SOLUTIONS OF DIAGONAL CONGRUENCES WITH VARIABLES RESTRICTED TO A BOX

by

MISTY OSTERGAARD

B.A., Washburn University, 2009

B.S., Washburn University, 2010

M.S., Kansas State University, 2013

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Abstract

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

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{p}$$

in any cube

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

of side length $B \geq p^{\frac{1}{k}+\varepsilon}$.

We further prove that for any positive integer k there exists a constant $c(k)$ such that for any positive integer $n \geq 3(k^2+k+1)$, prime p, and integers a_i with $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution of

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{p}$$

with $1 \leq x_i \leq c(k)p^{\frac{1}{k}}$.

We also prove that for any positive integer k, there exists a constant $c(k)$ such that for any positive integers n, q with $n > c(k)$ and cube

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

with side length $B \geq (q/k^2)^{1/k}$, such that for any prime factor p of q, the k-th powers $\pmod{p}$ are not constant on any edge $[c_i + 1, c_i + B]$ of $\mathcal{B}$, there exists a solution in $\mathcal{B}$ of the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{q}.$$

Solutions of Diagonal Congruences with Variables Restricted to a Box

by

Misty Ostergaard

B.A., Washburn University, 2009

B.S., Washburn University, 2010

M.S., Kansas State University, 2013

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas

2016

Approved by:

Co-Major Professor
Todd Cochrane

Approved by:

Co-Major Professor
Craig Spencer

Abstract

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

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{p}$$

in any cube

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

of side length $B \geq p^{\frac{1}{k}+\varepsilon}$.

We further prove that for any positive integer k there exists a constant $c(k)$ such that for any positive integer $n \geq 3(k^2 + k + 1)$, prime p, and integers a_i with $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution of

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{p}$$

with $1 \leq x_i \leq c(k) p^{\frac{1}{k}}$.

We also prove that for any positive integer k, there exists a constant $c(k)$ such that for any positive integers n, q with $n > c(k)$ and cube

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

with side length $B \geq (q/k^2)^{1/k}$, such that for any prime factor p of q, the k-th powers $\pmod{p}$ are not constant on any edge $[c_i + 1, c_i + B]$ of $\mathcal{B}$, there exists a solution in $\mathcal{B}$ of the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod{q}.$$

Table of Contents

Acknowledgments

I have had the pleasure of working with all three of the number theorists at Kansas State University, Professors Todd Cochrane, Craig Spencer, and Chris Pinner. All three of you were incredibly helpful, friendly, patient, supportive, and generous with your time. Thank you so much for everything! The work in this thesis represents joint work with my advisors Professors Cochrane and Spencer, to whom I am hugely indebted for all of their guidance and helpful comments.

I especially would like to thank my best friend and husband, Andrew Ostergaard. You have helped me more than I think you know, and I will be eternally grateful that you will be a part of my life.

Thank you to all of the faculty and staff in the Department of Mathematics at Kansas State University for your support and guidance during my graduate career. I especially want to express my gratitude to Professors Bob Burckel, Dan Volok, and Alexander Rosenberg who each helped me a great deal throughout my time at Kansas State University.

I also want to say thank you to some wonderful friends and collegues. Vincent Pigno and Badria Alsulmi, you two helped me learn so much about number theory, and you were both so easy and fun to work with. I learned a lot from my fellow graduate students Hui Chen, Nhan Tran, Xiaojin Ye, and Ben Larkin. Thank you for being great study partners and teachers. I am greatly appreciative of Hope Sneddon, Ana Luiza de Campos Paula, Luciana Signorelli, Ana Claudia Sant Anna, Omer Farooq, Data Mania, Mikhail Makouski, and Arjun Nepal for their friendship, support, and delightful conversations.

I would like to thank the other members of my committee, Professors Haiyan Wang and Anh-Thu Le, for their time, comments, and thoughtful questions.

Finally, I owe a huge debt of gratitude to my family for their support throughout my time working on this thesis and for all of the time before that when they were helping me get to where I am today.

Dedication

This thesis is dedicated to two of my biggest supporters, my mom and dad.

Chapter 1

Introduction

The main goal of this thesis is to find the minimal $B \in \mathbb{N}$ such that any cube

$$\mathcal{B} = \mathcal{B}(\mathbf{d}, B) := \{\underline{x} \in \mathbb{Z}^n : d_i + 1 \leq x_i \leq d_i + B, 1 \leq i \leq n\} \tag{1.1}$$

of side length B contains a solution of the congruence

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_n x_n^k \equiv c \pmod{q}. \tag{1.2}$$

Here, we let $d_i, a_i, c \in \mathbb{Z}$ for $1 \leq i \leq n$ and $(a_i, q) = 1$ for $1 \leq i \leq n$. Of particular interest are solutions with

$$\|\underline{x}\| := \max |x_i|$$

as small as possible.

1.1 History of the Problem

The main theorems in this thesis are motivated by the classical Waring Problem, stated here:

For a given $k \in \mathbb{N}$, is there a value n such that every $c \in \mathbb{N}$ may be written as

$$c = x_1^k + x_2^k + \cdots + x_n^k$$

for nonnegative integers $x_i, 1 \leq i \leq n$?

In 1909, Hilbert proved that such an n does exist:

Theorem 1.1.1 (Hilbert-Waring Theorem)**.** *For a fixed $k \in \mathbb{N}$, there is a number n such that every natural number can be expressed as a sum of at most n k^{th} powers of positve integers.*

Of particular interest is determining the minimal value of n given the degree k.

One of the most well-known results on Waring's Problem is Lagrange's Four Squares Theorem—that every natural number can be expressed as a sum of at most four squares. We also now know that every natural number can be expressed as a sum of at most nine cubes thanks to Wieferich and Kempner [34, 21] and as a sum of at most nineteen fourth powers due to Balasubramanian, Deshouillers, and Dress [6, 7].

We consider next Waring's Problem $\pmod{q}$ for a natural number q. For this task, we define $\gamma := \gamma(k, q)$ to be the smallest value n such that every integer c can be written as a sum of n k^{th} powers of integers $\pmod{q}$, that is,

$$c \equiv x_1^k + x_2^k + \cdots + x_n^k \pmod{q}.$$

Using the Chinese Remainder Theorem, one can show that if q has prime power factorization $q = \prod_{i=1}^{j} p_i^{\ell_i}$, then $\gamma(k, q)$ can be described by $\gamma(k, q) = \max_{1 \leq i \leq j} \gamma(k, p_i^{\ell_i})$; we prove this in Corollary 2.4.1. Thus, to find the value of $\gamma(k, q)$, we need only know $\gamma(k, \cdot)$ on prime powers. Hardy and Littlewood proved that for any prime power $p^t, t \in \mathbb{N}$, $\gamma(k, p^t) \leq 4k$, and $\gamma(k, p^t) \leq \frac{p}{p-1}k + 1$ for p odd. Thus, for any natural number $\pmod{q}$, $\gamma(k, q) \leq 4k$.

We may generalize Waring's Problem further by not only considering congruences $\pmod{q}$, but also allowing the k^{th} powers to have integer coefficients.

Definition 1.1.1. *Let $\Gamma(k, q)$ be the minimal n (should it exist) such that for any integers a_i with $(a_i, q) = 1, 1 \leq i \leq n$, and any integer c, the congruence*

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_n x_n^k \equiv c \pmod{q}$$

is solvable in integers $x_i, 1 \leq i \leq n$.

When all of the $a_i = 1$ this is just Waring's Problem $\pmod{q}$. We will show in Chapter 2.6, Theorem 2.6.1, that for any positive integers k, q, we have that $\Gamma(k, q) \leq 4k$, thus generalizing the result of Hardy and Littlewood, stated above. The hypothesis that $(a_i, q) = 1$ is natural to impose; otherwise, the congruence reduces to one in fewer variables for certain prime divisors of q.

1.2 Previous Results

The goal of this thesis is not merely to obtain the existence of solutions of (1.2), but rather to obtain solutions with the x_i restricted to a cube $\mathcal{B}$ as in (1.1). Of particular interest is to find small integer solutions to the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{q} \tag{1.3}$$

with $k, q \in \mathbb{N}$ and $a_i, c \in \mathbb{Z}$, $(a_i, q) = 1, 1 \leq i \leq n$. We say the congruence is homogeneous if $c = 0$. By small we mean $\|\underline{x}\| := \max|x_i| \leq \xi q^\lambda$ 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 $\mathcal{B} := \{\underline{x} : d_i + 1 \leq x_i \leq d_i + B, 1 \leq i \leq n\}$ with $d_i \in \mathbb{Z}$ for $1 \leq i \leq n$, contains a solution of (1.8).

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

As we shall see, by restricting our attention to a prime modulus or to a homogeneous congruence, one can often get much stronger results. For instance, Schmidt in [27, Equation (4.1)] proved that for k odd, $\varepsilon > 0$, and n sufficiently large, there exists a nonzero solution to the homogeneous congruence with prime modulus such that $\|\underline{x}\| \ll p^\varepsilon$. (See Section 2.1 for information on the Vinogradov notation, $f(x) \ll g(x)$.) 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.

R. Baker [4] and Dietmann [16] proved results in the homogeneous case for a composite modulus. In particular, Baker proved in [4, Theorem 1] that for any $\varepsilon > 0$, $q \in \mathbb{N}$, and integers $a_1, a_2, \ldots, a_n$, there is a nonzero solution of

$$a_1x_1^k + \cdots + a_nx_n^k \equiv 0 \pmod{q}$$

with

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

Dietmann [16] made an improvement for cubic congruences. He proved that for $a_1, \ldots, a_n \in \mathbb{Z}$, $n \geq 3$, and $q \in \mathbb{N}$, there is a nonzero solution of the congruence

$$a_1x_1^3 + \cdots + a_nx_n^3 \equiv 0 \pmod{q}$$

with

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

Cochrane [11, Equation (2.33), Example 4.8.14] considered a non-homogeneous congruence with prime modulus. He proved that for $k, n \in \mathbb{N}$, any prime p, and $a_i, c \in \mathbb{Z}$, with $p \nmid a_i$, $1 \leq i \leq n$, and $p \nmid c$, the diagonal congruence (1.3) with $q = p$ has a solution in any cube of side length B for which

$$B \gg_{k,n} p^{\frac{1}{2}+\frac{1}{2n}}. \tag{1.4}$$

For $c = 0$ and $n \geq 3$, the same result holds (as seen in [11, Theorem 4.7.13]) with

$$B \gg_{k,n} p^{\frac{1}{2}+\frac{1}{2(n-1)}}.$$

In [29, Theorem 3], Schmidt proved that for p a prime, k odd, $\varepsilon > 0$, and $a_i \in \mathbb{Z}$ with $p \nmid a_i$, $1 \le i \le n$, the congruence

$$\sum_{i=1}^{n} a_i x_i^k \equiv 0 \pmod{p}$$

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

$$\|\underline{x}\| \ll_{n,\varepsilon} p^{\frac{1}{3}+\frac{c(k)}{\sqrt{n}}+\varepsilon} \tag{1.5}$$

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

Applying a result of Schmidt [28, Theorem 3], Cochrane [11, Cor. 5.7] showed that for $k \ge 2$, there exists a solution to (1.3) when $q = p$ for arbitrary c in any cube with side length

$$B \gg_{\varepsilon,k,n} p^{\frac{1}{k}+\frac{1}{n}(1-\frac{1}{k})2^k\Phi(k)+\varepsilon} \tag{1.6}$$

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, there is a $\Phi(k) < (\log 2)^{-k} k!$ that one can take.

R. Baker proved in [5, Lemma 10.1] that for $q \in \mathbb{N}$, $a_i \in \mathbb{Z}$, $1 \le i \le n$, and $n \ge C(k, \varepsilon)$, there exist non-negative integers $x_1, \ldots, x_n$ satisfying

$$\sum_{i=1}^{n} a_i x_i^k \equiv 0 \pmod{q}$$

with

$$\|\underline{x}\| \le q^{\frac{1}{k}+\varepsilon}, \tag{1.7}$$

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

1.3 Main Results of This Thesis

We will highlight four of the main results in this thesis. In the first two theorems, we consider the case of a prime modulus with arbitrary c,

$$\sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{p}. \tag{1.8}$$

The first theorem deals with finding solutions in a general cube

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : d_i + 1 \leq x_i \leq d_i + B, 1 \leq i \leq n\} \tag{1.9}$$

of side length B.

Theorem 1.3.1. *For $k \geq 2$, $0 < \varepsilon < \frac{1}{k(k-1)}$, $n > \frac{k-1}{\varepsilon}$, prime $p > P(\varepsilon, k)$, and integers a_i, $0 \leq i \leq n$, with $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution $\underline{x}$ to the congruence (1.8) in any cube $\mathcal{B}$ of type (1.9) of side length $B \geq p^{\frac{1}{k}+\varepsilon}$.*

We deduce this theorem, given in Chapter 3, from Theorem 3.0.3 whose proof makes use of exponential sums and Weyl-type estimates. We note that the size of the cube given by the theorem is optimal up to removal of the epsilon.

The next three theorems deal with finding small solutions of (1.8).

Theorem 1.3.2. *For any positive integer k there exists a constant $c(k)$ such that for any positive integer $n \geq \frac{3}{2}(k^2 + k + 2)$, prime p, and integers a_i with $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution of (1.8) with $1 \leq x_i \leq c(k)p^{\frac{1}{k}}$.*

The proof of this theorem, given in Chapter 4, makes use of the Vinogradov Mean Value Theorem. We note that this result is best possible up to the determination of the constant $c(k)$. Ideally, we would like to obtain the same result for smaller values of n and for a cube in general position. While we have not achieved that, we do have the following two results for smaller values of n.

Theorem 1.3.3. *For $k \geq 2$ 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 $p \nmid a_i$, $1 \leq i \leq n$, there exists a nonzero solution $\underline{x}$ to (1.8) with*

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

Here, $\gamma = \gamma(\varepsilon, k)$ is the same constant as in Lemma 3.3.1.

The proof of Theorem 1.3.3 is given in Section 3.3.

Theorem 1.3.4. *For any positive $\varepsilon < 1$, $k \geq 4$, $n > \frac{3}{2}k\log(3e/\varepsilon) + 3$, prime p, and integers a_i, $0 \leq i \leq n$ with $p \nmid a_i$, $1 \leq i \leq n$, there is a solution of (1.8) with*

$$1 \leq x_i \ll_{\varepsilon,n,k} p^{\frac{1}{k}+\varepsilon}, \qquad 1 \leq i \leq n. \tag{1.10}$$

The proof of this theorem, given in Chapter 4, involves additive combinatorics and results in a solution in which all of the variables are smooth numbers (discussed in Section 4.8).

In contrast to the previous results, the next theorem pertains to the composite modulus case.

