32 Èmes Journées Arithmétiques 2023

SOLUTIONS TO POLYNOMIAL CONGRUENCES WITH VARIABLES RESTRICTED TO A BOX

TODD COCHRANE, KONSTANTINOS KYDONIATIS, AND CRAIG SPENCER

Kansas State University

Thursday, 6 July

Introduction

The goal of this talk is to obtain solutions to the congruence

$$f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n) \equiv c \pmod{q}.$$

with the variables restricted to a cube $\mathcal{B}$

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

and optimize the size of B. For convenience we also use the notation $\mathcal{B}(c, B)$ when $c_i = c, \forall i$ and $\mathcal{B}_0 = \mathcal{B}(0, B)$

Theorem

More specifically we obtain the following theorem on the distribution of the solutions.

Theorem

Let q, n, k be a positive integers, c be an integer, and $f_1(x), \ldots, f_n(x) \in \mathbb{Z}[x]$ be polynomials of degree k whose leading coefficients are relatively prime to q. Suppose that for $1 \leq i \leq n$ and $p \mid q$ with p prime, $f_i(x)$ is not constant modulo p.There exists a constant $N(k)$ such that if $n > N(k)$ and $\mathcal{B}$ is a cube of side length $B > \max\{q^{1/k}, k\}$, then there is a solution of the congruence

$$\sum_{i=1}^{n} f_i(x_i) \equiv c \pmod{q}$$ *in $\mathcal{B}$.*

Quality of the bound

This theorem is a generalization of the work of T.Cochrane, M. Ostergaard, and C. Spencer, which handles the case where each $f_i(x)$ is of the form $a_i x^k$ with $(a_i, q) = 1$. This is similar to how various authors have studied a generalized Waring problem that allows for polynomial summands; see for instance the work of Kamke, Hua, Načaev, Wooley, and Ford.

The theorem is best possible up to the determination of $N(k)$ and improvement in the constant 1 in front of $q^{1/k}$.

Quality of the bound

This theorem is a generalization of the work of T.Cochrane, M. Ostergaard, and C. Spencer, which handles the case where each $f_i(x)$ is of the form $a_i x^k$ with $(a_i, q) = 1$. This is similar to how various authors have studied a generalized Waring problem that allows for polynomial summands; see for instance the work of Kamke, Hua, Načaev, Wooley, and Ford.

The theorem is best possible up to the determination of $N(k)$ and improvement in the constant 1 in front of $q^{1/k}$.

Indeed, consider the congruence

$$x_1^k + \cdots + x_n^k \equiv \lceil q/2 \rceil \pmod{q},$$

and box $\mathcal{B}$ with $1 \le x_i \le B$, $1 \le i \le n$. Plainly with $n = N(k)$ we will need $B \gg_k q^{1/k}$ in order to solve this congruence. In the statement of the theorem, the condition that $f_i(x)$ is not constant modulo p is equivalent to requiring that $(x^p - x) \nmid (f_i(x) - f_i(0))$ over $(\mathbb{Z}/p\mathbb{Z})[x]$.

General Upper Bound

Crucial to the proof, is an upper bound for the number of the solutions of

$$f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n) \equiv c \pmod{q}.$$

We denote that number as $N_q(\mathcal{B})$.

General Upper Bound

Crucial to the proof, is an upper bound for the number of the solutions of

$$f_1(x_1) + f_2(x_2) + \cdots + f_n(x_n) \equiv c \pmod{q}.$$

We denote that number as $N_q(\mathcal{B})$.

Theorem

Let q, n, k be a positive integers, c be an integer, and $f_1(x), \ldots, f_n(x) \in \mathbb{Z}[x]$ be degree-k polynomials whose leading coefficients are relatively prime to q. Suppose $n \geq k^2 + k + 2$ and $\mathcal{B}$ be is a cube of edge length $B \leq q$. Then

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

Proof of the Upper Bound

For the proof of this theorem the following notation will be used. 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 $S_1, \ldots, S_{2n}$ of $\mathbb{Z}_q$, put $\mathcal{S} = S_1 \times \cdots \times S_n$. Define

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

along with $\mathcal{T} = S_1 \times \cdots \times S_{2n}$ and $\mathcal{S}_i^n$ to be the cartesian product of S_i with itself n times. We begin the proof of the theorem with the following lemma.

