#A14 INTEGERS 26 (2026)

A NOTE ON SMALL SOLUTIONS TO DIAGONAL CONGRUENCES

Todd Cochrane
Department of Mathematics, Kansas State University, Manhattan, Kansas
cochrane@math.ksu.edu

Misty Ostergaard
Department of Mathematics, University of Southern Indiana, Evansville, Indiana
m.ostergaard@usi.edu

Craig Spencer
Department of Mathematics, Kansas State University, Manhattan, Kansas
cvs@math.ksu.edu

Kathryn Wilson
Department of Mathematics, University of Nebraska-Lincoln, Lincoln, Nebraska
kwilson46@nebraska.edu

Received: 5/2/25, Accepted: 12/23/25, Published: 1/5/26

Abstract

Using a result of Chow, Lindqvist, and Prendiville, we establish that for any positive integer k, positive integer n with $n \geq \frac{3}{2}k(\log k + \log \log k + 2 + O(\log \log k / \log k))$, prime p, integer c, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq n$, there exists a solution to $a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv c \pmod{p}$ with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq n$.

1. Introduction

For prime p and positive integer k, let $\Gamma(k, p)$ denote the minimal positive integer n such that for any integers a_i with $p \nmid a_i$, $1 \leq i \leq n$, and integer c,

$$a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv c \pmod{p} \tag{1}$$

has a solution. In [5], Cochrane, Ostergaard, and Spencer were able to obtain solutions to Equation (1) with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq n$ when $n \geq \frac{3}{2}(k^2 + k + 2)$. The goal of this paper is to lower the required number of variables needed to obtain solutions to Equation (1) with variables of size $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq n$. Of note,

DOI: 10.5281/zenodo.18154204

by looking at the congruence $\sum_{i=1}^{n} x_i^k \equiv \frac{p-1}{2} \pmod{p}$, we see that $1 \le x_i \ll_k p^{\frac{1}{k}}$ for $1 \le i \le n$ is optimal.

Obtaining small solutions has been studied for homogeneous congruences as well. For homogeneous congruences of the form

$$a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv 0 \pmod{p} \tag{2}$$

where the a_i, $1 \le i \le n$, are integers and p is prime, Schmidt [10] found that when k is odd, $\epsilon > 0$, and n is sufficiently large, Equation (2) has a solution with $\max_i |x_i| \le p^{\epsilon}$. Later, Schmidt [11] showed that for $a_i \in \mathbb{Z}$, $1 \le i \le n$, p a prime, odd $k \ge 3$, $\epsilon > 0$, and a constant $c(k)$ depending only on k, Equation (2) has a solution with

$$\max_i |x_i| \ll_{n,\epsilon} p^{\frac{1}{3}+\sqrt{\frac{c(k)}{n}}+\epsilon}.$$

Baker [1] found that for a natural number m, $\epsilon > 0$, and integers a_i, $1 \le i \le n$, a non-zero solution to the congruence

$$a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv 0 \pmod{m} \tag{3}$$

can be found when

$$\max_i |x_i| < \begin{cases} m^{\frac{1}{2}+\frac{1}{2(n-1)}+\epsilon}, & \text{for } n \ge 4; \\ m^{\frac{2}{3}+\epsilon}, & \text{for } n = 3. \end{cases}$$

In the case of $k = 3$, Dietmann [7] showed that Equation (3) has a solution when

$$\max_i |x_i| \le \begin{cases} m^{\frac{1}{2}+\frac{1}{2n}}, & \text{for } n \text{ odd}; \\ m^{\frac{1}{2}+\frac{1}{2(n-1)}}, & \text{for } n \text{ even}. \end{cases}$$