Theorem 1.3.5. *For any positive integer k, there exists a constant $c(k)$ such that for any positive integers n, q with $n > c(k)$ and cube $\mathcal{B}$ of type (1.9) with side length $B \geq (q/k^2)^{1/k}$, such that for any prime factor p of q, the k^{th} powers $\pmod p$ are not constant on any edge $[c_i + 1, c_i + B]$ of $\mathcal{B}$ and $a_i \in \mathbb{Z}$ with $(a_i, q) = 1, 1 \leq i \leq n$, there exists a solution in $\mathcal{B}$ of the congruence*

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

We note the necessity of the additional hypothesis in our theorem, "for any prime factor p of q, the k^{th} powers $\pmod p$ are not constant on any edge $[c_i + 1, c_i + B]$ of $\mathcal{B}$." If the k^{th} powers are constant on an edge of $\mathcal{B}$, then we are essentially dealing with a congruence in fewer variables. Indeed, in the worst case, the congruence may not be solvable at all, no matter how many variables we use. We give such an example in Section 2.3. Once again, we have obtained an optimal result up to the determination of $c(k)$.

Chapter 2

Preliminary Information

2.1 Vinogradov Notation

When we write

$$f(x) \ll_t g(x)$$

we mean that for all x,

$$|f(x)| \leq c(t)|g(x)|$$

for some constant $c(t)$ depending only on t. In particular, $f(x) \ll g(x)$ means $|f(x)| \leq c|g(x)|$ for some absolute constant c.

2.2 Modular Arithmetic

Definition 2.2.1. *For a positive integer q and $a, b \in \mathbb{Z}$, if $q|(a-b)$ we say that a is congruent to b modulo q and write $a \equiv b \pmod{q}$.*

Notice that the following are equivalent for integers a, b and positive integer q:

- $a \equiv b \pmod{q}$,
- $a = b + tq$ for some integer t, and

- a and b have the same remainder when divided by q.

Lemma 2.2.1. *For all $a, b, x, y \in \mathbb{Z}$, if $x \equiv y \pmod{ab}$, then $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$.*

Proof. Suppose $x \equiv y \pmod{ab}$. By definition, this is equivalent to $ab|(x-y)$. Thus, both a and b divide $(x-y)$. Hence, $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$. □

Lemma 2.2.2. *If $(a, b) = 1$ (i.e. $\gcd(a, b) = 1$), $x \equiv y \pmod{a}$, and $x \equiv y \pmod{b}$, then $x \equiv y \pmod{ab}$.*

Proof. Since $x \equiv y \pmod{a}$ and $x \equiv y \pmod{b}$, by definition, $a|(x-y)$ and $b|(x-y)$. Then since $(a, b) = 1$, it follows that $ab|(x-y)$. Again by definition, this is equivalent to $x \equiv y \pmod{ab}$. □

We can generalize the above lemma so that it applies to any number of congruences by using mathematical induction.

Lemma 2.2.3. *If $(m_i, m_j) = 1$ for each $1 \leq i < j \leq n$ and $x \equiv y \pmod{m_i}$ for each $1 \leq i \leq n$, then $x \equiv y \pmod{\prod_{i=1}^{n} m_i}$.*

Proof. From Lemma 2.2.2, when $n = 2$ this lemma holds. Assume now that for some $n \geq 2$ we have that $x \equiv y \pmod{m_1 m_2 \ldots m_n}$. Consider m_{n+1} such that $(m_{n+1}, m_i) = 1, 1 \leq i \leq n$. Then $(m_{n+1}, m_1 m_2 \ldots m_n) = 1$. Thus, by Lemma 2.2.2 again, $x \equiv y \pmod{m_1 m_2 \ldots m_n \cdot m_{n+1}}$. □

Finally, in the Section 2.3, we will make use of the following theorem due to Fermat.

Theorem 2.2.1 (Fermat's Little Theorem (1640))**.** *If p is a prime and $p \nmid a$, then $a^{p-1} \equiv 1 \pmod{p}$.*

2.3 Additional Hypothesis in Theorem 1.3.5

Recall the additional hypothesis in Theorem 1.3.5, "for any prime factor p of q, the k^{th} powers $\pmod{p}$ are not constant on any edge $[c_i + 1, c_i + B]$ of $\mathcal{B}$." Otherwise, the diagonal sum $\sum_{i=1}^{n} a_i x_i^k$ will be constant $\pmod{p}$ on the cube $\mathcal{B}$.

As an example, if we suppose that q is a positive integer with prime factor p such that $(p-1)|k$ and the intervals $[d_i+1, d_i+B]$ do not contain a multiple of p, then, by Fermat's Little Theorem, for any $x_i \in [d_i+1, d_i+B]$

$$x_i^k \equiv 1 \pmod{p}.$$

That is, the k^{th} powers are constant on the edge $[d_i+1, d_i+B]$. In this case,

$$a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv a_1 + \cdots + a_n \pmod{p}.$$

Thus, without the added condition, we cannot solve the congruence for an arbitrary integer c.

2.4 Chinese Remainder Theorem

Theorem 2.4.1 (Chinese Remainder Theorem)**.** *Suppose that the positive integers $m_1, \ldots, m_j$ are pairwise co-prime. Then for any given integers $a_1, \ldots, a_j$, there exists an integer x that simultaneously solves the system of congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ &\vdots \\ x &\equiv a_j \pmod{m_j}, \end{aligned}$$

and it is unique $\pmod{\prod_{i=1}^{j} m_i}$.

For a proof of the Chinese Remainder Theorem, see [2, p. 117].

Corollary 2.4.1. *If q has prime power factorization $q = \prod_{i=1}^{j} p_i^{\ell_i}$, then $\gamma(k,q) = \max_{1\leq i\leq j} \gamma(k, p_i^{\ell_i})$.*

Proof. Let us begin by supposing that $n \geq \gamma(k, \prod_{i=1}^{j} p_i^{\ell_i})$, and let us pick an integer c. Then, there exist integers $x_1, \dots, x_n$ such that $c \equiv x_1^k + \cdots + x_n^k \pmod{\prod_{i=1}^{j} p_i^{\ell_i}}$. By Lemma 2.2.1, it follows that $c \equiv x_1^k + \cdots + x_n^k \pmod{p_i^{\ell_i}}$ for each $1 \leq i \leq j$. Since c was arbitrary, we have shown now that for any integer c, there exist integers $x_1, \dots, x_n$ such that $c \equiv x_1^k + \cdots + x_n^k \pmod{p_i^{\ell_i}}$ for every $1 \leq i \leq j$. Hence, $n \geq \gamma(k, p_i^{\ell_i})$ for all $1 \leq i \leq j$. Thus, $n \geq \max_{1 \leq i \leq j} \gamma(k, p_i^{\ell_i})$.

Next let us instead suppose that $n \geq \gamma(k, p_i^{\ell_i})$ for all $1 \leq i \leq j$, and let us pick an integer c. Then, for every $1 \leq i \leq j$, there exist integers $x_{it}, 1 \leq t \leq n$, such that

$$c \equiv x_{i1}^k + \cdots + x_{in}^k \pmod{p_i^{\ell_i}}.$$

For each $1 \leq t \leq n$, we are assured by the Chinese Remainder Theorem, Theorem 2.4.1, that there exist integers $x_t, 1 \leq t \leq n$, such that for all $1 \leq i \leq j$, $x_t \equiv x_{it} \pmod{p_i^{\ell_i}}$. Thus, $\displaystyle\sum_{t=1}^{n} x_t^k \equiv \sum_{t=1}^{n} x_{it}^k \equiv c \pmod{p_i^{\ell_i}}$ for $1 \leq i \leq j$. Thus, by Lemma 2.2.3, $c \equiv \sum_{t=1}^{n} x_t^k$ $\displaystyle\left(\text{mod } \prod_{i=1}^{j} p_i^{\ell_i}\right)$. □

In a similar manner, one can show:

Corollary 2.4.2. *If q has prime power factorization $q = \displaystyle\prod_{i=1}^{j} p_i^{\ell_i}$, then $\Gamma(k, q) = \displaystyle\max_{1 \leq i \leq j} \Gamma(k, p_i^{\ell_i})$.*

2.5 Calculation of $\gamma(2, q)$

To illustrate the calculation of Waring's number using Corollary 2.4.2, we consider the case when $k = 2$ and q is odd.

Lemma 2.5.1. *For any integer c and odd prime p, there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 \equiv c \pmod{p}$, i.e. $\gamma(2, p) = 2$.*

Before we begin the proof of Lemma 2.5.1, let us state Lagrange's Theorem which we will use in its proof.

Theorem 2.5.1 (Lagrange's Theorem)**.** *If p is a prime and $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is a polynomial of degree $d \geq 1$ whose coefficients are integers with $a_d \not\equiv 0 \pmod{p}$, then $f(x) \equiv 0 \pmod{p}$ has at most d solutions $\pmod{p}$.*

Proof of Lemma 2.5.1. Notice that for each positive integer a,

$$(p-a)^2 = p^2 - 2ap + a^2 \equiv a^2 \pmod{p}.$$

Hence, the nonzero squares $\pmod{p}$ can each be represented in two ways. That is, for $b \neq 0$, $x^2 - b \equiv 0 \pmod{p}$ has two solutions $\pmod{p}$, and by Lagrange's Theorem, it has no more than two solutions $\pmod{p}$. Thus, for an odd prime p, there are exactly $\frac{p+1}{2}$ distinct squares $\pmod{p}$. There are also $\frac{p+1}{2}$ distinct numbers $c - y^2 \pmod{p}$ for a fixed c. Now, there are p values $\pmod{p}$, and $\frac{p+1}{2} > \frac{p}{2}$ of them are squares $\pmod{p}$ while $\frac{p+1}{2} > \frac{p}{2}$ of them can be represented as $c - y^2 \pmod{p}$. Hence, there must be at least one square $\pmod{p}$ that can also be written as $c - y^2 \pmod{p}$. Therefore, there exist x, y with $x^2 \equiv c - y^2 \pmod{p}$. □

Lemma 2.5.2. *For any prime p with $p \equiv 1 \pmod{4}$, $\gamma(2, p^\ell) = 2$ for any positive integer ℓ.*

Proof. We will prove this lemma by induction. Theorem 2.5.1 assures that for any c and odd prime p, $x^2 + y^2 \equiv c \pmod{p}$ has a solution. If $p \nmid c$, then certainly $p \nmid x$ or $p \nmid y$. If $p | c$, then $x^2 + y^2 \equiv c \pmod{p^j}$ for some $j \geq 1$ implies that $x^2 + y^2 \equiv 0 \pmod{p}$. Since $p \equiv 1 \pmod{4}$, there exist x, y such that $x^2 + y^2 = p$. In this case too, we may say $p \nmid x$. (If, however, $p \equiv 3 \pmod{4}$, then $x^2 + y^2 \equiv 0 \pmod{p}$ would imply that $x \equiv y \equiv 0 \pmod{p}$. Thus, we need another variable in the case when $p \equiv 3 \pmod{4}$.)

Without loss of generality, let us say that $p \nmid x$. Suppose that for some $j \geq 1$ there exist x, y such that $x^2 + y^2 \equiv c \pmod{p^j}$ where $p \nmid x$. Consider $(x + p^j t)^2 + y^2 \pmod{p^{j+1}}$.

$$(x + p^j t)^2 + y^2 \equiv x^2 + y^2 + 2xp^j t + p^{2j} t^2 \equiv x^2 + y^2 + 2xp^j t \pmod{p^{j+1}}.$$

Let us choose $t \equiv 2^{-1} x^{-1} \frac{(c - x^2 - y^2)}{p^j} \pmod{p}$ (note that all of the inverses are $\pmod{p}$ and

$p^j | (c - x^2 - y^2)$ since $x^2 + y^2 \equiv c \pmod{p^j})$ so that:

$$\begin{aligned}(x + p^j t)^2 + y^2 &\equiv x^2 + y^2 + 2xp^j t \\ &\equiv x^2 + y^2 + 2xp^j 2^{-1} x^{-1} \frac{(c - x^2 - y^2)}{p^j} \\ &\equiv x^2 + y^2 + c - x^2 - y^2 \\ &\equiv c \pmod{p^{j+1}}.\end{aligned}$$

□

Lemma 2.5.3. *For any prime p with $p \equiv 3 \pmod 4$, $\gamma(2, p^\ell) = 3$ for any positive integer ℓ.*

Proof. One can prove this lemma by induction as well. Theorem 2.5.1 assures that for any c and odd prime p, $x^2 + y^2 \equiv c \pmod p$ has a solution. Now we will split our proof into two cases.

The proof of the case when $p \nmid c$ is the same as the proof for $\gamma(k, p^\ell) = 2$ when $p \equiv 1 \pmod 4$. That is, we only need two variables when $p \nmid c$ even when $p \equiv 3 \pmod 4$.

Let us consider the case when $p | c$. We note that $p | c$ implies that $p \nmid c - 1$. Thus by the first case, $x^2 + y^2 \equiv c - 1 \pmod{p^j}$ is solvable; that is, $x^2 + y^2 + 1 \equiv c \pmod{p^j}$ is solvable.

□

The next theorem follows from the previous two lemmas and Corollary 2.4.1.

Theorem 2.5.2. *For odd q, $\gamma(2, q) = 2$ if all prime divisors p of q are such that $p \equiv 1 \pmod 4$, and $\gamma(2, q) = 3$ if q has a prime divisor p such that $p \equiv 3 \pmod 4$.*

Proof. Let us say q has prime power factorization $q = \prod_{i=1}^{j} p_i^{\ell_i}$, then $\gamma(k, q) = \max_{1 \le i \le j} \gamma(k, p_i^{\ell_i})$ by Corollary 2.4.1 above. Thus, if all prime divisors p_i of q are such that $p_i \equiv 1 \pmod 4$, then $\gamma(k, q) = \max_{1 \le i \le j} \gamma(k, p_i^{\ell_i}) = 2$ by Lemma 2.5.2. If, however, q has a prime divisor p_j such that $p_j \equiv 3 \pmod 4$, then $\gamma(k, q) = \max_{1 \le i \le j} \gamma(k, p_i^{\ell_i}) = 3$ by Lemma 2.5.3. □

Note, in Theorem 2.6.1, we show that for any odd q, $\Gamma(k, q) \le \frac{3}{2}k$. This, of course, implies that $\gamma(2, q) \le 3$ for any odd q as we just discovered. One can prove in an identical manner that $\Gamma(2,q) = 3$ for any odd q.

2.6 A Generalized Waring Number $\pmod q$

Let us recall the definition of $\Gamma(k,q)$. For any positive integers q and k let $\Gamma(k,q)$ be the minimal n (should it exist) such that for any integers a_i with $(a_i,q) = 1, 1 \le i \le n$, and any integer c, the congruence

$$a_1x_1^k + a_2x_2^k + \cdots + a_nx_n^k \equiv c \pmod q \tag{2.1}$$

is solvable in integers $x_i, 1 \le i \le n$. When all of the $a_i = 1$ this is just Waring's Problem $\pmod q$, and in this case it is known by the work of Hardy and Littlewood [17] that if $n \ge 4k$, then every integer is a sum of at most n k-th powers $\pmod q$. We claim that the same is true for the more general congruence (2.1).

Theorem 2.6.1. *For any positive integers k, q, we have uniformly that $\Gamma(k,q) \le 4k$. Moreover for any odd q, $\Gamma(k,q) \le \frac{3}{2}k$, and for any prime p, $\Gamma(k,p) \le k$.*

We will make use of the following extension of the Cauchy-Davenport inequality due to Chowla [9].

