equiv 0 \mod m$$

with

$$\|\underline{x}\| \leqslant \begin{cases} m^{\frac{1}{2}+\frac{1}{2n}}, & n \text{ odd}; \\ m^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \text{ even}. \end{cases}$$

Cochrane [4, Equation (2.33), Example 4.8.14] considered a non-homogeneous congruence with prime moduli. He proved that for $k, n \in \mathbb{N}$, any prime p, and $a_i, c \in \mathbb{Z}$, with $p \nmid a_i$, $1 \leqslant i \leqslant n$, and $p \nmid c$, the diagonal congruence (1) has a solution in any cube of side length b for which

$$b \gg_{k,n} p^{\frac{1}{2}+\frac{1}{2n}}. \tag{2}$$

For $c = 0$ and $n \geqslant 3$, the same result holds (as seen in [4, Theorem 4.7.13]) with $b \gg_{k,n} p^{\frac{1}{2}+\frac{1}{2(n-1)}}$.

In [13, Theorem 3], Schmidt proved that for $a_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$, p a prime, $k \geqslant 3$ odd, and $\varepsilon > 0$, the congruence

$$\sum_{i=1}^{n} a_ix_i^k \equiv 0 \mod p$$

has a nonzero solution $\underline{x}$ with

$$\|\underline{x}\| \ll_{n,\varepsilon} p^{\frac{1}{3}+\sqrt{\frac{c(k)}{n}}+\varepsilon} \tag{3}$$

for a constant $c(k)$ depending on k.

Applying a result of Schmidt [12, Theorem 3], Cochrane [4, Cor. 5.7] showed that for $k \geqslant 2$, there exists a solution to (1) for arbitrary c in any cube with side length

$$b \gg_{\varepsilon,k,n} p^{\frac{1}{k}+\frac{1}{n}(1-\frac{1}{k})2^k\Phi(k)+\varepsilon} \tag{4}$$

where $\Phi(k)$ is a constant dependent upon k. The result of Schmidt shows that one can take $\Phi(2) = \Phi(3) = 1$, $\Phi(4) = 3$, $\Phi(5) = 13$, and in general, $\Phi(k) < (\log 2)^{-k}k!$.

Baker proved in [2, Lemma 10.1] that for $m \in \mathbb{N}$, $a_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$, and $n \geqslant C(k,\varepsilon)$, there exist non-negative integers $x_1, \dots, x_n$ satisfying

$$\sum_{i=1}^{n} a_i x_i^k \equiv 0 \mod m$$

with

$$\|\underline{x}\| \leqslant m^{\frac{1}{k}+\varepsilon}, \tag{5}$$

although no attempt was made to make $C(k,\varepsilon)$ explicit.

Here we improve on the above stated results for the case of prime moduli, establishing two main theorems, the first for cubes centered at the origin, and the second for a cube in general position. The results apply equally well to the homogeneous and non-homogeneous congruences.

Theorem 1. *For $k \geqslant 2$ and $\varepsilon > 0$, there exists a constant $P(\varepsilon,k)$ such that for any prime $p > P(\varepsilon,k)$ and integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a nonzero solution $\underline{x}$ to* (1) *with*

$$\|\underline{x}\| \leqslant \begin{cases} p^{\frac{k(\log k+\gamma\log\log k)}{n}+\varepsilon}, & \text{if } n \leqslant k(k-1)(\log k+\gamma\log\log k); \\ p^{\frac{1}{k-1}}, & \text{if } k(k-1)(\log k+\gamma\log\log k) < n \leqslant k(k-1)^2; \\ p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon}, & \text{if } n > k(k-1)^2. \end{cases}$$

Here, γ is the constant appearing in Lemma 2.