Proof of the Upper Bound

For the proof of this theorem the following notation will be used. 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 $S_1, \ldots, S_{2n}$ of $\mathbb{Z}_q$, put $\mathcal{S} = S_1 \times \cdots \times S_n$. Define

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

along with $\mathcal{T} = S_1 \times \cdots \times S_{2n}$ and $\mathcal{S}_i^n$ to be the cartesian product of S_i with itself n times. We begin the proof of the theorem with the following lemma.

Lemma

Let q, n, k be a positive integers, c be an integer, and $f_1(x), \ldots, f_{2n}(x) \in \mathbb{Z}[x]$ be degree-k polynomials whose leading coefficients are relatively prime to q. Then

$$\#\Big\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} f_i(x_i) \equiv c \pmod q\Big\} \leq \prod_{i=1}^{2n} I_{n,k,f_i}(\mathcal{S}_i^n)^{\frac{1}{2n}}.$$

Proof of Lemma

Proof.

We have

$$\#\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} f_i(x_i) \equiv c \pmod{q}\} = \frac{1}{q} \sum_{\underline{x} \in \mathcal{T}} \sum_{\lambda=1}^{q} e_q\left(\lambda\left(\sum_{i=1}^{2n} f_i(x_i) - c\right)\right)$$

$$\leq \frac{1}{q} \sum_{\lambda=1}^{q} \left| e_q(-\lambda c) \prod_{i=1}^{2n} \sum_{x_i \in S_i} e_q\left(\lambda f_i(x_i)\right) \right|$$

$$\leq \frac{1}{q} \left[\sum_{\lambda=1}^{q} \left| \sum_{x_1 \in S_1} e_q(\lambda f_1(x_1)) \right|^{2n}\right]^{\frac{1}{2n}} \cdots \left[\sum_{\lambda=1}^{q} \left| \sum_{x_{2n} \in S_{2n}} e_q(\lambda f_{2n}(x_{2n})) \right|^{2n}\right]^{\frac{1}{2n}},$$

by Hölder's inequality. □

Proof.

Now, for $1 \le i \le n$, the sum

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

is q times the number of solution of the congruence

$$f_i(x_1) + \cdots + f_i(x_n) \equiv f_i(y_1) + \cdots + f_i(y_n) \pmod{q},$$

with variables restricted to S_i. Therefore,

$$\#\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} f_i(x_i) \equiv c \pmod{q}\} \le \frac{1}{q} \prod_{i=1}^{2n} (q I_{n,k,f_i}(S_i^n))^{\frac{1}{2n}} = \prod_{i=1}^{2n} I_{n,k,f_i}(S_i^n)^{\frac{1}{2n}}.$$

□

Relating $I_{n,k,f}(\mathcal{B})$ to $J_{n,k}(B)$ and $J^*_{n,k}(B)$

A bound will be acquired for $I_{n,k,f}(\mathcal{B})$ with the help from bounds of $J_{n,k}(B)$ the number of solutions to the system of congruences

$$\begin{aligned} x_1 + \cdots + x_n &\equiv y_1 + \cdots + y_n \pmod q, \\ x_1^2 + \cdots + x_n^2 &\equiv y_1^2 + \cdots + y_n^2 \pmod q, \\ &\vdots \\ x_1^k + \cdots + x_n^k &\equiv y_1^k + \cdots + y_n^k \pmod q \end{aligned} \tag{1}$$

with $(\underline{x}, \underline{y}) \in \mathcal{B}_0 \times \mathcal{B}_0$. Those are achieved utilizing known results for $J^*_{n,k}(B)$, the number of solutions of the same system over the integers .

More specifically

Lemma

For any positive integers B, n, k, q *with* $B \leq q$*, integer* c*, cube* $\mathcal{B}(c, B)$ *of the aforementioned shape, and polynomial* $f(x) = \alpha_k x^k + \cdots + \alpha_0 \in \mathbb{Z}[x]$ *with* $(\alpha_k, q) = 1$*, we have*

$$I_{n,k,f}(\mathcal{B}) \leq (2n)^{k-1} B^{\frac{k(k-1)}{2}} J_{n,k}(B).$$

The fundamental idea of the proof is that the congruence we are interested in satisfies a system of equations whose number of solutions is bounded by $J_{n,k}(B)$.