Lemma 2.6.1. *Let q be a positive integer, and S, T be subsets of $\mathbb{Z}_q$ such that $0 \in S$, and for all nonzero $s \in S$ we have $(s,q) = 1$. Then $|S+T| \ge \min(q, |S| + |T| - 1)$.*

Proof of Theorem 2.6.1. It is plain that if q has prime power factorization $q = \prod_{i=1}^{j} p_i^{e_i}$ then $\Gamma(k,q) = \max_i \Gamma(k, p_i^{e_i})$ and so we may restrict our attention to prime power moduli $q = p^r$. We will actually prove a slightly stronger result than what is stated in the theorem. For $1 \le i \le n$, let a_i be an integer with $(a_i,q) = 1$ and

$$S_i := \{0\} \cup \{a_ix^k \in \mathbb{Z}_q \,:\, (x,q) = 1\}.$$

By successive applications of Chowla's Lemma, we see that for any positive integer n,

$$|S_1 + S_2 + \cdots + S_n| \geq \min(q, |S_1| + |S_2| + \cdots + |S_n| - (n-1)). \tag{2.2}$$

Suppose that p is odd, so that the group of units $\pmod q$ is cyclic. Then the subgroup of k-th powers has cardinality $\phi(q)/(k, \phi(q))$, and we get

$$|S_i| = \frac{\phi(q)}{(k, \phi(q))} + 1,$$

for $1 \leq i \leq n$. By (2.2),

$$|S_1 + S_2 + \cdots + S_n| \geq \min\left\{q, n\frac{\phi(q)}{(k, \phi(q))} + 1\right\}.$$

Thus, if $n\phi(q)/(k, \phi(q)) + 1 \geq q$, then $S_1 + \cdots + S_n = \mathbb{Z}_q$. It suffices to have $n \geq \frac{p}{p-1}k$. In the worst case, $p = 3$, we need $n \geq \frac{3}{2}k$. For $q = p$, it suffices to have $n \geq (k, p-1)$.

It is easy to verify that for any $k \geq 2$, $\Gamma(k, 2) = 1$ and $\Gamma(k, 4) = 3$. Suppose next that $q = 2^e$ with $e \geq 3$, the case where the group of units is not cyclic. The subgroup of k-th powers has cardinality 2^{e-1} if k is odd, and cardinality $\dfrac{2^{e-1}}{2(2^{e-2}, k)}$ if k is even. In the former case, $|S_i| = 2^{e-1} + 1$ and so it suffices to take $n = 2$, while in the latter case,

$$|S_i| = \frac{2^{e-1}}{2(2^{e-2}, k)} + 1 \geq \frac{2^{e-2}}{k} + 1,$$

and so, by (2.2), it suffices to take $n = 4k$. □

2.7 Cauchy-Davenport Type Result for an Abelian Group

We begin this section with the statement of the Cauchy-Davenport Theorem.

Theorem 2.7.1 (Cauchy-Davenport)**.** *For any prime p and nonempty subsets A and B of $\mathbb{Z}/p\mathbb{Z}$, $|A + B| \geq \min\{p, |A| + |B| - 1\}$.*

Theorem 2.7.2. *Suppose that A, B are finite, nonempty subsets of an additive abelian group G such that neither A nor B is contained in a coset of any proper subgroup of G. Then either $A+B=G$ or $|A+B| \geq \frac{3}{4}(|A|+|B|)$.*

Note that by considering $A = B = H \cup (H+a)$, where G is a finite group of odd order, H is a proper subgroup of G, and $a \notin H$, we see that the constant $\frac{3}{4}$ cannot be improved. In this case, $|A| = |B| = |H \cup (H+a)| = 2|H|$ since $a \notin H$. Also, $|A+B| = |H \cup (H+a) \cup (H+2a)| = 3|H|$. We deduce the result as a consequence of Kneser's Theorem following the method used to prove [32, Corollary 5.6].

Lemma 2.7.1. *Kneser's Theorem. For any finite, nonempty subsets A, B of an additive abelian group G, we have*

$$|A+B| \geq |A+H| + |B+H| - |H|,$$

where $H = stab(A+B) = \{x \in G : x + (A+B) = A+B\}$.

Proof of Theorem 2.7.2. Let A, B be subsets of G not contained in a coset of any proper subgroup of G. Suppose that $|A+B| < \frac{3}{4}(|A|+|B|)$. Let $H = stab(A+B)$. If $H = G$ then $A+B=G$. Assume now that H is a proper subgroup of G. By Kneser's Theorem we have

$$\frac{3}{4}(|A|+|B|) > |A+B| \geq |A+H| + |B+H| - |H| \geq |A| + |B| - |H|,$$

and so $|H| > \frac{1}{4}(|A|+|B|)$. Since $A+B$ is a union of cosets of H, and $|A+B| < \frac{3}{4}(|A|+|B|) < 3|H|$, we must have that $A+B$ is a union of one or two cosets of H. Suppose that $A+B$ is a union of two cosets. Then $|A+B| = 2|H|$. Also, $A+H$ and $B+H$ are unions of cosets of H, and so since neither A nor B is contained in a coset of H, $|A+H| \geq 2|H|$ and $|B+H| \geq 2|H|$. Thus by Kneser's Theorem,

$$2|H| = |A+B| \geq |A+H| + |B+H| - |H| \geq 2|H| + 2|H| - |H| = 3|H|,$$

a contradiction. Therefore, $A+B$ is a single coset of H, but this implies that A is contained in a coset of H, a contradiction. Hence $|A+B| \geq \frac{3}{4}(|A|+|B|)$. □

By induction on j, we obtain that for any collection of 2^j subsets A_i of $\mathbb{Z}_q$ of cardinality at least N, none of which are contained in a coset of a proper subgroup of $\mathbb{Z}_q$, that $|A_1 + \cdots + A_{2^j}| \geq \min\{q, (3/2)^j N\}$. Hence, we obtain the following corollary.

Corollary 2.7.1. *Let $A_1, \ldots, A_n$ be subsets of $\mathbb{Z}_q$ of cardinality at least N, none of which are contained in a coset of any proper subgroup of $\mathbb{Z}_q$. Then*

$$|A_1 + \cdots + A_n| \geq \min\{q, (n/2)^{\frac{\log(3/2)}{\log 2}} N\}.$$

Proof. Given $2^j \leq n < 2^{j+1}$ and $|A_i| \geq N$ for all $1 \leq i \leq n$,

$$|A_1 + A_2 + \cdots + A_n| \geq |A_1 + A_2 + \cdots + A_{2^j}| \geq \min\{q, (3/2)^j N\}.$$

Note that

$$(3/2)^j = 2^{\log_2 (3/2)^j} = 2^{j \cdot \frac{\log(3/2)}{\log 2}},$$

and since $\frac{\log(3/2)}{\log 2} > 0$ and $\frac{n}{2} < 2^j$, we obtain $2^{j \cdot \frac{\log(3/2)}{\log 2}} > (n/2)^{\frac{\log(3/2)}{\log 2}}$, and hence

$$|A_1 + A_2 + \cdots + A_n| \geq (n/2)^{\frac{\log(3/2)}{\log 2}} N.$$

□

2.8 Exponential Sums

An example of an exponential sum is

$$\sum_{x=1}^{B} e^{\frac{2\pi i}{q}(ax^k)} \tag{2.3}$$

where $q, k, B \in \mathbb{N}$, $i = \sqrt{-1}$, and $a \in \mathbb{Z}$. We will define $e_q(x) := e^{\frac{2\pi i x}{q}}$ so that we may more briefly write (2.3) as

$$\sum_{x=1}^{B} e_q(ax^k).$$

For our purposes, we need to estimate the size of such exponential sums. A trivial upper bound is given by

$$\left| \sum_{x=1}^{B} e_q(ax^k) \right| \leq B,$$

since each term has absolute value 1.

We can compute the number of solutions of (1.8) in $\mathcal{B}$ using the following two lemmas involving exponential sums.

Lemma 2.8.1. *For any positive integer q,*

$$\sum_{x=1}^{q} e_q(ax) = \begin{cases} q, & \text{if } q|a \\ 0, & \text{if } q \nmid a. \end{cases}$$

Proof. If $q|a$, then $e_q(ax) = 1$ for $x = 1, 2, \ldots, q$ implying that $\sum_{x=1}^{q} e_q(ax) = \sum_{x=1}^{q} 1 = q$. If $q \nmid a$, then

$$\sum_{x=1}^{q} e_q(ax) = \frac{e_q(a) - e_q(a(q+1))}{1 - e_q(a)} = \frac{e_q(a) - e_q(a)}{1 - e_q(a)} = 0.$$

□

Lemma 2.8.2. *Fix $n \geq 2$, $k \geq 2$, and $\varepsilon > 0$, and let c, a_i be integers, $1 \leq i \leq n$, $q \in \mathbb{N}$, $\mathcal{B}$ be a cube*

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

of side length B where $B, d_i \in \mathbb{Z}$, $1 \leq i \leq n$, $B \geq 1$, and N be the number of solutions of (1.8) in $\mathcal{B}$. Then

$$N = \frac{B^n}{q} + \frac{1}{q} \sum_{\lambda=1}^{q-1} e_q(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=1}^{B} e_q\left(\lambda a_i (x_i + d_i)^k\right).$$

Proof. Let N be the number of solutions of (1.8) in $\mathcal{B}$. Notice that via Lemma 2.8.1

$$\sum_{\lambda=1}^{q} e_q\left(\lambda\left(\sum_{i=1}^{n} a_i x_i^k - c\right)\right) = \begin{cases} q, & \text{if } q | \left(\sum_{i=1}^{n} a_i x_i^k - c\right) \\ 0, & \text{otherwise }, \end{cases}$$

and so this sum is non-zero only when $\sum_{i=1}^{n} a_i x_i^k - c \equiv 0 \pmod{q}$, that is, only when $\sum_{i=1}^{n} a_i x_i^k \equiv c \pmod{q}$. Hence if we multiply this sum by $\frac{1}{q}$ and sum over all $\underline{x} \in \mathcal{B}$, we obtain a sum that counts the number of solutions to (1.8) in $\mathcal{B}$. Therefore,

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

and thus

$$N = \frac{B^n}{q} + \frac{1}{q} \sum_{\lambda=1}^{q-1} e_q(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=1}^{B} e_q\left(\lambda a_i (x_i + d_i)^k\right).$$

□

Theorem 2.8.1. *[33, Weil] For any polynomial $P[x]$ over $\mathbb{Z}$ of degree k and prime p such that $P[x]$ is not a constant function $\pmod{p}$ (that is, $P(x) \not\equiv g(x)^p - g(x) + c \pmod{p}$ for any polynomial $g(x)$ and constant c),*

$$\left| \sum_{x \pmod{p}} e_p(P(x)) \right| \leq (k-1)p^{\frac{1}{2}}.$$

Using the Weil estimate in the case when $q = p$ is prime, we get from Lemma 2.8.2 that

$$\left| N - \frac{B^n}{p} \right| \leq \frac{p-1}{p} \left((k-1)p^{\frac{1}{2}}\right)^n < (k-1)^n p^{\frac{n}{2}},$$

and so $N > 0$ provided that

$$B \geq (k-1)p^{\frac{1}{2}+\frac{1}{n}}.$$

Thus, we obtain a result similar to that in (1.4). Unfortunately though, using the Weil estimate above, we cannot reach any result below $p^{\frac{1}{2}}$ no matter how large n is.

In our application, we need a bound of the type

$$\max_{1 \leq a < p} \left| \sum_{x=1}^{B} e_p(ax^k) \right| \ll_{\varepsilon,k} B^{1+\varepsilon-\sigma} \tag{2.4}$$

for some value $\sigma = \sigma(k)$, depending only on k, that holds for any $\varepsilon > 0$. If $B < p^{\frac{1}{k}}$, we may not obtain much cancellation, and so such an estimate cannot hold. Indeed, in this case, the sum in (2.4) can remain close to B in size for certain a. For $B > p^{\frac{1}{k-1}}$,

- the classical Weyl sum estimate (1920) establishes that the result in (2.4) holds for $\sigma = \frac{1}{2^{k-1}}$;
- Wooley [39] established the result in (2.4) for $k \geq 3$ with $\sigma = \frac{1}{2(k-1)(k-2)}$; and
- Bourgain, Demeter, and Guth [8] established the result in (2.4) for $k \geq 2$ with $\sigma = \frac{1}{k(k-1)}$.

Inserting the bound in (2.4) into the value of N in Lemma 2.8.2, we see that

$$\left| N - \frac{B^n}{p} \right| \ll_{\varepsilon,k} \frac{p-1}{p} \left(B^{1+\varepsilon-\sigma} \right)^n < B^{n-n\sigma+n\varepsilon},$$

and thus $N > 0$ provided that

$$\frac{B^n}{p} \gg_{\varepsilon,k,n} B^{n-n\sigma+\varepsilon},$$

that is,

$$B \gg_{\varepsilon,k,n} p^{\frac{1}{n\sigma}+\varepsilon}.$$

Hence, if we use Weyl sum estimates such as that in Bourgain, Demeter, and Guth [8] where it was proven that $\max_{1 \leq a < p} \left| \sum_{x=1}^{B} e_p(ax^k) \right| \ll_{\varepsilon,k} B^{1+\varepsilon-\frac{1}{k(k-1)}}$, we would find that $N > 0$

provided that

$$B \gg_{\varepsilon,k,n} \max\{p^{\frac{1}{k-1}}, p^{\frac{k(k-1)}{n}+\varepsilon}\}.$$

For $p^{\frac{1}{k}} < B < p^{\frac{1}{k-1}}$, we make use of a variation of (2.4) provided in (3.9).

Chapter 3

Using Weyl Sum Estimates

In this chapter we improve on the results stated in Section 1.2 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 3.0.2. *For $k \geq 2$ 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 $p \nmid a_i$, $1 \leq i \leq n$, there exists a nonzero solution $\underline{x}$ to* (1.8) *with*

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

Here, $\gamma = \gamma(\varepsilon, k)$ is the same constant as in Lemma 3.3.1.

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 (1.8) 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 (1.8). The first two estimates in the theorem are consequences of Proposition 3.3.1 in Section 3.3 while the third follows from Proposition 3.2.1 in Section 3.2, 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 (1.4) for $n > (2+\mathrm{o}(1))k\log k$ and uniformly improve on (1.5) and (1.6).

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

Theorem 3.0.3. *i) For $k \geq 2$ 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 $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution $\underline{x}$ to (1.8) in an arbitrary cube $\mathcal{B}$ of side length B provided that*

$$B \geq \begin{cases} p^{\frac{k(k-1)}{n}+\varepsilon}, & \text{if } n \leq k(k-1)^2; \\ p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon}, & \text{if } n > k(k-1)^2. \end{cases} \tag{3.1}$$

ii) For $2 \leq k \leq 5$, the inequalities in (3.1) may be improved to

$$B \geq \begin{cases} p^{\frac{2^{k-1}}{n}+\varepsilon}, & \text{if } n \leq 2^{k-1}(k-1); \\ p^{\frac{1}{k}+\frac{2^{k-1}}{nk}+\varepsilon}, & \text{if } n > 2^{k-1}(k-1). \end{cases} \tag{3.2}$$

These results yield improvements on the bound in (1.4) for $k \geq 6$ and $n \geq 2k(k-1)$ and uniformly improve on (1.6). They also yield improvements on (1.4) for $k = 3$, $n \geq 8$; $k = 4$, $n \geq 16$; and $k = 5$, $n \geq 32$. We have nothing new to offer here for $k = 2$.