Thus, as $n \to \infty$, we approach the optimal estimate $\|\underline{x}\| \ll p^{\frac{1}{k}}$. In particular, for any positive $\varepsilon' < \frac{1}{k(k-1)}$ and $n > \frac{k-1}{\varepsilon'}$, applying the theorem with $\varepsilon = \varepsilon' - \frac{k-1}{n}$, gives a solution of (1) with $\|\underline{x}\| \ll p^{\frac{1}{k}+\varepsilon'}$, for p sufficiently large. Indeed, as the next theorem illustrates, for such n, p, any box of side length $b \gg p^{\frac{1}{k}+\varepsilon'}$ contains a solution of (1). The first two estimates in the theorem are consequences of Proposition 2 in Section 3 while the third follows from Proposition 1 in Section 2, as we indicate after the statement of these propositions. These estimates improve on the estimate $\|\underline{x}\| \ll p^{\frac{1}{2}+\frac{1}{2n}}$ available from (2) for $n > (2+\mathrm{o}(1))k\log k$ and uniformly improve on (3) and (4).

For solutions in an arbitrary cube, we establish the following result.

Theorem 2.

i) *For $k \geqslant 2$ and $\varepsilon > 0$, there exists a constant $P(\varepsilon,k)$ such that for any prime $p > P(\varepsilon,k)$ and integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution $\underline{x}$ to* (1) *in an arbitrary cube $\mathcal{B}$ of side length b provided that*

$$b \geqslant \begin{cases} p^{\frac{k(k-1)}{n}+\varepsilon}, & \text{if } n \leqslant k(k-1)^2; \\ p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon}, & \text{if } n > k(k-1)^2. \end{cases} \tag{6}$$

ii) *For $2 \leqslant k \leqslant 5$, the inequalities in* (6) *may be improved to*

$$b \geqslant \begin{cases} p^{\frac{2^{k-1}}{n}+\varepsilon}, & \text{if } n \leqslant 2^{k-1}(k-1); \\ p^{\frac{1}{k}+\frac{2^{k-1}}{nk}+\varepsilon}, & \text{if } n > 2^{k-1}(k-1). \end{cases} \tag{7}$$

These results yield improvements on the bound in (2) for $k \geqslant 6$ and $n \geqslant 2k(k-1)$ and uniformly improve on (4). They also yield improvements on (2) for $k = 3$, $n \geqslant 8$; $k = 4$, $n \geqslant 16$; and $k = 5$, $n \geqslant 32$. We have nothing new to offer here for $k = 2$.

2. Solutions in a general cube

We start by recalling a classical result of Hua and Vandiver [8] and Weil [14] on the number $N_n(c)$ of solutions of the equation

$$\sum_{i=1}^{n} a_i x_i^k = c \tag{8}$$

over the finite field $\mathbb{F}_p$ in p elements, where $a_i \neq 0$, $1 \leqslant i \leqslant n$: If $c \neq 0$ then

$$|N_n(c) - p^{n-1}| \leqslant (k-1)^n p^{\frac{n-1}{2}}. \tag{9}$$

Thus, for $c \neq 0$, and $n \geqslant 2$, the equation (8) is guaranteed to have at least one solution provided that

$$p > k^{\frac{2n}{n-1}}. \tag{10}$$

For $c = 0$, (8) always has the trivial solution $\underline{x} = \underline{0}$. We note that $N_n(c)$ is just the number of solutions of (1) in a cube of side length $b = p$.

Next we turn to finding solutions in a restricted cube

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : d_i + 1 \leqslant x_i \leqslant d_i + b\} \tag{11}$$

of side length b where $b, d_i \in \mathbb{Z}$, $1 \leqslant i \leqslant n$, $b \geqslant 1$. The key ingredient to our investigation is a Weyl sum estimate for the incomplete exponential sum $\sum_{x=1}^{X} e(\alpha_1 x + \cdots + \alpha_k x^k)$; here, $e(x) := e^{2\pi i x}$ for $x \in \mathbb{R}$. The classical Weyl sum bound is stated in the next lemma; see [5, Lemma 3.1].