More specifically

Lemma

For any positive integers B, n, k, q with $B \leq q$, integer c, cube $\mathcal{B}(c, B)$ of the aforementioned shape, and polynomial $f(x) = \alpha_k x^k + \cdots + \alpha_0 \in \mathbb{Z}[x]$ with $(\alpha_k, q) = 1$, we have

$$I_{n,k,f}(\mathcal{B}) \leq (2n)^{k-1} B^{\frac{k(k-1)}{2}} J_{n,k}(B).$$

The fundamental idea of the proof is that the congruence we are interested in satisfies a system of equations whose number of solutions is bounded by $J_{n,k}(B)$. That is:

$$\begin{aligned} (x_1 - c) + \cdots + (x_n - c) &\equiv (y_1 - c) + \cdots + (y_n - c) + h_1 \pmod{q} \\ &\vdots \\ (x_1 - c)^{k-1} + \cdots + (x_n - c)^{k-1} &\equiv (y_1 - c)^{k-1} + \cdots + (y_n - c)^{k-1} + h_{k-1} \pmod{q} \\ f(x_1) + \cdots + f(x_n) &\equiv f(y_1) + \cdots + f(y_n) \pmod{q} \end{aligned} \tag{2}$$

with $(\underline{x}, \underline{y}) \in \mathcal{B} \times \mathcal{B}$

Proof of 4

The number of solutions, $N(\underline{h})$, of the previous system, is bounded from above by the case were all the $h_j = 0$. This follows by applying the triangle inequality to the exponential sum representation for the number of solutions of the system,

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

By a change of variables $x_i \to x_i + c, y_i \to y_i + c$, $N(\underline{0})$ equals the number of solutions of the system of congruences

$$
\begin{gathered}
x_1 + \cdots + x_n \equiv y_1 + \cdots + y_n \pmod q \\
\vdots \\
x_1^{k-1} + \cdots + x_n^{k-1} \equiv y_1^{k-1} + \cdots + y_n^{k-1} \pmod q \\
f(x_1 + c) + \cdots + f(x_n + c) \equiv f(y_1 + c) + \cdots + f(y_n + c) \pmod q,
\end{gathered}
$$

with $(\underline{x}, \underline{y}) \in \mathcal{B}_0 \times \mathcal{B}_0$.

By a change of variables $x_i \to x_i + c, y_i \to y_i + c$, $N(\underline{0})$ equals the number of solutions of the system of congruences

$$\begin{gathered} x_1 + \cdots + x_n \equiv y_1 + \cdots + y_n \pmod q \\ \vdots \\ x_1^{k-1} + \cdots + x_n^{k-1} \equiv y_1^{k-1} + \cdots + y_n^{k-1} \pmod q \\ f(x_1 + c) + \cdots + f(x_n + c) \equiv f(y_1 + c) + \cdots + f(y_n + c) \pmod q, \end{gathered}$$

with $(\underline{x}, \underline{y}) \in \mathcal{B}_0 \times \mathcal{B}_0$.
By the Binomial Theorem, the congruence

$$f(x_1 + c) + \cdots + f(x_n + c) \equiv f(y_1 + c) + \cdots + f(y_n + c) \pmod q$$

can be replaced with

$$x_1^k + \cdots + x_n^k \equiv y_1^k + \cdots + y_n^k \pmod q.$$

since the leading coefficients are relatively prime to q. The proof is complete by taking into account the contribution of all possible options for the h_i .
Therefore, $N(h_1, \ldots, h_{k-1}) \leq N(\underline{0}) \leq J_{n,k}(B)$ uniformly.

Correlation of $J_{n,k}(B)$ and $J^*_{n,k}(B)$

By results of Cochrane, Ostergaard, and Spencer, which relates $J_{n,k}(B)$ to $J^*_{n,k}(B)$, the following bound is immediate.

Lemma

For any positive integers B, n, k, q with $B \leq q$, integer c, cube $\mathcal{B}(c, B)$, and polynomial $f(x) = \alpha_k x^k + \cdots + \alpha_0 \in \mathbb{Z}[x]$ with $(\alpha_k, q) = 1$, we have

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

Bounds for $J^*_{n,k}(B)$

The task of estimating $J^*_{n,k}(B)$ has been a central problem in additive number theory since Vinogradov's seminal work on Waring's problem. By the recent work of Bourgain, Demeter, and Guth and Wooley, there exists a positive constant $c_1(n,k)$ such that for $n > \frac{1}{2}k(k+1)$, one has

$$J^*_{n,k}(B) \leq c_1(n,k)B^{2n-\frac{1}{2}k(k+1)}.$$

Here is where the condition $n \geq k^2+k+2$ stems from. Combining this result with the previous upper bound for $I_{n,k,f}(\mathcal{B})$, we obtain the following upper bound.