Proof of Theorem 1.3.1. If $n > \frac{k-1}{\varepsilon}$ and $\varepsilon < \frac{1}{k(k-1)}$, then $\varepsilon > \frac{k-1}{n}$ and $n > k(k-1)^2$. Applying (3.1) in Theorem 3.0.3, it is sufficient to take $B \geq p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon} \geq p^{\frac{1}{k}+\varepsilon+\varepsilon} = p^{\frac{1}{k}+\varepsilon'}$. □

3.1 Best Bounds Among Known Results

In this section we give a summary of the best known bounds, including results from this chapter and the next, on the size of solutions to the diagonal congruence

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

for a given k, c, and n. We will separate the results into the four possible cases based upon whether the congruence is homogeneous or not and whether the solution is small or in a general cube. For the results obtained in other papers, we will include a citation next to the bound. We will also use $\kappa_1(k)$ as the same constant as in Theorem 4.7.1 while $\kappa_2(k, \varepsilon, n)$ will be the implicit constant in Theorem 4.9.1.

3.1.1 Small Solutions of a Homogeneous ($c = 0$) Diagonal Congruence

Degree	Size of Solution for $p \geq P(\varepsilon, k)$
$k = 2$	$0 < \lVert \underline{x} \rVert \leq p^{\frac{1}{2}}, \quad n \geq 4, \quad \text{[10]}.$
$k = 3$	$0 < \lVert \underline{x} \rVert \leq \begin{cases} p^{\frac{1}{2}}, & 4 \leq n \leq 8, \text{ [11]}; \\ p^{\frac{1}{3}+\frac{4}{3n}+\varepsilon}, & 9 \leq n < 21, \text{ Theorem 3.0.3}; \\ \kappa_1(3) p^{\frac{1}{3}}, & n \geq 21, \text{ Theorem 4.7.1}. \end{cases}$
$k = 4$	$0 < \lVert \underline{x} \rVert \leq \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 14, \text{ [11]}; \\ p^{\frac{8}{n}+\varepsilon}, & 14 < n \leq 24, \text{ Theorem 3.0.3}; \\ p^{\frac{1}{4}+\frac{2}{n}+\varepsilon}, & 24 < n \leq 32, \text{ Theorem 3.0.3}; \\ \kappa_1(4) p^{\frac{1}{4}}, & n \geq 33, \text{ Theorem 4.7.1}. \end{cases}$
$k = 5$	$0 < \lVert \underline{x} \rVert \leq \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 30, \text{ [11]}; \\ p^{\frac{16}{n}+\varepsilon}, & 30 < n \leq 47, \text{ Theorem 3.0.3}; \\ \kappa_1(5) p^{\frac{1}{5}}, & n \geq 48, \text{ Theorem 4.7.1}. \end{cases}$
$k \geq 6$	$0 < \lVert \underline{x} \rVert \leq \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq (2+\mathrm{o}(1))k \log k, \text{ [11]}; \\ p^{\frac{k(\log k+\gamma \log\log k)}{n}+\varepsilon}, & (2+\mathrm{o}(1))k\log k < n < \frac{3}{2}(k^2+k+2), \text{ Theorem 3.0.2}; \\ \kappa_1(k) p^{\frac{1}{k}}, & n \geq \frac{3}{2}(k^2+k+2), \text{ Theorem 4.7.1}. \end{cases}$

Note that from Theorem 4.9.1, we obtain a solution with

$$0 < \|\underline{x}\| \leq \kappa_2(k,\varepsilon,n)p^{\frac{1}{k}} + 3\exp\left(1 - \tfrac{2}{3}\tfrac{n-3}{k}\right),$$

which for k sufficiently large can yield further improvements for certain n. (See Remark 4.9.1.) For k odd, it is known [11] that for $n > k$, there is a nonzero solution with $\|\underline{x}\| < p^{\frac{1}{2}}$.

3.1.2 Solution in a General Cube of a Homogeneous ($c = 0$) Diagonal Congruence

Degree	Size of Solution for $p \geq P(\varepsilon, k)$
$k = 2$	$B \gg p^{\frac{1}{2}+\frac{1}{2(n-1)}}$, [11].
$k = 3$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 6, \ \text{[11]}; \\ p^{\frac{4}{n}+\varepsilon}, & n = 7, 8, \ \text{Theorem 3.0.3}; \\ p^{\frac{1}{3}+\frac{4}{3n}+\varepsilon}, & n \geq 9, \ \text{Theorem 3.0.3}. \end{cases}$
$k = 4$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 14, \ \text{[11]}; \\ p^{\frac{8}{n}+\varepsilon}, & 14 < n \leq 24, \ \text{Theorem 3.0.3}; \\ p^{\frac{1}{4}+\frac{2}{n}+\varepsilon}, & n > 24, \ \text{Theorem 3.0.3}. \end{cases}$
$k = 5$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 30, \ \text{[11]}; \\ p^{\frac{16}{n}+\varepsilon}, & 30 < n \leq 64, \ \text{Theorem 3.0.3}; \\ p^{\frac{1}{5}+\frac{16}{5n}+\varepsilon}, & n > 64, \ \text{Theorem 3.0.3}. \end{cases}$
$k \geq 6$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2(n-1)}}, & n \leq 2k(k-1)-2, \ \text{[11]}; \\ p^{\frac{k(k-1)}{n}+\varepsilon}, & 2k(k-1)-2 < n \leq k(k-1)^2, \ \text{Theorem 3.0.3}; \\ p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon}, & n > k(k-1)^2, \ \text{Theorem 3.0.3}. \end{cases}$

3.1.3 Small Solutions of a Non-homogeneous ($c \neq 0$) Diagonal Congruence

Degree	Size of Solution for $p \ge P(\varepsilon, k)$
$k = 2$	$0 < \Vert\underline{x}\Vert \le \begin{cases} p^{\frac{1}{2}}\log p, & 4 \le n < 12, \ \text{[13]}; \\ \kappa_1(2)p^{\frac{1}{2}}, & n \ge 12, \ \text{Theorem 3.0.2}. \end{cases}$
$k = 3$	$0 < \Vert\underline{x}\Vert \le \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \le 7, \ \text{[11]}; \\ p^{\frac{1}{2}+\varepsilon}, & n = 8, \ \text{Theorem 3.0.2}; \\ p^{\frac{1}{3}+\frac{4}{3n}+\varepsilon}, & 9 \le n < 21, \ \text{Theorem 3.0.3}; \\ \kappa_1(3)p^{\frac{1}{3}}, & n \ge 21, \ \text{Theorem 4.7.1}. \end{cases}$
$k = 4$	$0 < \Vert\underline{x}\Vert \le \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \le 15, \ \text{[11]}; \\ p^{\frac{8}{n}+\varepsilon}, & 16 \le n < 24, \ \text{Theorem 3.0.3}; \\ p^{\frac{1}{4}+\frac{2}{n}+\varepsilon}, & 24 \le n < 33, \ \text{Theorem 3.0.3}; \\ \kappa_1(4)p^{\frac{1}{4}}, & n \ge 33, \ \text{Theorem 4.7.1}. \end{cases}$
$k = 5$	$0 < \Vert\underline{x}\Vert \le \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \le 31, \ \text{[11]}; \\ p^{\frac{16}{n}+\varepsilon}, & 32 \le n < 48, \ \text{Theorem 3.0.3}; \\ \kappa_1(5)p^{\frac{1}{5}}, & n \ge 48, \ \text{Theorem 4.7.1}. \end{cases}$
$k \ge 6$	$0 < \Vert\underline{x}\Vert \le \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \le (2+\mathrm{o}(1))k\log k, \ \text{[11]}; \\ p^{\frac{k(\log k+\gamma\log\log k)}{n}+\varepsilon}, & (2+\mathrm{o}(1))k\log k < n < \frac{3}{2}(k^2+k+2), \ \text{Theorem 3.0.2}; \\ \kappa_1(k)p^{\frac{1}{k}}, & n \ge \frac{3}{2}(k^2+k+2), \ \text{Theorem 4.7.1}. \end{cases}$

Again, we note that from Theorem 4.9.1, we obtain a solution with

$$0 < \|\underline{x}\| \le \kappa_2(k, \varepsilon, n)p^{\frac{1}{k}} + 3\exp\left(1 - \tfrac{2}{3}\tfrac{n-3}{k}\right)$$

for k sufficiently large and for certain n. (See Remark 4.9.1.)

3.1.4 Solutions in a General Cube of a Non-homogeneous ($c \neq 0$) Diagonal Congruence

Degree	Size of solution
$k = 2$	$B \gg p^{\frac{1}{2}+\frac{1}{2n}}$, [11].
$k = 3$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \leq 7, \text{ [11];} \\ p^{\frac{1}{2}+\varepsilon}, & n = 8, \text{ Theorem 3.0.3;} \\ p^{\frac{1}{3}+\frac{4}{3n}+\varepsilon}, & n \geq 9, \text{ Theorem 3.0.3.} \end{cases}$
$4 \leq k \leq 5$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n \leq 2^k - 1, \text{ [11];} \\ p^{\frac{2^{k-1}}{n}+\varepsilon}, & 2^k \leq n \leq 2^{k-1}(k-1), \text{ Theorem 3.0.3;} \\ p^{\frac{1}{k}+\frac{2^{k-1}}{nk}+\varepsilon}, & n > 2^{k-1}(k-1), \text{ Theorem 3.0.3.} \end{cases}$
$k \geq 6$	$B \gg \begin{cases} p^{\frac{1}{2}+\frac{1}{2n}}, & n < 2k(k-1), \text{ [11];} \\ p^{\frac{k(k-1)}{n}+\varepsilon}, & 2k(k-1) \leq n \leq k(k-1)^2, \text{ Theorem 3.0.3;} \\ p^{\frac{1}{k}+\frac{k-1}{n}+\varepsilon}, & n > 2k(k-1)^2, \text{ Theorem 3.0.3.} \end{cases}$

3.2 Solutions in a General Cube

We start by recalling a classical result of Hua and Vandiver [20] and Weil [33] on the number $N_n(c)$ of solutions of the equation

$$\sum_{i=1}^{n} a_i x_i^k = c \tag{3.3}$$

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

$$|N_n(c) - p^{n-1}| \leq (k-1)^n p^{\frac{n-1}{2}}. \tag{3.4}$$

Thus, for $c \neq 0$, and $n \geq 2$, the equation (3.3) is guaranteed to have at least one solution provided that

$$p > k^{\frac{2n}{n-1}}. \tag{3.5}$$

For $c = 0$, (3.3) always has the trivial solution $\underline{x} = \underline{0}$. We note that $N_n(c)$ is just the number of solutions of (1.8) in a cube of side length $B = p$.

Next we turn to finding solutions in a restricted cube

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : d_i + 1 \leq x_i \leq d_i + B\} \tag{3.6}$$

of side length B where $B, d_i \in \mathbb{Z}$, $1 \leq i \leq n$, $1 \leq B \leq p$. The key ingredient to our investigation is a Weyl sum estimate for the exponential sum $\sum\limits_{x=1}^{B} e(\alpha_1 x + \cdots + \alpha_k x^k)$; 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 [15, Lemma 3.1].

Lemma 3.2.1. *Let $k \geq 2$ be an integer, and $\alpha_i \in \mathbb{R}$, $1 \leq i \leq k$. Suppose that for some $a \in \mathbb{Z}$, $q \in \mathbb{N}$ with $(a, q) = 1$, one has $|\alpha_k - \frac{a}{q}| \leq q^{-2}$. Then with $\sigma = \sigma(k) = 2^{1-k}$, we have for any $B \in \mathbb{N}$*

$$\left| \sum_{x=1}^{B} e(\alpha_1 x + \cdots + \alpha_k x^k) \right| \leq c_\varepsilon B^{1+\varepsilon} \left(\frac{1}{q} + \frac{1}{B} + \frac{q}{B^k} \right)^{\sigma} \tag{3.7}$$

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

Wooley [38, Theorem 11.1] established an improved estimate, obtaining the inequality in (3.7) with $\sigma(k) = \frac{1}{2k(k-2)}$ for $k \geq 4$, and made further improvements in [40, Theorem 11.1] and [39, Theorem 7.3], obtaining in the latter, $\sigma(k) = \frac{1}{2(k-1)(k-2)}$ for $k \geq 3$. Bourgain, Demeter and Guth [8] recently obtained $\sigma(k) = \frac{1}{k(k-1)}$ for $k \geq 2$. The latter value improves on Wooley's estimates and the classical value $\sigma(k) = 2^{1-k}$ for $k \geq 6$. For $k = 6$, an estimate of Heath-Brown [19] is better for certain ranges of q. Finally, Montgomery [22, 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 3.2.1. *Fix $n \geq 2$, $k \geq 2$, and suppose that the Weyl sum estimate in (3.7) holds for some positive real $\sigma = \sigma(k)$. For any $\varepsilon > 0$, there exists a constant $P(\varepsilon, k)$ such that for any prime $p \geq P(\varepsilon, k)$ and any integers c, a_i with $p \nmid a_i$, $1 \leq i \leq n$, there exists a solution $\underline{x}$ to (1.8) in any cube $\mathcal{B}$ of side length $B \leq p$ with*

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

Applying the proposition with the value of Bourgain, Demeter and Guth, $\sigma = \frac{1}{k(k-1)}$, immediately yields Theorem 3.0.3 (i) and the third inequality in Theorem 3.0.2. For $2 \leq k \leq 5$ we use the classical value $\sigma = 2^{k-1}$ to obtain Theorem 3.0.3 (ii).

Proof. Fix $n \geq 2$, $k \geq 2$, and $\varepsilon > 0$, and let c, a_i be integers with $p \nmid a_i$, $1 \leq i \leq n$, $\mathcal{B}$ be a cube as in (3.6), N the number of solutions of (1.8) 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

$$N = \frac{B^n}{p} + \frac{1}{p}\sum_{\lambda=1}^{p-1} e_p(-\lambda c)\prod_{i=1}^{n}\sum_{x_i=1}^{B} e_p\left(\lambda a_i (x_i+d_i)^k\right). \tag{3.8}$$

We now apply the Weyl sum estimate of Lemma 3.2.1 to the polynomial $\lambda a_i(x_i+d_i)^k$ with $q = p$ and $\alpha_k = \frac{\lambda a_i}{p}$. We observe that with $a = \lambda a_i$ and $1 \leq \lambda \leq p-1$, we have $(a, p) = 1$ and $|\alpha_k - \frac{a}{p}| = 0 < \frac{1}{p^2}$. Note that, it is also plain that with B satisfying the lower bound stated in the proposition, $B^k \geq p$. By (3.7), we have

$$\left| \sum_{x_i=1}^{B} e_p(\lambda a_i (x_i + d_i)^k) \right| \leq c_{\varepsilon'} B^{1+\varepsilon'} \left(\frac{1}{p} + \frac{1}{B} + \frac{p}{B^k} \right)^{\sigma} \tag{3.9}$$

for any $\varepsilon' > 0$. We use (3.8) to determine a lower bound for B such that the error term is less than the main term in (3.8). It suffices to have B satisfy

$$\frac{B^n}{p} > \frac{1}{p} \left| \sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i=1}^{B} e_p\left(\lambda a_i (x_i + d_i)^k\right) \right|. \tag{3.10}$$

With (3.10) satisfied, we are assured a solution to (1.8) in $\mathcal{B}$.