Lemma 1. *Let $k \geqslant 2$ be an integer, and $\alpha_i \in \mathbb{R}$, $1 \leqslant i \leqslant k$. Suppose that for some $a \in \mathbb{Z}$, $q \in \mathbb{N}$ with $(a, q) = 1$, one has $|\alpha_k - \frac{a}{q}| \leqslant q^{-2}$. Then with $\sigma = \sigma(k) = 2^{1-k}$, we have*

$$\left|\sum_{x=1}^{X} e(\alpha_1 x + \cdots + \alpha_k x^k)\right| \leqslant c_\varepsilon X^{1+\varepsilon} \left(\frac{1}{q} + \frac{1}{X} + \frac{q}{X^k}\right)^{\sigma} \tag{12}$$

for some constant $c_\varepsilon := c_\varepsilon(k)$.

Wooley [17, Theorem 11.1] established an improved estimate, obtaining the inequality in (12) with $\sigma(k) = \frac{1}{2k(k-2)}$ for $k \geqslant 4$, and made further improvements in [19, Theorem 11.1], and [18, Theorem 7.3] obtaining in the latter, $\sigma(k) = \frac{1}{2(k-1)(k-2)}$ for $k \geqslant 3$. Bourgain, Demeter and Guth [3] recently obtained $\sigma(k) = \frac{1}{k(k-1)}$ for $k \geqslant 2$. The latter value improves on Wooley's estimates and the classical value $\sigma(k) = 2^{1-k}$ for $k \geqslant 6$. For $k = 6$, an estimate of Heath-Brown [7] is better for certain ranges of q. Finally, Montgomery [9, Conjecture 1, p. 46] has conjectured that one can in fact take $\sigma(k) = \frac{1}{k}$, which would be best possible. Such a value is currently only known to hold for $k = 2$.

Proposition 1. *Fix $n \geqslant 2$, $k \geqslant 2$, and suppose that the Weyl sum estimate in (12) holds for some positive real $\sigma = \sigma(k)$. For any $\varepsilon > 0$, there exists a constant $P(\varepsilon, k)$ such that for any prime $p \geqslant P(\varepsilon, k)$ and any integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, there exists a solution $\underline{x}$ to (1) in any cube $\mathcal{B}$ of side length*

$$b \geqslant \begin{cases} p^{\frac{1}{\sigma n}+\varepsilon}, & \text{if } n \leqslant (k-1)\sigma^{-1}; \\ p^{\frac{1}{k}+\frac{1}{\sigma n k}+\varepsilon}, & \text{if } n > (k-1)\sigma^{-1}. \end{cases}$$

Applying the proposition with the value of Bourgain, Demeter and Guth, $\sigma = \frac{1}{k(k-1)}$, immediately yields Theorem 2 (i) and the third inequality in Theorem 1. For $2 \leqslant k \leqslant 5$ we use the classical value $\sigma = 2^{k-1}$ to obtain Theorem 2 (ii).

Proof. Fix $n \geqslant 2$, $k \geqslant 2$, and $\varepsilon > 0$, and let c, a_i be integers with $p \nmid a_i$, $1 \leqslant i \leqslant n$, $\mathcal{B}$ be a cube as in (11), N the number of solutions of (1) in $\mathcal{B}$, and $e_p(\xi) = e^{\frac{2\pi i}{p}\xi}$. Then

$$\begin{aligned} N &= \frac{1}{p} \sum_{\underline{x} \in \mathcal{B}} \sum_{\lambda=1}^{p} e_p\left(\lambda\left(\sum_{i=1}^{n} a_i x_i^k - c\right)\right) \\ &= \frac{|\mathcal{B}|}{p} + \frac{1}{p}\sum_{\lambda=1}^{p-1} e_p(-\lambda c) \sum_{\underline{x}\in\mathcal{B}} e_p\left(\lambda\left(\sum_{i=1}^{n} a_i x_i^k\right)\right) \\ &= \frac{b^n}{p} + \frac{1}{p}\sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=d_i+1}^{d_i+b} e_p\left(\lambda a_i x_i^k\right), \end{aligned}$$

and thus

$$N = \frac{b^n}{p} + \frac{1}{p}\sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=1}^{b} e_p\left(\lambda a_i (x_i+d_i)^k\right). \tag{13}$$