Finalizing the proof of the upper bound

Proposition

For any positive integers B, n, k, q with $B \leq q$ and $n > \frac{1}{2}k(k+1)$, integer c, cube $\mathcal{B}(c, B)$, and polynomial $f(x) = \alpha_k x^k + \cdots + \alpha_0 \in \mathbb{Z}[x]$ with $(\alpha_k, q) = 1$, we have

$$I_{n,k,f}(\mathcal{B}) \leq 5\ c_1(n,k)(2n)^k \left(\frac{B^{2n}}{q} + \frac{1}{2n} B^{2n-k} \right).$$

where $c_1(n,k)$ is the positive constant appearing in the previous bound.

The proof of upper bound for the number of the solutions is now complete if one combines the above proposition with a previous lemma.

The value set of $\sum_{i=1}^{n} f_i(x_i)$

The reason we we went through the trouble of proving this upper bound was to show that the value set of a sum of such polynomials is of comparable size to the size of the modulus. Specifically

Lemma

For any positive integers k, n, B, q with $n \geq \frac{1}{2}(k^2 + k + 2)$, cube $\mathcal{B}$ with side length $B > q^{1/k}$, and polynomials $f_1(x), \ldots, f_n(x) \in \mathbb{Z}[x]$ of degree k whose leading coefficients are relatively prime to q, we have

$$S_{\mathcal{B}} := \left\{ \sum_{i=1}^{n} f_i(x_i) \in \mathbb{Z}_q : \underline{x} \in \mathcal{B} \right\}, \quad |S_{\mathcal{B}}| \gg_k q.$$

The value set of $\sum_{i=1}^{n} f_i(x_i)$

The reason we we went through the trouble of proving this upper bound was to show that the value set of a sum of such polynomials is of comparable size to the size of the modulus. Specifically

Lemma

For any positive integers k, n, B, q with $n \geq \frac{1}{2}(k^2 + k + 2)$, cube $\mathcal{B}$ with side length $B > q^{1/k}$, and polynomials $f_1(x), \ldots, f_n(x) \in \mathbb{Z}[x]$ of degree k whose leading coefficients are relatively prime to q, we have

$$S_{\mathcal{B}} := \left\{ \sum_{i=1}^{n} f_i(x_i) \in \mathbb{Z}_q : \underline{x} \in \mathcal{B} \right\}, \quad |S_{\mathcal{B}}| \gg_k q.$$

The proof is entirely based on the relationship $|S_{\mathcal{B}}| \geq B^{2n}/N_q(\mathcal{B} \times \mathcal{B})$ and the theorem that provided the upper bound for $N_q(\mathcal{B} \times \mathcal{B})$.

In order to prove our theorem, the variant of the Cauchy-Davenport Theorem by Cochrane, Ostergaard, and Spencer, is used.

Theorem

Let $n \geq 1$ and $A_1, \ldots, A_r$ be finite, nonempty subsets of an abelian group G, such that no A_i is contained in a coset of a proper subgroup of G. Then

$$|A_1 + \cdots + A_r| \geq \min\left\{|G|, \left(\tfrac{1}{2} + \tfrac{1}{2r}\right)\sum_{i=1}^{r} |A_i|\right\}.$$

In order to prove our theorem, the variant of the Cauchy-Davenport Theorem by Cochrane, Ostergaard, and Spencer, is used.

Theorem

Let $n \geq 1$ and $A_1, \ldots, A_r$ be finite, nonempty subsets of an abelian group G, such that no A_i is contained in a coset of a proper subgroup of G. Then

$$|A_1 + \cdots + A_r| \geq \min\left\{|G|, \left(\tfrac{1}{2} + \tfrac{1}{2r}\right)\sum_{i=1}^{r}|A_i|\right\}.$$

Let $A_1, \ldots, A_r$ be value sets of the type $S_{\mathcal{B}}$. Then since we have shown that such sets are of size $\geq \frac{q}{w_k}$ we only need to calculate r, as long as they are not contained in a coset of a proper subgroup.

In order to prove our theorem, the variant of the Cauchy-Davenport Theorem by Cochrane, Ostergaard, and Spencer, is used.