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

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

for $\varepsilon \leq \frac{\beta}{k(k-1)n}$, which we may assume, for if there exists a solution of (1.8) with $\varepsilon \leq \frac{\beta}{k(k-1)n}$, then trivially there exists a solution for larger values of ε. Using $B^{k-1} \leq p$ and $B \leq p$, the Weyl sum estimate in (3.9) simplifies to

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

for any $\varepsilon' > 0$. Applying this estimate and the triangle inequality to the right-hand side of (3.10), we find that we are guaranteed a solution to (1.8) if

$$\frac{B^n}{p} > c_{\varepsilon'}^{n} \left(B^{(1+\varepsilon')n} \right) \left(\frac{3p}{B^k} \right)^{n\sigma} \tag{3.11}$$

or equivalently

$$B^{n(k\sigma-\varepsilon')} \geq 3^{n\sigma} c_{\varepsilon'}^{n} p^{1+n\sigma}.$$

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 we may use $(1-x)^{-1} < 1+2x$ for $0 < x < \frac{1}{2}$ to 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 $n \leq (k-1)\sigma^{-1}$. In this case we set $B = \lceil p^{\frac{1}{\sigma n}+\varepsilon} \rceil$. Then plainly $B^{k-1} > p^{\frac{k-1}{\sigma n}} \geq p$, and thus the Weyl sum estimate simplifies to

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

for any $\varepsilon' > 0$. Then by (3.10), we find we are guaranteed a solution to (1.8) if

$$\frac{B^n}{p} > {c_{\varepsilon'}}^{n} \left(B^{(1+\varepsilon')n}\right) \left(\frac{3}{B}\right)^{\sigma n}, \tag{3.12}$$

and thus it suffices to have

$$B \gg_{\varepsilon',k} p^{\frac{1}{\sigma n(1-\varepsilon'/\sigma)}}. \tag{3.13}$$

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

$$B \gg_{\varepsilon',k} p^{\frac{1}{\sigma n}+\frac{2\epsilon'}{\sigma^2 n}}. \tag{3.14}$$

Thus, for ε' sufficiently small and p sufficiently large, our choice $B = \lceil p^{\frac{1}{\sigma n}+\varepsilon} \rceil$ suffices.

□

3.3 Small Solutions via Sums Over Smooth Numbers

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

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

and for each real number α, we define the corresponding exponential 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 [35] Wooley established the following estimate for $f(\alpha; P, R)$.

Lemma 3.3.1. *[35, 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 $|\alpha - a/q| \leq \frac{1}{qP^{k-1}}$, one has $q > P$. Then when $\eta = \eta(\varepsilon, k)$ is a sufficiently small positive number, and $2 \leq R \leq P^\eta$, we have,*

$$\sup_{\alpha \in \mathfrak{m}} |f(\alpha; P, R)| \leq \xi_\varepsilon P^{1-\sigma'+\varepsilon} \tag{3.15}$$

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

$$\sigma' = \sigma'(k) := k^{-1}(\log k + \gamma \log\log k)^{-1}.$$

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

Proposition 3.3.1. *Suppose that the inequality in (3.15) holds for a given $\sigma' = \sigma'(k)$. Then for $k \geq 2$, $n > \sigma'^{-1}$, and $\varepsilon > 0$, there exist constants $P(\varepsilon, k)$ and $\eta'(\varepsilon, k)$ such that for any positive integer ℓ satisfying $\frac{1}{\ell} \leq \eta'(\varepsilon, k)$, prime $p > P(\varepsilon, k)$, integers c, a_i with $p \nmid a_i$, $1 \leq i \leq n$, 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 (1.8) *with $x_i \in \mathcal{A}(B, B^{\frac{1}{\ell}})$, $1 \le i \le n$.*

Applying the proposition with Wooley's value $\sigma' = k^{-1}(\log k + \gamma \log\log k)^{-1}$, yields the first two inequalities in Theorem 3.0.2.

Proof. Suppose that $k \ge 2$, $n > \sigma'^{-1}$, and B satisfies $p^{\frac{1}{k-1}} < B < p$. We apply Lemma 3.3.1 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 $\sum\limits_{i=1}^{n} a_i x_i^k \equiv c \mod p$ with $\underline{x} \in \mathcal{A}^n$ is

$$\begin{aligned} M &= \frac{1}{p} \sum_{\underline{x} \in \mathcal{A}^n} \sum_{\lambda=1}^{p} e_p\left(\lambda\left(\sum_{i=1}^{n} a_i x_i^k - c\right)\right) \\ &= \frac{|\mathcal{A}|^n}{p} + \frac{1}{p} \sum_{\lambda=1}^{p-1} e_p(-\lambda c) \prod_{i=1}^{n} \sum_{x_i \in \mathcal{A}} e_p\left(\lambda a_i x_i^k\right). \end{aligned} \tag{3.16}$$

Let $\mathfrak{m}$ be as defined in Lemma 3.3.1. We note that for $1 \le \lambda \le p-1$, $\alpha := \frac{\lambda a_i}{p} \in \mathfrak{m}$. Indeed, suppose that $(a, q) = 1$ and that $|\frac{\lambda a_i}{p} - \frac{a}{q}| \le \frac{1}{qB^{k-1}}$. Then either $q = p$, whence $q > B$, or $q \ne p$, whence

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

that is $p \ge B^{k-1}$, contradicting $B > p^{\frac{1}{k-1}}$. Thus for any $\varepsilon' > 0$ and ℓ sufficiently large, $\ell \ge 1/\eta(\varepsilon', k)$, we have by Lemma 3.3.1 that

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

Combining this with (3.16), 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 [24], 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 $|\mathcal{A}(B, B^{\frac{1}{\ell}})| \geq \frac{1}{2}\rho(\ell)B$. Hence it suffices to have

$$\frac{\rho(\ell)^n B^n}{2^n p} > \xi_{\varepsilon'}^n B^{(1-\sigma'+\varepsilon')n}, \tag{3.17}$$

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 3.3.1. In his work [36, 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 3.3.1 to boxes in arbitrary position. Unfortunately, for the application here, this estimate leads to a weaker result than what is already available from Proposition 3.2.1.

Chapter 4

Using Vinogradov Mean Value Estimates

4.1 Introduction

Let q, n, k be positive integers, a_i be integers with $(a_i, q) = 1$, $1 \leq i \leq n$, and c be any integer. Our interest here is in obtaining solutions to the diagonal congruence

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_n x_n^k \equiv c \pmod{q}, \tag{4.1}$$

with variables restricted to a cube

$$\mathcal{B} := \{\underline{x} \in \mathbb{Z}^n : d_i + 1 \leq x_i \leq d_i + B, 1 \leq i \leq n\}, \tag{4.2}$$

of edge length $B \in \mathbb{N}$ with $B \leq q$; here $d_i \in \mathbb{Z}$, $1 \leq i \leq n$. First we give a general upper bound on the number of solutions of (4.1) in $\mathcal{B}$.

Theorem 4.1.1. *Let q, n, k be positive integers with $n \geq k^2 + k + 2$, $\mathcal{B}$ be any cube of edge* *length B as in (4.2), a_i be integers with $(a_i,q)=1$, $1\le i\le n$, and $c\in\mathbb{Z}$. Then*

$$\#\left\{\underline{x}\in\mathcal{B}:\sum_{i=1}^{n}a_ix_i^k\equiv c\pmod q\right\}\ll_k\left(\frac{B^n}{q}+B^{n-k}\right).$$

In some sense this upper bound is the best one can hope for. Indeed, as c runs from 0 to $q-1$, the average number of solutions of the congruence (4.1) with $\underline{x}\in\mathcal{B}$, is B^n/q. On the other hand, if $A:=\sum_{i=1}^n|a_i|$ is fixed, and c is allowed to run from $-AB^k$ to AB^k, then the average number of solutions of the equation $\sum_{i=1}^n a_ix_i^k=c$ with $1\le x_i\le B$ is of order B^{n-k}. Thus for large B, we can do no better than B^n/q, while for small B (namely, for $B\ll_k q^{\frac{1}{k}}$) and boxes cornered at the origin, we can do no better than B^{n-k}.

The upper bound in Theorem 4.1.1 implies that for $n>k^2+k+2$, the value set of the diagonal form,

$$\left\{\sum_{i=1}^{n}a_ix_i^k\pmod q:\underline{x}\in\mathcal{B}\right\},$$

has cardinality on the order of q provided that $B\gg_k q^{1/k}$. Using further variables and arithmetic combinatorics we can then represent all values by the diagonal form.

Theorem 4.1.2. *For any positive integer k, there exists a constant $c_3(k)$ such that for any positive integers q,n with $n>c_3(k)$, cube $\mathcal{B}$ of type (4.2) with side length $B\ge(q/k^2)^{1/k}$, and integers a_i with $(a_i,q)=1$, $1\le i\le n$, such that for any prime factor p of q, the k-th powers $\pmod p$ are not constant on any edge $[d_i+1,d_i+B]$ of $\mathcal{B}$, there exists a solution of (4.1) in $\mathcal{B}$.*

For prime moduli, we can obtain a much stronger result.

Theorem 4.1.3. *For any positive integer k there exists a constant $c_4(k)$ such that for any positive integer $n\ge\frac{3}{2}(k^2+k+2)$, prime p, and integers a_i with $p\nmid a_i$, $1\le i\le n$, there exists a solution of*

$$a_1x_1^k+\cdots+a_nx_n^k\equiv c\pmod p,\tag{4.3}$$

with $1\le x_i\le c_4(k)p^{\frac{1}{k}}$.

This improves on Theorem 3.0.2 for $n > \frac{3}{2}(k^2+k+2)$ and on Theorem 3.0.3 for $n > \frac{3}{2}(k^2+k+2)$ and cubes cornered at the origin.

4.2 A General Upper Bound on the Number of Solutions of (4.1)

Let $\mathbb{Z}_q$ denote the residue class ring mod q. For any subsets $S_1, \ldots, S_n$ of $\mathbb{Z}_q$, put $\mathcal{S} = S_1 \times \cdots \times S_n$, and define

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

Lemma 4.2.1. *Let q, n, k be positive integers, $S_1, \ldots, S_{2n}$ be subsets of $\mathbb{Z}_q$, and $\mathcal{T} = S_1 \times \cdots \times S_{2n}$. For any integers a_i, $0 \le i \le 2n$, with $(a_i, q) = 1$, $1 \le i \le 2n$, we have*

$$\#\Big\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\Big\} \le \prod_{i=1}^{2n} I_{n,k}(\mathcal{S}_i^n)^{\frac{1}{2n}},$$

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

Proof. We have

$$\begin{aligned}
\#\{\underline{x} \in \mathcal{T} : \textstyle\sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\} &= \frac{1}{q} \sum_{\underline{x} \in \mathcal{T}} \sum_{\lambda=1}^{q} e_q\left(\lambda\left(\sum_{i=1}^{2n} a_i x_i^k - a_0\right)\right) \\
&= \frac{1}{q} \sum_{\lambda=1}^{q} e_q(-\lambda a_0) \sum_{\mathbf{x} \in \mathcal{T}} e_q\left(\lambda \sum_{i=1}^{2n} a_i x_i^k\right) \\
&= \frac{1}{q} \sum_{\lambda=1}^{q} e_q(-\lambda a_0) \prod_{i=1}^{2n} \sum_{x_i \in S_i} e_q\left(\lambda a_i x_i^k\right) \\
&= \frac{1}{q} \left|\sum_{\lambda=1}^{q} e_q(-\lambda a_0) \prod_{i=1}^{2n} \sum_{x_i \in S_i} e_q\left(\lambda a_i x_i^k\right)\right|.
\end{aligned}$$

Then by the triangle inequality and Hölder's inequality, we have that

$$\begin{aligned}\#\{\underline{x} \in \mathcal{T} : &\textstyle\sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\} \\ &\leq \frac{1}{q} \sum_{\lambda=1}^{q} \left| e_q(-\lambda a_0) \prod_{i=1}^{2n} \sum_{x_i \in S_i} e_q\left(\lambda a_i x_i^k\right) \right| \\ &= \frac{1}{q} \sum_{\lambda=1}^{q} \left| \sum_{x_1 \in S_1} e_q(\lambda a_1 x_1^k) \sum_{x_2 \in S_2} e_q(\lambda a_2 x_2^k) \cdots \sum_{x_{2n} \in S_{2n}} e_q(\lambda a_{2n} x_{2n}^k) \right| \\ &\leq \frac{1}{q} \left[\sum_{\lambda=1}^{q} \left| \sum_{x_1 \in S_1} e_q(\lambda a_1 x_1^k) \right|^{2n} \right]^{\frac{1}{2n}} \cdots \left[\sum_{\lambda=1}^{q} \left| \sum_{x_{2n} \in S_{2n}} e_q(\lambda a_{2n} x_{2n}^k) \right|^{2n} \right]^{\frac{1}{2n}}.\end{aligned}$$

Consider now the sum

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

for a fixed i, $1 \leq i \leq 2n$.

$$\begin{aligned}&\sum_{\lambda=1}^{q} \left(\left| \sum_{x_i \in S_i} e_q(\lambda a_i x_i^k) \right| \right)^{2n} \\ &\quad = \sum_{\lambda=1}^{q} \left[\left(\sum_{x_1 \in S_i} e_q(\lambda a_i x_1^k) \right) \left(\sum_{y_1 \in S_i} e_q(-\lambda a_i y_1^k) \right) \ldots \left(\sum_{x_n \in S_i} e_q(\lambda a_i x_n^k) \right) \left(\sum_{y_n \in S_i} e_q(-\lambda a_i y_n^k) \right) \right] \\ &\quad = \sum_{\lambda=1}^{q} \sum_{x_1 \in S_i} \sum_{y_1 \in S_i} \cdots \sum_{x_n \in S_i} \sum_{y_n \in S_i} e_q\left(\lambda a_i (x_1^k + x_2^k + \cdots + x_n^k - y_1^k - y_2^k - \cdots - y_n^k)\right) \\ &\quad = \sum_{x_1 \in S_i} \sum_{y_1 \in S_i} \cdots \sum_{x_n \in S_i} \sum_{y_n \in S_i} \sum_{\lambda=1}^{q} e_q\left(\lambda a_i (x_1^k + x_2^k + \cdots + x_n^k - y_1^k - y_2^k - \cdots - y_n^k)\right).\end{aligned}$$

This counts q times the number of solutions to the congruence

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

with variables restricted to S_i, and since $(a_i, q) = 1$ this is just $qI_{n,k}(S_i^n)$. Therefore,

$$\#\{\underline{x} \in \mathcal{T} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\} \leq \frac{1}{q} \prod_{i=1}^{2n} (qI_{n,k}(S_i^n))^{\frac{1}{2n}} = \prod_{i=1}^{2n} I_{n,k}(S_i^n)^{\frac{1}{2n}}.$$