In [2, Lemma 10.1], Baker further refined his bound on solutions to homogeneous congruences with a composite modulus by proving that for a natural number m, $\epsilon > 0$, integers a_i, $1 \le i \le n$, and $n \ge C(k, \epsilon)$ where $C(k, \epsilon)$ is a constant, Equation (3) has a solution with

$$\max_i |x_i| \le m^{\frac{1}{k}+\epsilon}.$$

This paper uses smooth numbers and a result from the work of Chow, Lindqvist and Prendiville [4] to lower the number of variables needed to establish a solution for Equation (1) with $1 \le x_i \ll_k p^{\frac{1}{k}}$ for $1 \le i \le n$. Using this result we are able to reduce the number of variables needed from $n \ge \frac{3}{2}(k^2 + k + 2)$ to

$$n \ge \frac{3}{2}k(\log k + \log\log k + 2 + O(\log\log k/\log k)).$$

Theorem 1. *For any positive integer k, positive integer n with*

$$n \geq \begin{cases} 9, & \textit{for } k = 2; \\ 12, & \textit{for } k = 3; \\ \frac{3}{2}k(\log\, k + \log\,\log\, k + 2 + O(\log\,\log\, k/\log\, k)), & \textit{for } k \geq 4; \end{cases}$$

prime p, integer c, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq n$, there exists a solution to Equation (1) with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq n$.

2. Preliminary Results

First, we introduce the new result that leads to the reduction in the size of n. For any positive real number η and positive integer B, we define $\mathcal{A} = \mathcal{A}(B, B^\eta)$ to be the set

$$\mathcal{A} := \{x \in [1, B] \cap \mathbb{Z} : p \text{ prime}, p \mid x \text{ implies } p \leq B^\eta\},$$

which we call the set of B^η*-smooth* numbers. Now we are able to state the following theorem, shown by Chow, Lindqvist, and Prendiville [4].

Theorem 2 ([4], Theorem B.1)**.** *Let $c_1, \ldots, c_s \in \mathbb{Z}\backslash\{0\}$ with $\sum_{i \in I} c_i = 0$ for some non-empty subset I of $\{1, 2, \ldots, s\}$. Then, for $k \geq 2$, there exists a positive real number $\eta_0(k)$ and positive integers $s_0(k)$ and $N_0(\underline{c}, \eta, k)$ such that for $0 < \eta \leq \eta_0(k)$, $s \geq s_0(k)$ and $N \geq N_0(\underline{c}, \eta, k)$, we have*

$$\#\left\{\underline{x} \in \mathcal{A}(N, N^\eta)^s : \sum_{i=1}^{s} c_i x_i^k = 0\right\} \asymp_{\underline{c}, \eta, k} N^{s-k}.$$

Moreover, one can take $s_0(2) = 5$, $s_0(3) = 8$, and for $k \geq 4$,

$$s_0(k) = k(\log\, k + \log\,\log\, k + 2 + O(\log\,\log\, k/\log\, k)).$$

Let

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

$$\tilde{N}_{\mathcal{A}^n} := \#\left\{(\underline{x}, \underline{y}) \in \mathcal{A}^n \times \mathcal{A}^n : \sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod p\right\},$$

and

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

We define the *Dickman function*, $\rho(u)$, which is the continuous function on the non-negative real numbers that is uniquely defined by the differential equation $u\rho'(u) = -\rho(u-1)$, with the initial condition that $\rho(u) = 1$ for $u \in [0,1]$.

In the following lemma we will consider the set of B^η-smooth numbers, and we will use the bound

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

which was established by Ramaswami [8].

Let $\eta_0(k)$ and $s_0(k)$ be defined as in Theorem 2. We also define the additive character $e_p(\cdot) = e^{2\pi i(\cdot)/p}$. We can now prove the following lemma.

Lemma 1. *For any positive integers k and n and prime p with $k \geq 2$, $0 < \eta \leq \eta_0(k)$, $2n \geq s_0(k)$, $nB^k \leq p$, and integers a_i with $(a_i, p) = 1$, $1 \leq i \leq n$, we have $|S_{\mathcal{A}^n}| \gg_{k,n,\eta} B^k$.*