We now apply the Weyl sum estimate of Lemma 1 to the polynomial $\lambda a_i (x_i + d_i)^k$ with $X = b$, $q = p$, and $\alpha_k = \frac{\lambda a_i}{p}$. We observe that with $a = \lambda a_i$, we have $(a, p) = 1$ and $|\alpha_k - \frac{a}{p}| = 0 < \frac{1}{p^2}$. It is also plain that with b satisfying the lower bound stated in the proposition, $b^k \geqslant p$. Thus, by (12), we have

$$\left|\sum_{x_i=1}^{b} e_p(\lambda a_i (x_i + d_i)^k)\right| \leqslant c_{\varepsilon'} b^{1+\varepsilon'} \left(\frac{1}{p} + \frac{1}{b} + \frac{p}{b^k}\right)^{\sigma} \tag{14}$$

for any $\varepsilon' > 0$. We use (13) to determine a lower bound for b such that the error term is less than the main term in (13). It suffices to have b satisfy

$$\frac{b^n}{p} > \frac{1}{p}\left|\sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=1}^{b} e_p\left(\lambda a_i (x_i + d_i)^k\right)\right|. \tag{15}$$

First, let us consider the case where $n > (k-1)\sigma^{-1}$. In this case, we put $b = \lfloor p^{\frac{1}{k}+\frac{1}{\sigma nk}+\varepsilon} \rfloor$. We claim that $b^{k-1} \leqslant p$. Indeed, say $n = (k-1)\sigma^{-1} + \beta$, with $\beta > 0$, so that, $n - \beta = (k-1)\sigma^{-1}$. Then

$$b^{k-1} \leqslant p^{\frac{k-1}{k}+\frac{k-1}{\sigma kn}+\varepsilon(k-1)} \leqslant p^{1-\frac{1}{k}+\frac{n-\beta}{kn}+\varepsilon(k-1)} = p^{1-\frac{\beta}{kn}+\varepsilon(k-1)} \leqslant p,$$

for $\varepsilon \leqslant \frac{\beta}{k(k-1)n}$, which we may assume. Using $b^{k-1} \leqslant p$, the Weyl sum estimate in (14) simplifies to

$$\left| \sum_{x_i=1}^{b} e_p(\lambda a_i (x_i + d_i)^k) \right| \leqslant c_{\varepsilon'} b^{1+\varepsilon'} \left(\frac{3p}{b^k} \right)^{\sigma}$$

for any $\varepsilon' > 0$. Applying this estimate and the triangle inequality to the right-hand side of (15), we find that we are guaranteed a solution to (1) if

$$\frac{b^n}{p} > c_{\varepsilon'}^n \left(b^{(1+\varepsilon')n} \right) \left(\frac{3p}{b^k} \right)^{n\sigma} \tag{16}$$

or equivalently

$$b^{n\left(k\sigma - \varepsilon'\right)} \geqslant 3^{n\sigma} c_{\varepsilon'}^n p^{1+n\sigma}.$$

Thus it suffices to have

$$b \gg_{k,\varepsilon'} p^{\frac{1+n\sigma}{n(k\sigma-\varepsilon')}} = p^{\frac{1}{k-\varepsilon'\sigma^{-1}}+\frac{\sigma^{-1}}{n(k-\varepsilon'\sigma^{-1})}} = p^{\frac{1}{k(1-\varepsilon'\sigma^{-1}k^{-1})}+\frac{\sigma^{-1}}{nk(1-\varepsilon'\sigma^{-1}k^{-1})}}.$$

If $\frac{\varepsilon'}{\sigma k} < \frac{1}{2}$ then using $(1-x)^{-1} < 1 + 2x$ for $0 < x < \frac{1}{2}$, we see that it suffices to have

$$b \gg_{k,\varepsilon'} p^{\frac{1}{k}+2\frac{\varepsilon'}{\sigma k^2}+\frac{1}{\sigma nk}+2\frac{\varepsilon'}{\sigma^2 nk^2}}.$$

By taking ε' sufficiently small and p sufficiently large, we see that the latter bound holds for $b = \lfloor p^{\frac{1}{k}+\frac{1}{\sigma nk}+\varepsilon} \rfloor$.