Theorem

Let $n \geq 1$ and $A_1, \ldots, A_r$ be finite, nonempty subsets of an abelian group G, such that no A_i is contained in a coset of a proper subgroup of G. Then

$$|A_1 + \cdots + A_r| \geq \min\left\{|G|, \left(\tfrac{1}{2} + \tfrac{1}{2r}\right)\sum_{i=1}^{r} |A_i|\right\}.$$

Let $A_1, \ldots, A_r$ be value sets of the type $S_{\mathcal{B}}$. Then since we have shown that such sets are of size $\geq \frac{q}{w_k}$ we only need to calculate r, as long as they are not contained in a coset of a proper subgroup.
A necessary and sufficient condition for $S_{\mathcal{B}}$ to be contained in such a coset is that there is prime $p|q$ such that polynomials are constant mod p on the edge of our cube.

Proof of the Main Theorem

Proof.

Let $B > \max\{q^{1/k}, k\}$ and let p be any prime divisor of q. If $p \leq B$, every edge contains a full set of residues mod p so $f_i(x_i)$ takes on at least two distinct values mod p; since by assumption the polynomial is not constant $mod p$. On the other hand, if $p > B$, then for fixed a, the congruence $f_i(x_i) \equiv a \pmod{p}$ has at most $k < B$ solutions on the edge $[c_i + 1, c_i + B]$, and so again $f_i(x_i)$ takes on at least two distinct values mod p on each edge. Thus sets of the type $S_{\mathcal{B}}$ are not contained in a coset of a proper subgroup of $\mathbb{Z}_q$.

Proof of the Main Theorem

Proof.

Let $B > \max\{q^{1/k}, k\}$ and let p be any prime divisor of q. If $p \leq B$, every edge contains a full set of residues mod p so $f_i(x_i)$ takes on at least two distinct values mod p; since by assumption the polynomial is not constant $mod p$. On the other hand, if $p > B$, then for fixed a, the congruence $f_i(x_i) \equiv a \pmod{p}$ has at most $k < B$ solutions on the edge $[c_i + 1, c_i + B]$, and so again $f_i(x_i)$ takes on at least two distinct values mod p on each edge. Thus sets of the type $S_{\mathcal{B}}$ are not contained in a coset of a proper subgroup of $\mathbb{Z}_q$.

According to what was mentioned earlier it follows that for $r \geq 2w_k - 1$, we have $A_1 + \cdots + A_r = \mathbb{Z}_q$. Set $r = \lceil 2w_k \rceil - 1$. If we start with a form in at least $\frac{1}{2}(k^2 + k + 2)r$ variables, we may partition the variables into r disjoint sets, each with at least $\frac{1}{2}(k^2 + k + 2)$ variables, and form r value sets $A_1, \ldots, A_r$ of the type $S_{\mathcal{B}}$, with $A_1 + \cdots + A_r = \mathbb{Z}_q$, completing the proof. □

Thank you!

[1] J. Bourgain, C. Demeter, L. Guth, *Proof of the Main Conjecture in Vinogradov's Mean Value Theorem for Degrees Higher Than Three*, Ann. of Math. 184(2) (2016), 633–682.

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

[3] ______, *Cauchy-Davenport theorem for Abelian groups and diagonal congruences*, Proc. Amer. Math. Soc. 147 (2019), 3339–3345.

[4] K. Ford, *Waring's problem with polynomial summands*, J. London Math. Soc. 61 (2000), 671–680.

[5] L.-K. Hua, *On Waring's problem with polynomial summands*, Amer. J. Math. 58 (1936), 553–562.

[6] ______, *On a generalized Waring problem*, Proc. London Math. Soc. (2) 43 (1937), 161–182.

[7] ______, *On a generalized Waring problem II*, J. Chinese Math. Soc. 2 (1940), 175–191.

[8] E. Kamke, *Verallgemeinerungen des Waring'Hilbertschen Satzes*, Math. Ann. 83 (1921), 85–112.

[9] V. I. Načaev, *Waring's problem for polynomials*, Amer. Math. Soc. Transl. 3 (1956), 39–89.

[10] I. M. Vinogradov, *New estimates for Weyl sums*, Dokl. Akad. Nauk SSSR 8 (1935), 195–198.

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

[12] ______, *Nested efficient congruencing and relatives of Vinogradov's mean value theorem*, Proc. Lond. Math. Soc. 118 (2019), 942–1016.