Proof. The statement is trivial if B is less than a constant depending only on η and k, so we may assume that B is sufficiently large in terms of η and k, as needed. Using the Cauchy-Schwarz inequality, we see that

$$\begin{aligned}
|\mathcal{A}|^{2n} &= \left(\sum_{z \in S_{\mathcal{A}^n}} \#\left\{\underline{x} \in \mathcal{A}^n : \sum_{i=1}^n a_i x_i^k \equiv z \pmod p\right\}\right)^2 \\
&\leq \left(\sum_{z \in S_{\mathcal{A}^n}} 1\right) \sum_{z \in S_{\mathcal{A}^n}} \left(\#\left\{\underline{x} \in \mathcal{A}^n : \sum_{i=1}^n a_i x_i^k \equiv z \pmod p\right\}\right)^2 \\
&= |S_{\mathcal{A}^n}| N_{\mathcal{A}^n}.
\end{aligned}$$

Thus, we have that $|S_{\mathcal{A}^n}| \geq |\mathcal{A}|^{2n}/N_{\mathcal{A}^n}$.

Now we consider $N_{\mathcal{A}^n}$. Note that, by Hölder's inequality, we have

$$\begin{aligned}
N_{\mathcal{A}^n} &= \frac{1}{p}\sum_{\lambda=1}^p \sum_{\underline{x}, \underline{y} \in \mathcal{A}^n} e_p\left(\lambda\left(\sum_{i=1}^n a_i x_i^k - \sum_{i=1}^n a_i y_i^k\right)\right) \\
&\leq \frac{1}{p}\sum_{\lambda=1}^p \prod_{i=1}^n \left|\sum_{x_i \in \mathcal{A}} e_p(\lambda a_i x_i^k)\right|^2 \\
&\leq \prod_{i=1}^n \left(\frac{1}{p}\sum_{\lambda=1}^p \Big|\sum_{x \in \mathcal{A}} e_p(\lambda a_i x^k)\Big|^{2n}\right)^{1/n}.
\end{aligned}$$

We notice that

$$\frac{1}{p}\sum_{\lambda=1}^p \Big|\sum_{x \in \mathcal{A}} e_p(\lambda a_i x^k)\Big|^{2n}$$

counts the number of solutions to the congruence

$$a_i(x_1^k + \cdots + x_n^k) \equiv a_i(y_1^k + \cdots + y_n^k) \pmod{p}.$$

Since $(a_i, p) = 1$, this is the number of solutions to

$$x_1^k + \cdots + x_n^k \equiv y_1^k + \cdots + y_n^k \pmod{p}. \tag{4}$$

In conclusion, $N_{\mathcal{A}^n} \leq \tilde{N}_{\mathcal{A}^n}$. Since $nB^k \leq p$, any solution to Equation (4) with $1 \leq x_i, y_i \leq B$ is a solution to $x_1^k + \cdots + x_n^k = y_1^k + \cdots + y_n^k$. Thus, we have by Theorem 2 that $\tilde{N}_{\mathcal{A}^n} \ll_{k,n,\eta} B^{2n-k}$, so $N_{\mathcal{A}^n} \ll_{k,n,\eta} B^{2n-k}$. For B sufficiently large, we have that $|\mathcal{A}| > \frac{1}{2}\rho\left(\frac{1}{\eta}\right)B$. Therefore, we find that $|S_{\mathcal{A}^n}| \gg_{k,n,\eta} B^k$. □

We now recall two lemmas from [5]. The first lemma follows from the Cauchy-Davenport Theorem [3,6].

Lemma 2 ([5], Lemma 8.1)**.** *For any prime p and positive integer k, we have $\Gamma(k, p) \leq k$.*

We define the following *sumset* and *product set* notation. For $A, B \subseteq \mathbb{Z}_p$, we use $A + B = \{a + b : a \in A, b \in B\}$ and $AB = \{ab : a \in A, b \in B\}$.

The following lemma is a direct consequence of a result of Sárközy [9, Corollary A].

Lemma 3 ([5], Lemma 8.3)**.** *If A_1, A_2, A_3, and D are subsets of $\mathbb{Z}_p$ with $|A_1||A_2||A_3||D| > p^3$, then $A_1D + A_2 + A_3 = \mathbb{Z}_p$.*

We now have all of the necessary tools to prove Theorem 1.