Next, let us consider the case where $n \leqslant (k-1)\sigma^{-1}$. In this case we set $b = \lfloor p^{\frac{1}{\sigma n}+\varepsilon} \rfloor$. Then plainly $b^{k-1} > p^{\frac{k-1}{\sigma n}} \geqslant p$, and so the Weyl sum estimate simplifies to

$$\left| \sum_{x_i=1}^{b} e_p(\lambda a_i (x_i + d_i)^k) \right| \leqslant c_{\varepsilon'} b^{1+\varepsilon'} \left(\frac{3}{b} \right)^{\sigma},$$

for any $\varepsilon' > 0$. Then by (15), we find we are guaranteed a solution to (1) if

$$\frac{b^n}{p} > c_{\varepsilon'}{}^n \left(b^{(1+\varepsilon')n} \right) \left(\frac{3}{b} \right)^{\sigma n}, \tag{17}$$

and so it suffices to have

$$b \gg_{\varepsilon',k} p^{\frac{1}{\sigma n(1-\varepsilon'/\sigma)}}. \tag{18}$$

If $\varepsilon'/\sigma < \frac{1}{2}$, then it suffices to have

$$b \gg_{\varepsilon',k} p^{\frac{1}{\sigma n}+\frac{2\epsilon'}{\sigma^2 n}}. \tag{19}$$

Thus, for ε' sufficiently small and p sufficiently large, our choice $b = \lfloor p^{\frac{1}{\sigma n}+\varepsilon} \rfloor$ suffices. ■

3. Small solutions via sums over smooth numbers

Let $k \in \mathbb{N}$ and P be a large real number. When $2 \leqslant R \leqslant P$, we define the set of R-smooth numbers, $\mathcal{A}(P,R)$, by

$$\mathcal{A}(P,R) = \{n \in [1,P] \cap \mathbb{Z} : p \text{ prime}, p|n \implies p \leqslant R\},$$

and for each real number α, we define the corresponding Weyl sum over smooth numbers, $f(\alpha; P, R)$, by

$$f(\alpha; P, R) := \sum_{x \in \mathcal{A}(P,R)} e(\alpha x^k).$$

In [15] Wooley established the following estimate for $f(\alpha; P, R)$.

Lemma 2. *[15, Theorem 1.1] Let $\mathfrak{m}$ denote the set of real numbers α such that whenever $a \in \mathbb{Z}, q \in \mathbb{N}, (a,q) = 1$, and $|\alpha - a/q| \leqslant \frac{1}{qP^{k-1}}$, one has $q > P$. Then when $\eta = \eta(\varepsilon, k)$ is a sufficiently small positive number, and $2 \leqslant R \leqslant P^{\eta}$, we have with $\sigma' = \sigma'(k) := k^{-1}(\log k + \gamma \log\log k)^{-1}$,*

$$\sup_{\alpha \in \mathfrak{m}} |f(\alpha; P, R)| \leqslant \xi_\varepsilon P^{1-\sigma'+\varepsilon} \tag{20}$$

for some constants $\xi_\varepsilon := \xi(\varepsilon, k)$ and $\gamma := \gamma(\varepsilon, k)$.

As a consequence of this lemma we shall deduce the following result.

Proposition 2. *Suppose that the inequality in (20) holds for a given $\sigma' = \sigma'(k)$. Then for $k \geqslant 2$, $n > \sigma'^{-1}$ and $\varepsilon > 0$, there exist constants $P(\varepsilon, k)$ and $\eta'(\varepsilon, k)$ such that for any positive integer ℓ satisfying $\frac{1}{\ell} \leqslant \eta'(\varepsilon, k)$, prime $p > P(\varepsilon, k)$, integers c, a_i with $p \nmid a_i$, $1 \leqslant i \leqslant n$, and positive integer b with*

$$b > \max\left\{p^{\frac{1}{\sigma' n}+\varepsilon}, p^{\frac{1}{k-1}}\right\},$$

there exists a solution $\underline{x}$ to (1) with $x_i \in \mathcal{A}(b, b^{\frac{1}{\ell}})$, $1 \leqslant i \leqslant n$.