□

4.3 Relating $I_{n,k}(\mathcal{B})$ to $J_{n,k}(B)$

Next, we obtain an estimate for $I_{n,k}(\mathcal{B})$ for a cube of the type

$$\mathcal{B} = \mathcal{B}(c, B) := \{\underline{x} \in \mathbb{Z}^n : c + 1 \leq x_i \leq c + B, 1 \leq i \leq n\}, \tag{4.4}$$

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

$$\begin{aligned} x_1 + \cdots + x_n &\equiv y_1 + \cdots + y_n \pmod{q}, \\ x_1^2 + \cdots + x_n^2 &\equiv y_1^2 + \cdots + y_n^2 \pmod{q}, \\ &\vdots \\ x_1^k + \cdots + x_n^k &\equiv y_1^k + \cdots + y_n^k \pmod{q} \end{aligned} \tag{4.5}$$

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

Proposition 4.3.1. *For any positive integers n, k, q and cube $\mathcal{B}(c, B)$ as in (4.4) we have*

$$I_{n,k}(\mathcal{B}) \leq (2n)^{k-1} B^{\frac{k(k-1)}{2}} J_{n,k}(B). \tag{4.6}$$

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

$$I_{n,k}(\mathcal{B}) \leq (2n)^{j-1} B^{\frac{j(j-1)}{2}} q^{k-j} J_{n,k}(B). \tag{4.7}$$

Lemma 4.3.1. *Let $n, k,$ and q be fixed positive integers, c be any integer, and $(\underline{x}, \underline{y}) \in$*

$\mathbb{Z}^n \times \mathbb{Z}^n$. Then $(\underline{x}, \underline{y})$ is a solution of (4.5) if and only if $(\underline{x}, \underline{y})$ is a solution of the system

$$\begin{aligned} (x_1 - c) + \cdots + (x_n - c) &\equiv (y_1 - c) + \cdots + (y_n - c) \pmod q, \\ (x_1 - c)^2 + \cdots + (x_n - c)^2 &\equiv (y_1 - c)^2 + \cdots + (y_n - c)^2 \pmod q, \\ &\vdots \\ (x_1 - c)^k + \cdots + (x_n - c)^k &\equiv (y_1 - c)^k + \cdots + (y_n - c)^k \pmod q. \end{aligned} \tag{4.8}$$

Proof. Note that by considering a translation of the variables, it is enough to show that whenever $(\underline{x}, \underline{y})$ solves (4.8), it also solves (4.5). We will show by induction on the degree k that the result holds. First note that trivially $(\underline{x}, \underline{y})$ being a solution of $\sum_{i=1}^{n}(x_i - c) \equiv \sum_{i=1}^{n}(y_i - c) \pmod q$ implies that $\sum_{i=1}^{n} x_i \equiv \sum_{i=1}^{n} y_i \pmod q$.

Let us now assume that the result holds for systems of polynomials up to degree $k - 1$ and consider a system up to degree k. Suppose that $(\underline{x}, \underline{y})$ is a solution of

$$\sum_{i=1}^{n}(x_i - c)^\tau \equiv \sum_{i=1}^{n}(y_i - c)^\tau \pmod q \text{ for each } 1 \leq \tau \leq k. \tag{4.9}$$

We know by the induction hypothesis that $(\underline{x}, \underline{y})$ is also a solution to

$$\sum_{i=1}^{n} x_i^\tau \equiv \sum_{i=1}^{n} y_i^\tau \pmod q \text{ for each } 1 \leq \tau \leq k - 1. \tag{4.10}$$

We need only to show that $(\underline{x}, \underline{y})$ is a solution to

$$\sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod q. \tag{4.11}$$

By the binomial theorem, $(\underline{x}, \underline{y})$ is a solution of

$$(x_1 - c)^k + \cdots + (x_n - c)^k \equiv (y_1 - c)^k + \cdots + (y_n - c)^k \pmod q$$

if and only if $(\underline{x}, \underline{y})$ is a solution of

$$\sum_{i=1}^{n}\sum_{t=0}^{k}\binom{k}{t}x_i^t(-c)^{k-t} \equiv \sum_{i=1}^{n}\sum_{t=0}^{k}\binom{\tau}{t}y_i^t(-c)^{k-t} \pmod{q}.$$

In other words, $(\underline{x}, \underline{y})$ is a solution of

$$\sum_{i=1}^{n} x_i^k + \sum_{i=1}^{n}\sum_{t=0}^{k-1}\binom{k}{t}x_i^t(-c)^{k-t} \equiv \sum_{i=1}^{n} y_i^k + \sum_{t=0}^{k-1}\binom{k}{t}y_i^t(-c)^{k-t} \pmod{q}. \tag{4.12}$$

By (4.10),

$$\begin{aligned}\sum_{i=1}^{n}\sum_{t=0}^{k-1}\binom{k}{t}x_i^t(-c)^{k-t} &= \sum_{t=0}^{k-1}\left(\binom{k}{t}(-c)^{k-t}\sum_{i=1}^{n}x_i^t\right)\\ &\equiv \sum_{t=0}^{k-1}\left(\binom{k}{t}(-c)^{k-t}\sum_{i=1}^{n}y_i^t\right)\\ &\equiv \sum_{i=1}^{n}\sum_{t=0}^{k-1}\binom{k}{t}y_i^t(-c)^{k-t} \pmod{q},\end{aligned}$$

and thus (4.12) implies

$$\sum_{i=1}^{n} x_i^k \equiv \sum_{i=1}^{n} y_i^k \pmod{q}. \tag{4.13}$$

□

In our application we actually consider a hybrid system

$$\begin{aligned}(x_1-c)+\cdots+(x_n-c) &\equiv (y_1-c)+\cdots+(y_n-c) \pmod{q},\\ (x_1-c)^2+\cdots+(x_n-c)^2 &\equiv (y_1-c)^2+\cdots+(y_n-c)^2 \pmod{q},\\ &\;\vdots\\ (x_1-c)^{k-1}+\cdots+(x_n-c)^{k-1} &\equiv (y_1-c)^{k-1}+\cdots+(y_n-c)^{k-1} \pmod{q}\\ x_1^k+\cdots+x_n^k &\equiv y_1^k+\cdots+y_n^k \pmod{q}.\end{aligned} \tag{4.14}$$

It follows from the arguments in the proof of Lemma 4.3.1 that this system is also equivalent to the systems considered in Lemma 4.3.1. That is, $\underline{x}$ is a solution of (4.8) (or equivalently (4.5)) if and only if $\underline{x}$ is a solution of (4.14). In particular, if $\underline{x}$ with $c+1 \leq x_i \leq c+B$ for $1 \leq i \leq n$ solves (4.14), then it solves (4.8). Thus, $\underline{x}, \underline{y}$ with $1 \leq x_i, y_i \leq B$ solves (4.5). Hence, the number of solutions $\underline{x}$ with $c+1 \leq x_i \leq c+B, 1 \leq i \leq n$ that solve (4.14) is $J_{n,k}(B)$. This leads us to our next lemma.

Lemma 4.3.2. *Let $\mathcal{B}(c,B)$ be a cube as in (4.4). The number of solutions of the system (4.14) with $\underline{x}, \underline{y} \in \mathcal{B}(c,B)$ is $J_{n,k}(B)$.*

We are now in a position to prove Proposition 4.3.1.

Proof of Proposition 4.3.1. Let $\mathcal{B} = \mathcal{B}(c,B)$ be a cube as in (4.4). For any $\underline{x}, \underline{y} \in \mathcal{B}$ we set

$$\begin{aligned} h_1 =& (x_1 - c) + \cdots + (x_n - c) - (y_1 - c) - \cdots - (y_n - c) \\ &\vdots \\ h_{k-1} =& (x_1 - c)^{k-1} + \cdots + (x_n - c)^{k-1} - (y_1 - c)^{k-1} - \cdots - (y_n - c)^{k-1}. \end{aligned}$$

It is plain that for any choice of $\underline{x}, \underline{y} \in \mathcal{B}$, we have $|h_j| \leq n(B^j - 1)$, $1 \leq j \leq k-1$. Thus, by summing over the potential values for the h_j and writing $\sum\limits_{\underline{x} \in \mathcal{B}}$ to denote $\sum\limits_{x_1=c+1}^{c+B} \cdots \sum\limits_{x_n=c+1}^{c+B}$, we have

$$
\begin{aligned}
I_{n,k}(\mathcal{B}) &= \sum_{\substack{\underline{x}\in\mathcal{B} \\ x_1^k+\cdots+x_n^k\equiv y_1^k+\cdots+y_n^k \pmod q}} \sum_{\underline{y}\in\mathcal{B}} 1 \\
&= \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \sum_{\substack{c+1\le x_1,\ldots,x_n\le c+B \\ c+1\le y_1,\ldots,y_n\le c+B \\ h_1\equiv\sum_{i=1}^n (x_i-c)-\sum_{i=1}^n (y_i-c) \pmod q \\ \vdots \\ h_{k-1}\equiv\sum_{i=1}^n (x_i-c)^{k-1}-\sum_{i=1}^n (y_i-c)^{k-1} \pmod q \\ x_1^k+\cdots+x_n^k\equiv y_1^k+\cdots+y_n^k \pmod q}} 1 \\
&= \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} \\
&\qquad e_q\left[\lambda_k\left(\sum_{i=1}^n x_i^k-\sum_{i=1}^n y_i^k\right)+\sum_{j=1}^{k-1}\lambda_j\left(\sum_{i=1}^n (x_i-c)^j-\sum_{i=1}^n (y_i-c)^j-h_j\right)\right] \\
&= \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} \\
&\qquad e_q\left[\sum_{j=1}^{k}-\lambda_j h_j\right] e_q\left[\lambda_k\left(\sum_{i=1}^n x_i^k-\sum_{i=1}^n y_i^k\right)+\sum_{j=1}^{k-1}\lambda_j\left(\sum_{i=1}^n (x_i-c)^j-\sum_{i=1}^n (y_i-c)^j\right)\right] \\
&= \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} e_q\left[\sum_{j=1}^{k}-\lambda_j h_j\right] \times \\
&\qquad \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} e_q\left[\lambda_k\left(\sum_{i=1}^n x_i^k-\sum_{i=1}^n y_i^k\right)+\sum_{j=1}^{k-1}\lambda_j\left(\sum_{i=1}^n (x_i-c)^j-\sum_{i=1}^n (y_i-c)^j\right)\right]
\end{aligned}
$$

By the triangle inequality and Lemma 4.3.2, we obtain

$$\begin{aligned}
I_{n,k}(\mathcal{B}) = \Bigg| & \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} e_q\left[\sum_{j=1}^{k} -\lambda_j h_j\right] \times \\
& \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} e_q\left[\lambda_k \left(\sum_{i=1}^{n} x_i^k - \sum_{i=1}^{n} y_i^k\right) + \sum_{j=1}^{k-1} \lambda_j \left(\sum_{i=1}^{n} (x_i-c)^j - \sum_{i=1}^{n} (y_i-c)^j\right)\right] \Bigg| \\
\le & \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} \Bigg| \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} \\
& e_q\left[\lambda_k \left(\sum_{i=1}^{n} x_i^k - \sum_{i=1}^{n} y_i^k\right) + \sum_{j=1}^{k-1} \lambda_j \left(\sum_{i=1}^{n} (x_i-c)^j - \sum_{i=1}^{n} (y_i-c)^j\right)\right] \Bigg| \\
= & \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} \frac{1}{q^k} \sum_{\lambda_1=1}^{q} \cdots \sum_{\lambda_k=1}^{q} \sum_{\underline{x}\in\mathcal{B}} \sum_{\underline{y}\in\mathcal{B}} \\
& e_q\left[\lambda_k \left(\sum_{i=1}^{n} x_i^k - \sum_{i=1}^{n} y_i^k\right) + \sum_{j=1}^{k-1} \lambda_j \left(\sum_{i=1}^{n} (x_i-c)^j - \sum_{i=1}^{n} (y_i-c)^j\right)\right] \\
= & \sum_{|h_1|\le n(B-1)} \cdots \sum_{|h_{k-1}|\le n(B^{k-1}-1)} J_{n,k}(B) \\
\le & \, 2^{k-1} n^{k-1} B^{\frac{k(k-1)}{2}} J_{n,k}(B).
\end{aligned}$$

If for some $j < k$ we have $n(B^{j-1}-1) < q/2 \le n(B^j - 1)$, then the upper bound can be improved by simply allowing $h_j, \ldots, h_{k-1}$ to each run through a complete residue system (mod 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, and so we obtain the second inequality in the theorem. □

4.4 Estimation of $J_{n,k}(B)$

Let $J^*_{n,k}(B)$ denote the number of integer solutions of the system of equations

$$\begin{aligned} x_1 + \cdots + x_n &= y_1 + \cdots + y_n, \\ x_1^2 + \cdots + x_n^2 &= y_1^2 + \cdots + y_n^2, \\ &\vdots \\ x_1^k + \cdots + x_n^k &= y_1^k + \cdots + y_n^k, \end{aligned} \tag{4.15}$$

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

We call a nonnegative real number $\Delta^*_{n,k}$ an admissible exponent for the system (4.15) if

$$J^*_{n,k}(B) \leq c_1(n,k) B^{2n - \frac{1}{2}k(k+1) + \Delta^*_{n,k}} \tag{4.16}$$

for some constant $c_1(n,k)$. In his seminal work on Waring's problem, Wooley [37, 38] established the following estimates for $J^*_{n,k}(B)$ and $\Delta^*_{n,k}$.

Lemma 4.4.1. *(i) [37, Theorem 1.1] Suppose that n and k are natural numbers with $k \geq 2$ and $n \geq k(k+1)$. Then for any $\epsilon > 0$ we can take $\Delta^*_{n,k} = \epsilon$.*

(ii) [37, Theorem 1.2] Suppose that $k \geq 3$. Then for $n \geq k^2 + k + 1$, we have

$$J^*_{n,k}(B) \sim c(n,k) B^{2n - \frac{1}{2}k(k+1)}, \tag{4.17}$$

for the positive constant $c(n,k)$ as given in (4.19) below. Consequently, for such n, k we can take $\Delta^*_{n,k} = 0$.

(iii) [38, Theorem 1.1] If $k \geq 3$ and $n \geq k^2 - 1$ then for any $\epsilon > 0$ we can take $\Delta^*_{n,k} = \epsilon$.

Recently, Bourgain, Demeter, and Guth proved the following.

Lemma 4.4.2. *[8] Let n and k be natural numbers such that $n \geq \frac{1}{2}k(k+1)$ and $k \geq 2$, and* *let $\varepsilon > 0$. Then*

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

Furthermore, if $n > \frac{1}{2}k(k+1)$, then

$$J^*_{n,k}(B) \sim c(n,k)B^{2n-\frac{1}{2}k(k+1)}, \tag{4.18}$$

where $c(n,k)$ is the positive constant in (4.19) below.