3. Proof of Theorem 1

Proof of Theorem 1. Let k be a positive integer, and $s_0(k)$, $\eta_0(k)$, and N_0 be as defined in Theorem 2. We may assume that $n = 3\left\lceil \frac{s_0(k)}{2} \right\rceil$ by setting $n - 3\left\lceil \frac{s_0(k)}{2} \right\rceil$ variables equal to arbitrary values in their specified intervals if $n > 3\left\lceil \frac{s_0(k)}{2} \right\rceil$. We note that for $k = 2, 3$, we have

$$3\left\lceil \frac{s_0(2)}{2} \right\rceil = 3\left\lceil \frac{5}{2} \right\rceil = 9 \quad \text{and} \quad 3\left\lceil \frac{s_0(3)}{2} \right\rceil = 3\left\lceil \frac{8}{2} \right\rceil = 12.$$

Let $0 < \eta \leq \eta_0(k)$, p be prime, and c, a_i be integers such that $p \nmid a_i$ for $1 \leq i \leq n$. Set $B = \left\lfloor \left(\frac{3p}{n}\right)^{\frac{1}{k}} \right\rfloor$ and define $m = \left\lceil \frac{s_0(k)}{2} \right\rceil$.

If p is less than the implied constant in $1 \leq x_i \ll_k p^{\frac{1}{k}}$, then the x_i are any elements of the complete residue system modulo p. By Lemma 2, we have that

Equation (1) is solvable. Thus, we may assume that p is larger than any constant depending only on k as needed. In particular, we may assume that $p > \left\lceil \frac{s_0(k)}{2} \right\rceil$, so that $B \geq 1$.

We divide our variables into three sets, each with m elements. Define

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

and define A_2 and A_3 similarly for the variables $x_{m+1}, \ldots, x_{2m}$ and $x_{2m+1}, \ldots, x_{3m}$, respectively. We now apply Lemma 1 with n replaced by m, checking that $mB^k \leq p$ and $2m \geq s_0(k)$ by our definitions of B and m. Since $mB^k \leq p$, it follows from Lemma 1 that there exists a positive constant $c_0(k, \eta)$ with $|A_i| \geq c_0(k, \eta)p$ for $1 \leq i \leq 3$.

We set

$$L = \left\lceil \frac{k}{c_0(k, \eta)^3} \right\rceil$$

and take p to be sufficiently large so that $p > L$. Furthermore, we set $D = \{1^k, 2^k, 3^k, \ldots, L^k\} \subseteq \mathbb{Z}_p$. Note that there are at least L/k distinct values mod p in the set D. Thus, $|A_1||A_2||A_3||D| > p^3$. Therefore, by Lemma 3, $A_1 D + A_2 + A_3 = \mathbb{Z}_p$. It follows that for any integer c, there exists a solution to Equation (1) with $1 \leq x_i \leq LB \ll_k p^{\frac{1}{k}}$. □

References

[1] R. C. Baker, Small solutions of congruences, *Mathematika* **30** (2) (1983), 164-188.

[2] R. C. Baker, *Diophantine Inequalities*, The Clarendon Press, Oxford University Press, New York, 1986.

[3] A. Cauchy, Recherches sur les nombres, *J. Ecole Polytechnique* **9** (1813), 99-116.

[4] S. Chow, S. Lindqvist, and S. Prendiville, Rado's criterion over squares and higher powers, *J. Eur. Math. Soc. (JEMS)* **23** (6) (2021), 1925-1997.

[5] T. Cochrane, M. Ostergaard, and C. Spencer, Solutions to diagonal congruences with variables restricted to a box, *Mathematika* **64** (2) (2018), 430-444.

[6] H. Davenport, On the addition of residue classes, *J. Lon. Math. Soc.* **10** (1) (1935), 30-32.

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

[8] 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.

[9] A. Sárközy, On products and shifted products of residues modulo p, *Integers* **8** (2) (2008), #A9, 8pp.

[10] W. M. Schmidt, Small zeros of additive forms in many variables II, *Acta Math.* **143** (1979), 219-232.

[11] W. M. Schmidt, Small solutions of congruences with prime modulus, in *Diophantine Analysis: Proceedings at the Number Theory Section of the 1985 Australian Mathematical Society Convention*, Cambridge University Press, Cambridge, 1986, 37-66.