Applying the proposition with Wooley's value $\sigma' = k^{-1}(\log k + \gamma \log\log k)^{-1}$, yields the first two inequalities in Theorem 1.

Proof. Suppose that $k \geqslant 2$, $n > \sigma'^{-1}$ and that b satisfies $p^{\frac{1}{k-1}} < b < p$. We apply Lemma 2 with $P = b$, $R = b^{1/\ell}$ where ℓ will be chosen below. For the sake of brevity, we'll define $\mathcal{A} := \mathcal{A}(b, b^{\frac{1}{\ell}})$ and let $\mathcal{A}^n = \mathcal{A} \times \mathcal{A} \times \cdots \times \mathcal{A}$, n times. The number of solutions M of $\sum_{i=1}^{n} a_i x_i^k \equiv c \mod p$ with $\underline{x} \in \mathcal{A}^n$ is

$$\begin{aligned} M &= \frac{1}{p} \sum_{\underline{x} \in \mathcal{A}^n} \sum_{\lambda=1}^{p} e_p\left(\lambda\left(\sum_{i=1}^{n} a_i x_i^k - c\right)\right) \\ &= \frac{|\mathcal{A}|^n}{p} + \frac{1}{p} \sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i \in \mathcal{A}} e_p\left(\lambda a_i x_i^k\right). \end{aligned} \tag{21}$$

Let $\mathfrak{m}$ be as defined in Lemma 2. We note that for $1 \leqslant \lambda \leqslant p-1$, $\alpha := \frac{\lambda a_i}{p} \in \mathfrak{m}$. Indeed, suppose that $(a, q) = 1$ and that $|\frac{\lambda a_i}{p} - \frac{a}{q}| \leqslant \frac{1}{qb^{k-1}}$. Then either $q = p$, whence $q > b$, or $q \neq p$, whence

$$\frac{1}{pq} \leqslant \left|\frac{\lambda a_i}{p} - \frac{a}{q}\right| \leqslant \frac{1}{qb^{k-1}};$$

that is $p \geqslant b^{k-1}$, contradicting $b > p^{\frac{1}{k-1}}$. Thus for any $\varepsilon' > 0$ and ℓ sufficiently large, $\ell \geqslant 1/\eta(\varepsilon', k)$, we have by Lemma 2 that

$$\left|\sum_{x_i \in \mathcal{A}} e_p\left(\lambda a_i x_i^k\right)\right| \leqslant \xi_{\varepsilon'} b^{1-\sigma'+\varepsilon'}.$$

Combining this with (21), we see that $M > 0$ provided that

$$\frac{|\mathcal{A}|^n}{p} > \xi_{\varepsilon'}^n b^{(1-\sigma'+\varepsilon')n}.$$

By the work of Ramaswami [10], we have

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

where ρ is the Dickman function. Thus for b sufficiently large in terms of ℓ, we have $|\mathcal{A}(b, b^{\frac{1}{\ell}})| \geqslant \frac{1}{2}\rho(\ell)b$. Hence it suffices to have

$$\frac{\rho(\ell)^n b^n}{2^n p} > \xi_{\varepsilon'}^n b^{(1-\sigma'+\varepsilon')n}, \tag{22}$$

that is,

$$b^{\sigma'-\varepsilon'} > \xi_{\varepsilon'} \frac{2p^{\frac{1}{n}}}{\rho(\ell)}$$

or equivalently

$$b \gg_{\varepsilon',\ell,k} p^{\frac{1}{\sigma' n(1-\varepsilon'\sigma'^{-1})}}.$$

Assuming that $\varepsilon'\sigma'^{-1} < \frac{1}{2}$, we see that it suffices to have

$$b \gg_{\varepsilon',\ell,k} p^{\frac{1}{\sigma' n} + \frac{2\varepsilon'}{\sigma'^2 n}}.$$