Define

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

and

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

Whenever the asymptotic formula in (4.17) is valid it is known that

$$c(n,k) = \mathfrak{S}(n,k)\mathfrak{J}(n,k). \tag{4.19}$$

In this case we can take the constant $c_1(n,k)$ in (4.16) to be $c(n,k)+\varepsilon$ for any $\varepsilon > 0$, provided that B is sufficiently large in terms of $\varepsilon, n,$and k. In Section 4.10 we show that

$$e^{\frac{73}{450}(k+1)(k+4)}\mathfrak{J}(n,k) < c(n,k) < \left(1 - \tfrac{k}{2}\right) e^{1.74(k^3+k^2+2k)}\mathfrak{J}(n,k).$$

It is shown in Arkhipov, Chubarikov and Karatsuba [3, Theorem 3.9] that for $n \geq 2k^2 \log k + k^2 \log\log k + 4.5k^2$,

$$J^*_{n,k}(B) \leq k^{30k^3} B^{2n-\frac{1}{2}k(k+1)}.$$

In [31, Theorem 1.1], Steiner proved that for $k \geq 3, n \geq k^2+k+2$, $\lambda = \frac{k^2+1}{k^2} > 1$ and

$B \geq n^{10}$, we have the estimate

$$J_{n,k}(B) \leq CB^{2n-\frac{1}{2}k(k+1)},$$

where C is the maximum of $4k^{30k^3}$ and

$$\left[e^{1.03973k^2+6.57361k+3.86874}k^{\frac{1}{2}k^2+\frac{19}{6}k-\frac{15}{2}+\frac{5}{2}D}e^{\frac{1}{2}\lambda k}\log(\lambda)^{\frac{5}{2}}\mathcal{M}_0\right]^{\frac{3.87}{68}\log(\lambda)k^{D+1}} \cdot 4(2k)^{2k+11},$$

where

$$D = \left\lceil \frac{4\log k + \log\log k + 4.2}{\log \lambda} \right\rceil$$

and

$$\mathcal{M}_0 = \max_{\gamma \in \{1, \frac{n-k}{n-2k}\}} \left\{ \left(e^{1.09658k^2+6.21267k-0.52770}k^{-\frac{1}{2}k^2+\frac{19}{3}k-4}(\lambda+1)^k e^{\frac{\lambda}{2\cdot 6^6}}\right)^{\gamma}, e^{-0.34657k^2-1.27076k+3.86874} \right\}.$$

Lemma 4.4.3. *For any integers $l_1, \ldots, l_k$ the number of integer solutions of the system*

$$\begin{aligned} x_1 + \cdots + x_n &= y_1 + \cdots + y_n + l_1, \\ x_1^2 + \cdots + x_n^2 &= y_1^2 + \cdots + y_n^2 + l_2, \\ &\vdots \\ x_1^k + \cdots + x_n^k &= y_1^k + \cdots + y_n^k + l_k, \end{aligned} \tag{4.20}$$

with $1 \leq x_i, y_i \leq B$ is at most $J^*_{n,k}(B)$.

Proof. Note that

$$\int_0^1 e^{2\pi i \lambda n}\, d\lambda = \begin{cases} 1, & n = 0; \\ 0, & n \in \mathbb{Z} \setminus \{0\}. \end{cases}$$

The number of solutions is given by

$$\begin{aligned}
&\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1} e^{2\pi i\lambda_1(x_1+\cdots-y_n-l_1)}\cdots e^{2\pi i\lambda_k(x_1^k+\cdots-y_n^k-l_k)}d\underline{\lambda}\\
&=\left|\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1}\prod_{i=1}^{k} e^{2\pi i\lambda_i(x_1^i+\cdots-y_n^i-l_i)}d\underline{\lambda}\right|\\
&=\left|\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1}\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\prod_{i=1}^{k} e^{2\pi i\lambda_i(x_1^i+\cdots-y_n^i-l_i)}d\underline{\lambda}\right|\\
&=\left|\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1}\prod_{i=1}^{k} e^{-2\pi i\lambda_i l_i}\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\prod_{i=1}^{k} e^{2\pi i\lambda_i(x_1^i+\cdots-y_n^i)}d\underline{\lambda}\right|\\
&\leq\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1}\left|\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\prod_{i=1}^{k} e^{2\pi i\lambda_i(x_1^i+\cdots-y_n^i)}\right|d\underline{\lambda}\\
&=\int_{\lambda_k=0}^{1}\cdots\int_{\lambda_1=0}^{1}\sum_{x_1=1}^{B}\cdots\sum_{y_n=1}^{B}\prod_{i=1}^{k} e^{2\pi i\lambda_i(x_1^i+\cdots-y_n^i)}d\underline{\lambda}\\
&=J_{n,k}^*(B). \qquad \square
\end{aligned}$$

Lemma 4.4.4. *If for some j with $1 \leq j \leq k$ we have that $n(B^{j-1}-1) < q/2 \leq n(B^j-1)$, then*

$$J_{n,k}(B) \leq 6c_1(n,k)(2n)^{k-j+1}q^{j-k-1}B^{2n-\frac{j(j-1)}{2}+\Delta_{n,k}^*}.$$

Remark 4.4.1. If $n > \frac{1}{2}k(k+1)$, then we may remove the $\Delta_{n,k}^*$ from the exponent of B by Lemma 4.4.2.

Proof. For $1 \leq t \leq j-1$ we have $n(B^t-1) < q/2$, and thus any integer solution of the congruence

$$x_1^t+\cdots+x_n^t \equiv y_1^t+\cdots+y_n^t \pmod q, \tag{4.21}$$

with $1 \leq x_i, y_i \leq B, 1 \leq i \leq n$, is in fact a solution of the equation

$$x_1^t+\cdots+x_n^t = y_1^t+\cdots+y_n^t.$$

For $t \geq j$ any solution of (4.21) is a solution of an integer equation of the form

$$x_1^t + \cdots + x_n^t = y_1^t + \cdots + y_n^t + l_t q$$

for some integer l_t with $|l_t| \leq n(B^t - 1)/q$. Thus there are at most $2\lfloor \frac{n}{q}(B^t - 1)\rfloor + 1$ choices for l_t, and altogether at most

$$\prod_{t=j}^{k} \left(2 \left\lfloor \frac{n}{q}(B^t - 1) \right\rfloor + 1 \right)$$

choices for $l_j, \ldots, l_k$. In order to simplify this product we define for $j \leq t \leq k$,

$$\beta_t := \frac{2\lfloor \frac{n}{q}(B^t - 1)\rfloor + 1}{\frac{2n}{q} B^t}.$$

Using the fact that $B^j - 1 \geq \frac{q}{2n}$, we have

$$\begin{aligned} \beta_t &\leq \frac{2\frac{n}{q}B^t - \frac{2n}{q} + 1}{\frac{2n}{q}B^t} = 1 + \frac{1 - \frac{2n}{q}}{\frac{2n}{q}B^j B^{t-j}} \\ &< 1 + \frac{1 - \frac{2n}{q}}{\frac{2n}{q}\frac{q}{2n}B^{t-j}} \\ &< 1 + \frac{1 - \frac{2n}{q}}{B^{t-j}} < 1 + \frac{1}{B^{t-j}}, \end{aligned}$$

and thus for $B \geq 2$,

$$\begin{aligned} \prod_{t=j}^{k} \beta_t &\leq \left(1 + \frac{1}{1}\right)\left(1 + \frac{1}{B}\right)\left(1 + \frac{1}{B^2}\right)\cdots\left(1 + \frac{1}{B^{k-j}}\right) \\ &< 2e^{\sum_{t=1}^{\infty} \frac{1}{B^t}} = 2e^{\frac{1}{B-1}} < 6. \end{aligned}$$

Therefore, the number of choices for $l_j, \ldots, l_k$ is at most

$$\prod_{t=j}^{k} \beta_t \frac{2n}{q} B^t < 6(2n)^{k-j+1} q^{j-k-1} B^{\frac{k(k+1)}{2} - \frac{j(j-1)}{2}}.$$

Each such choice of the l_t gives a system of the type (4.20) having at most $J^*_{n,k}(B)$ solutions, by the preceding lemma. The result now follows from the upper bound $J^*_{n,k}(B) \leq c_1(n,k)B^{2n-\frac{k(k+1)}{2}+\Delta^*_{n,k}}$. □

Theorem 4.4.1. *For any positive integers n, k and cube $\mathcal{B}$ as in (4.4), we have*

$$I_{n,k}(\mathcal{B}) \leq 6c_1(n,k)(2n)^k \max\left\{\frac{B^{2n}}{q}, B^{2n-k}\right\} B^{\Delta^*_{n,k}}. \tag{4.22}$$

Proof. If for some $j \leq k-1$ we have $n(B^{j-1}-1) < q/2 \leq n(B^j - 1)$, then by Lemma 4.4.4

$$J_{n,k}(B) \leq 6c_1(n,k)(2n)^{k-j+1}q^{j-k-1}B^{2n-\frac{j(j-1)}{2}+\Delta^*_{n,k}},$$

while by Proposition 4.3.1

$$I_{n,k}(\mathcal{B}) \leq (2n)^{j-1}B^{\frac{j(j-1)}{2}}q^{k-j}J_{n,k}(B) \leq 6c_1(n,k)(2n)^k B^{2n+\Delta^*_{n,k}}q^{-1}.$$

Similarly, if $n(B^{k-1}-1) < q/2 \leq n(B^k-1)$, then

$$J_{n,k}(B) \leq 6c_1(n,k)(2n)q^{-1}B^{2n-\frac{k(k-1)}{2}+\Delta^*_{n,k}},$$

while

$$I_{n,k}(\mathcal{B}) \leq (2n)^{k-1}B^{\frac{k(k-1)}{2}}J_{n,k}(B) \leq 6c_1(n,k)(2n)^k B^{2n+\Delta^*_{n,k}}q^{-1}.$$

Finally, if $n(B^k-1) < q/2$, then $J_{n,k}(B) = J^*_{n,k}(B) \leq c_1(n,k)B^{2n-\frac{k(k+1)}{2}+\Delta^*_{n,k}}$, and so

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

The theorem is now immediate. □

Corollary 4.4.1. *Let q, n, k be positive integers and $\mathcal{C}$ be any cube of edge length B as in*

(4.2) *with n replaced by $2n$. For any integers a_i with $(a_i, q) = 1$, $1 \leq i \leq 2n$, we have*

$$\#\left\{\mathbf{x} \in \mathcal{B} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod q\right\} \leq 6c_1(n,k)(2n)^k \max\left\{\frac{B^{2n}}{q}, B^{2n-k}\right\} B^{\Delta^*_{n,k}}.$$

Proof. For $1 \leq i \leq 2n$, let $S_i = \{x \in \mathbb{Z} : c_i + 1 \leq x \leq c_i + B\}$, making S_i^n a cube of type (4.4). By Theorem 4.4.1, we have

$$I_{n,k}(S_i^n) \leq 6c_1(n,k)(2n)^k \max\left\{\frac{B^{2n}}{q}, B^{2n-k}\right\} B^{\Delta^*_{n,k}}$$

for each of the cubes S_i^n, and thus the corollary follows immediately from Lemma 4.2.1. □

We are now in a position to prove Theorem 4.1.1.

Proof of Theorem 4.1.1. Let q, n, k be positive integers with $n \geq k^2 + k + 2$, $\mathcal{B}$ be any cube of edge length B as in (4.2), and a_i be integers with $a_0 \in \mathbb{Z}$ and $(a_i, q) = 1$, $1 \leq i \leq n$. It suffices to prove the upper bound for $n = k^2 + k + 2$. Indeed, if $n > k^2 + k + 2$, then for $k^2 + k + 2 < i \leq n$, we can assign any of the B possible values in the i-th interval to x_i, and apply the upper bound for $n = k^2 + k + 2$ to the resulting congruence. Set $m = \frac{k^2+k+2}{2}$. By the work of Bourgain, Demeter, and Guth [8], we can take $\Delta^*_{m,k} = 0$. Thus, by Corollary 4.4.1,

$$\#\{\mathbf{x} \in \mathcal{B} : \sum_{i=1}^{n} a_i x_i^k \equiv a_0 \pmod q\} \leq 6c_1(m,k)(2n)^k \max\left\{\frac{B^n}{q}, B^{n-k}\right\}.$$

□

4.5 Lower Bound on the Number of Values of a Diagonal Form $\pmod q$

For any cube $\mathcal{B}$ as in (4.2), 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 $\pmod q$ as $\mathbf{x}$ runs through $\mathcal{B}$,

$$S_{\mathcal{B}} := \{\sum_{i=1}^{n} a_i x_i^k \in \mathbb{Z}_q : \mathbf{x} \in \mathcal{B}\}, \tag{4.23}$$

and put

$$N_{\mathcal{B}} := \# \left\{ (\mathbf{x}, \mathbf{y}) \in \mathcal{B} \times \mathcal{B} : \sum_{i=1}^{n} a_i x_i^k \equiv \sum_{i=1}^{n} a_i y_i^k \pmod q \right\}. \tag{4.24}$$

Lemma 4.5.1. *For any cube $\mathcal{B}$ and diagonal form $\sum_{i=1}^{n} a_i x_i^k$, we have*

$$|S_{\mathcal{B}}| \geq B^{2n}/N_{\mathcal{B}}.$$

Proof. For any integer ν define n_ν by $n_\nu := \# \left\{ \underline{x} \in \mathcal{B} \mid \sum_{i=1}^{n} a_i x_i^k \equiv \nu \pmod q \right\}$. Then by the Cauchy-Schwarz inequality,

$$B^n = |\mathcal{B}| = \sum_{\nu=1}^{q} (1 \cdot n_\nu) \leq \left(\sum_{\substack{\nu=1 \\ n_\nu \neq 0}}^{q} 1 \right)^{1/2} \left(\sum_{\nu=1}^{q} n_\nu^2 \right)^{1/2}.$$

After squaring both ends of the inequality, we arrive at

$$B^{2n} \leq \left(\sum_{\substack{\nu=1 \\ n_\nu \neq 0}}^{q} 1 \right) \left(\sum_{\nu=1}^{q} n_\nu^2 \right),$$

where $\sum_{\substack{\nu=1 \\ n_\nu \neq 0}}^{q} 1$ is the number of values of ν that can be represented as $\sum_{i=1}^{n} a_i x_i^k \equiv \nu \pmod q$

with $\underline{x} \in \mathcal{B}$ and $\sum_{\nu=1}^{q} n_\nu^2$ is the number of solutions to $\sum_{i=1}^{n} a_i x_i^k \equiv \sum_{i=1}^{n} a_i y_i^k \pmod q$ with $\underline{x}, \underline{y} \in \mathcal{B}$. That is,

$$B^{2n} \le \left|S_{\mathcal{B}}\right| \cdot N_{\mathcal{B}}.$$

One now only needs to divide both sides of the inequality by $N_{\mathcal{B}}$ to complete the proof. □

By Theorem 4.1.1, if $(a_i, q) = 1$, $1 \le i \le n$, then for any cube $\mathcal{B}$,

$$N_{\mathcal{B}} \le 6c_1(n,k)(2n)^k \max\left\{\frac{B^{2n}}{q}, B^{2n-k}\right\} B^{\Delta^*_{n,k}}, \tag{4.25}$$

and so we derive from the preceding lemma the following result.