Thus with ε' sufficiently small and p sufficiently large, we obtain a solution in $\mathcal{A}^n$ provided that $b > \max\left\{p^{\frac{1}{\sigma' n}+\varepsilon}, p^{\frac{1}{k-1}}\right\}$. We note that since $n > \sigma'^{-1}$, for ε small enough, $p^{\frac{1}{\sigma' n}+\varepsilon} < p$. Thus we may take $p^{\frac{1}{k-1}} < b < p$ as assumed. ∎

Remark 3.1. In his work [16, Theorem 5], Wooley obtains an estimate for a more general Weyl sum over smooth numbers that one may hope would allow us to generalize Proposition 2 to boxes in arbitrary position. Unfortunately, for the application here, this estimate leads to a weaker result than what is already available from Proposition 1.

Acknowledgment. We would like to thank the referee for his/her many valuable comments which greatly improved the paper. 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 Math. Soc. 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. Math. **184** (2016), no. 2, 633–682.

[4] T. Cochrane, *Exponential Sums and the Distribution of Solutions of Congruences*, Inst. of Math., Academia Sinica, Taipei, Taiwan (1994), 1–84.

[5] H. Davenport, *Analytic Methods for Diophantine Equations and Diophantine Inequalities*, 2nd ed., edited and prepared for publication by T.D. Browning, CUP, 2005.

[6] R. Dietmann, *Small solutions of additive cubic congruences*, Arch. Math. **75** (2000), 195–197.

[7] D.R. Heath-Brown, *Weyl's inequality, Hua's inequality, and Waring's problem*, J. London Math. Soc. (20) **38** (1988), 396–414.

[8] L.K. Hua and H.S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 94–99.

[9] H.L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, 84. Published for the Conference Board of the Mathematical Sciences, Washington, DC; by the American Mathematical Society, Providence, RI, 1994.

[10] V. Ramaswami, *On the Number of Positive Integers Less Than x and Free of Prime Divisors Greater Than x^c*, Bulletin of the American Mathematical Society **55** (1949), 1122–1127.

[11] W.M. Schmidt, *Small zeros of additive forms in many variables. II.*, Acta Math. **143** (1979), no. 3-4, 219–232.

[12] W.M. Schmidt, *Bounds on exponential sums*, Acta Arith. **94** (1984), no. 3, 281-297.

[13] W.M. Schmidt, *Small solutions of congruences with prime modulus*, Diophantine analysis, Proc. Number Theory Sect. Aust. Math. Soc. Conv. 1985, London Math. Soc. Lect. Note Ser. **109**, (1986), 37–66.

[14] A. Weil, *Number of solutions of equations in finite fields,* Bull. AMS **55** (1949), 497–508.

[15] T.D. Wooley, *New estimates for smooth Weyl sums*, J. London Math. Soc. **51** (1995), 1–13.

[16] T.D. Wooley, *On exponential sums over smooth numbers*, J. Reine Angew. Math. **488** (1997), 79–140.

[17] T.D. Wooley, *Vinogradov's mean value theorem via efficient congruencing, II*, Duke Math. J. **162** (2013), 673–730.

[18] T.D. Wooley, *Translation invariance, exponential sums, and Waring's problem*, Proceedings of the International Congress of Mathematicians, August 13–21, 2014, Seoul, Korea, Volume II, Kyung Moon Sa Co. Ltd., Seoul, Korea, 2014, 505–529.

[19] T.D. Wooley, *Multigrade efficient congruencing and Vinogradov's mean value theorem*, Proc. London Math. Soc. (3) **111** (2015), no. 3, 519–560.

Addresses: Todd Cochrane and Craig Spencer: Department of Mathematics, Kansas State University, Manhattan, KS 66506, USA;
Misty Ostergaard: Department of Mathematics, University of Southern Indiana, Evansville, IN 47712, USA.

E-mail: cochrane@math.ksu.edu, m.ostergaard@usi.edu, cvs@math.ksu.edu

Received: 9 March 2015; **revised:** 16 March 2016