Corollary 4.5.1. *For any positive integers k, n, q, integers a_i with $(a_i, q) = 1$, $1 \le i \le n$, and cube $\mathcal{B}$ as in (4.2) of edge length B, we have*

i) If $B^k \le q$ then

$$|S_{\mathcal{B}}| \ge \frac{1}{6} c_1(n,k)^{-1}(2n)^{-k} B^{k-\Delta^*_{n,k}}, \tag{4.26}$$

where $c_1(n,k)$ is the constant in (4.16).

ii) If $B^k \ge q$ then

$$|S_{\mathcal{B}}| \ge \frac{1}{6} c_1(n,k)^{-1}(2n)^{-k} B^{-\Delta^*_{n,k}} q. \tag{4.27}$$

4.6 Solutions of a Diagonal Congruence $\pmod q$ in a Cube

We return now to obtaining solutions to the diagonal congruence

$$a_1 x_1^k + \cdots + a_n x_n^k \equiv c \pmod q, \tag{4.28}$$

in a cube.

Lemma 4.6.1. *For any cube $\mathcal{B}$ as in* (4.2)*, and diagonal form* $\sum_{i=1}^{n} a_i x_i^k$ *with* $(a_i, q) = 1$*,* $1 \le i \le n$*, the value set* $S_{\mathcal{B}}$ *is contained in a coset of a proper additive subgroup of* $\mathbb{Z}_q$ *if and only if there exists a prime divisor* $p|q$*, such that* $x^k \pmod{p}$ *is constant on every edge* $[c_i + 1, c_i + B]$ *of the cube.*

Proof. Suppose that $S_{\mathcal{B}}$ is contained in a coset $p\mathbb{Z}_q + l$ for some $p|q$, $p \ne 1$, and $l \in \mathbb{Z}$. We may assume that p is a prime by enlarging the subgroup if necessary. Thus, for all $\underline{x} \in \mathcal{B}$ we have $\sum_{i=1}^{n} a_i x_i^k \equiv l \pmod{p}$. In particular, $x_i^k \pmod{p}$ must be constant on the interval $[c_i + 1, c_i + B]$. The converse is trivial. □

Theorem 4.6.1. *For any positive integer* k*, there exists a constant* $c_5(k)$ *such that for any positive integers* n, q *with* $n > c_5(k)$ *and cube* $\mathcal{B}$ *of type* (4.2) *with side length* $B \ge (q/k^2)^{1/k}$*, such that for any prime factor* p *of* q*, the* k*-th powers* $\pmod{p}$ *are not constant on any edge* $[c_i + 1, c_i + B]$ *of* $\mathcal{B}$*, there exists a solution of* (4.28) *in* $\mathcal{B}$*.*

The constant $(1/k^2)^{1/k}$ in the size of B required for success can be reduced further at the expense of increasing the value of $c_5(k)$, given in (4.31).

Proof. Set $n_1 := \frac{k^2+k+2}{2}$. We may assume that $n > 2(2^{k-1}n_1)^{\frac{\log 2}{\log 1.5}}$. Suppose first that $q \le 2^k n_1$. For $1 \le i \le n$ set

$$A_i := \{a_i x_i^k \pmod{q} : c_i + 1 \le x_i \le c_i + B\}.$$

By the assumption that the k-th powers $\pmod{p}$ are not constant on $[c_i+1, c_i+B]$, we know by Lemma 4.6.1 that the A_i are not contained in a coset of any proper additive subgroup of $\mathbb{Z}_q$. Moreover, each A_i has cardinality at least 2. Thus by Corollary 2.7.1

$$|A_1 + \cdots + A_n| \ge \min\{q, 2(n/2)^{\frac{\log 1.5}{\log 2}}\} = q,$$

the latter equality following from our assumption on the size of n and q.

Suppose next that $q > 2^k n_1$. Let $\mathcal{B}$ be any cube in n variables with edge length B satisfying $\frac{1}{2}(q/n_1)^{1/k} \le B < (q/n_1)^{1/k}$. Note $\frac{1}{2}(q/n_1)^{1/k} > 1$ by our assumption on the size of q, so such an integer B will exist. Divide the n variables into $L := \lfloor \frac{n}{n_1} \rfloor$ sets each with at least n_1 variables and no more than $2n_1$ variables; let $\mathcal{B}_i$ be the cube corresponding to the i-th set of variables, $1 \leq i \leq L$, and $S_i = S_{\mathcal{B}_i}$, the set of values assumed by the sum over the i-th set of variables. To be clear, the first set of variables will have n_1 variables. If say $x_1, \ldots, x_{n_1}$ is the first set of variables, then S_1 is the value set of the diagonal form $a_1 x_1^k + \cdots + a_{n_1} x_{n_1}^k \pmod{q}$, as the x_i run through the intervals $[c_i + 1, c_i + B]$, $1 \leq i \leq n_1$, and so on.

Let us define $C_1 := \dfrac{1}{6} \max\limits_{n_1 \leq n_1^* < 2n_1} \{c_1(n_1^*, k)(2n_1^*)^k\}$ with $c_1(n, k)$ as given in (4.16). Since $n_1 B^k < n_1 q / n_1 = q$, it follows by Corollary 4.5.1 that for $1 \leq i \leq L$,

$$|S_i| \geq C_1^{-1} B^k \geq c_2(k) q, \tag{4.29}$$

for some constant $c_2(k)$, which we may take to be

$$c_2(k) := (2C_1 n_1)^{-1}. \tag{4.30}$$

By Lemma 4.6.1 the S_i are not contained in a coset of any proper additive subgroup of $\mathbb{Z}_q$ (by our assumption that the k-th powers are not constant $\pmod{p}$ on any edge of $\mathcal{B}$ for prime $p|q$), and thus by Corollary 2.7.1,

$$|S_1 + \cdots + S_L| \geq \min\{q, (L/2)^{\frac{\log 1.5}{\log 2}} c_2(k) q\}.$$

Since $c_2(k) < 1$, if $L \geq 2c_2(k)^{-2}$, we conclude that $S_1 + \cdots + S_L = \mathbb{Z}_q$. Since $L = \lfloor \frac{n}{n_1} \rfloor$, it suffices to have

$$n \geq (2c_2(k)^{-2} + 1) \left(\frac{k^2 + k + 2}{2} \right) =: c_5(k). \tag{4.31}$$

□

4.7 Small Solutions of a Diagonal Congruence with Prime Modulus

For prime moduli and boxes cornered at the origin, we obtain a result that allows the number of variables to be much smaller, at the expense of a slightly larger solution. We make use of the following lemma due to Sárközy [26].

Lemma 4.7.1. *[26, 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 is the following lemma.

Lemma 4.7.2. *If A_1, B_1, A_2, B_2 are subsets of $\mathbb{Z}_p$ with $|A_1||B_1||A_2||B_2| > p^3$, then $A_1B_1 + A_2 + B_2 = \mathbb{Z}_p$.*

Proof. For any $x \in \mathbb{Z}_p$, apply Sárközy's Lemma with $A = A_2 - x, B = B_2, C = -A_1, D = B_1$. □

Theorem 4.7.1. *For any positive integer k there exists a constant $\kappa_1(k)$ such that for any positive integer $n \geq \frac{3}{2}(k^2 + k + 2)$, prime p, and integers c, a_i with $p \nmid a_i, 1 \leq i \leq n$, there exists a solution of*

$$a_1x_1^k + \cdots + a_nx_n^k \equiv c \pmod{p}, \tag{4.32}$$

with $1 \leq x_i \leq \kappa_1(k)p^{\frac{1}{k}}$.

Proof. Put $n_1 = \frac{k^2+k+2}{2}$ and assume $n \geq 3n_1$. We may also assume $\kappa_1(k) > \max\{2^kn_1, k/c_2(k)^3\}$, with $c_2(k)$ as given in (4.30). If $p \leq \max\{2^kn_1, k/c_2(k)^3\} < \kappa_1(k)$, the result is trivial. In this case the x_i are allowed to run through a complete residue system $\pmod{p}$, and since $\Gamma(k,p) \leq k$ by Theorem 2.6.1, it suffices to have $n \geq k$. Thus we may assume that $p > \max\{2^kn_1, k/c_2(k)^3\}$.

Let $\mathcal{B}$ be the cube $1 \leq x_i \leq B$, $1 \leq i \leq n$, in n variables with side length B satisfying $\frac{1}{2}(p/n_1)^{1/k} \leq B < (p/n_1)^{1/k}$. Such an integer B exists since $p > 2^kn_1$. Divide the n variables into three sets, say F_1, F_2, F_3, each with at least n_1 variables. Say that F_j has f_j-many variables with $f_j \geq n_1, 1 \leq j \leq 3$. Let $\mathcal{B}_i$ be the cube corresponding to the i-th set of variables, and let A_1, A_2, B_2 be the value sets of the diagonal sums over each of these sets of variables. Thus, for the first set of variables, F_1, we have that

$$A_1 = \{a_1 x_1^k + \cdots + a_{f_1} x_{f_1}^k \pmod{p} : 1 \leq x_i \leq B, 1 \leq i \leq f_1\}$$

and similarly for A_2 and B_2. Put $B_1 := \{1^k, 2^k, \ldots, L^k\} \subseteq \mathbb{Z}_p$ (with L a parameter to be chosen later), which is a set with at least L/k distinct values $\pmod{p}$ assuming that $L \leq p$. As in (4.29) we have,

$$|A_1|, |A_2|, |B_2| \gg c_2(k)p. \tag{4.33}$$

Thus, if $L \leq p$ and $c_2(k)^3 p^3 L/k > p^3$, we can apply Lemma 4.7.2 to obtain $A_1B_1 + A_2 + B_2 = \mathbb{Z}_p$. It suffices to take $L = \lceil \frac{k}{c_2(k)^3} \rceil$, a value that is at most p by our assumption that $p > k/c_2(k)^3$. If the first set of variables is $x_1, \ldots, x_\ell$, then

$$A_1B_1 = \left\{ \textstyle\sum_{i=1}^{\ell} a_i (yx_i)^k \pmod{p} : 1 \leq y \leq L, 1 \leq x_i \leq B, 1 \leq i \leq \ell \right\}.$$

Here $1 \leq yx_i \leq LB < L(p/n_1)^{1/k} \leq \kappa_1(k)p^{1/k}$ for some constant $\kappa_1(k)$.

□

Remark 4.7.1. 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. In this way we can obtain a solution of (4.32) with roughly one third of the variables restricted to the interval $[1, B]$, and the other two thirds in arbitrary intervals of length $B \gg \kappa_1 p^{1/k}$.

Remark 4.7.2. The constant κ_1 in Theorem 4.7.1 may be taken to be

$$\kappa_1 = \frac{\left\lceil \frac{k}{c_2(k)^3} \right\rceil}{n_1^{\frac{1}{k}}} = \frac{\lceil (2C_1 n_1)^3 k \rceil}{n_1^{\frac{1}{k}}}$$

where $c_2(k)$ is as in (4.30).

4.8 Smooth Solutions (mod q)

Let k, q, n, ℓ, and B be positive integers and $\mathcal{A} = \mathcal{A}(B, B^{\frac{1}{\ell}})$ be the set of $B^{\frac{1}{\ell}}$-smooth numbers defined by

$$\mathcal{A} := \{x \in [1, B] \cap \mathbb{Z} : p \text{ prime}, \, p|x \Rightarrow p \leq B^{\frac{1}{\ell}}\}. \tag{4.34}$$

By the work of Ramaswami [24], we have

$$|\mathcal{A}| = |\mathcal{A}(B, B^{\frac{1}{\ell}})| = B\rho(\ell) + \mathrm{O}\left(\frac{B}{\log B}\right), \tag{4.35}$$

where $\rho(\ell)$ is the Dickman function. Put

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

The following definition and lemma are from [35, §2].

Definition 4.8.1. *[35, §2, p. 4] We call an exponent $\Delta_{n,k}$ permissible when*

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

Lemma 4.8.1. *[35, Lemma 2.1] For $k \geq 4$, $n \geq 2$, let $\Delta_{n,k}$ be the unique positive solution of the equation $\Delta_{n,k} e^{\frac{\Delta_{n,k}}{k}} = ke^{1-2n/k}$. Then $\Delta_{n,k}$ is permissible. In particular, the exponent $\Delta^*_{n,k} = ke^{1-2n/k}$ is permissible.*

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

$$\Delta^*_{n,k} := ke^{1-2n/k} \leq ke^{1-\log(ek/\delta)} = \delta. \tag{4.36}$$

Now we define

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

Note that if we assume that $B^k < \frac{q}{n}$, then any solution of $\sum_{i=1}^{n}(x_i^k - y_i^k) \equiv 0 \pmod{q}$ is a solution of $\sum_{i=1}^{n}(x_i^k - y_i^k) = 0$. That is, if we assume that $B^k < \frac{q}{n}$, then $I_{n,k}(\mathcal{A}^n) = I^*_{n,k}(\mathcal{A}^n)$.

Corollary 4.8.1. *For any integers a_i with $(a_i, q) = 1$ for $1 \le i \le 2n$, $B^k < q/n$, and any permissible exponent $\Delta_{n,k}$ we have*

$$\#\left\{\underline{x} \in \mathcal{A}^{2n} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\right\} \le c(\varepsilon, k, \ell, n) B^{2n-k+\varepsilon+\Delta_{n,k}}.$$

Proof. Applying Lemma 4.2.1 with $S_i = \mathcal{A}$ with $\mathcal{A}$ as in (4.34), $1 \le i \le 2n$, we have that

$$\begin{aligned}
&\#\left\{\underline{x} \in \mathcal{A}^{2n} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\right\} \\
&= \#\left\{\underline{x} \in S_1 \times \cdots \times S_{2n} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\right\} \\
&\le \prod_{i=1}^{2n} I_{n,k}(S_i^n)^{\frac{1}{2n}} \\
&= I_{n,k}(\mathcal{A}^n).
\end{aligned}$$

By Definition 4.8.1, for any permissible $\Delta_{n,k}$, we have

$$I_{n,k}(\mathcal{A}^n) \le c(\varepsilon, k, \ell, n) B^{2n-k+\varepsilon+\Delta_{n,k}},$$

and so

$$\#\left\{\underline{x} \in \mathcal{A}^{2n} : \sum_{i=1}^{2n} a_i x_i^k \equiv a_0 \pmod{q}\right\} \le c(\varepsilon, k, \ell, n) B^{2n-k+\varepsilon+\Delta_{n,k}}.$$

□

Letting $N_{\mathcal{A}^n}$ denote the value

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

we have as a special case of the corollary that if $\Delta_{n,k}$ is a permissible exponent, then

$$N_{\mathcal{A}^n} \le c(\varepsilon, k, \ell, n) B^{2n-k+\varepsilon+\Delta_{n,k}}. \tag{4.37}$$

Corollary 4.8.2. *Let* $S_{\mathcal{A}^n} := \left\{ \sum_{i=1}^{n} a_i x_i^k \in \mathbb{Z}_q : \underline{x} \in \mathcal{A}^n \right\}$. *If* $B^k < q/n$ *then*

$$|S_{\mathcal{A}^n}| \ge \tfrac{1}{2}\rho(\ell)^{2n} B^{2n} / N_{\mathcal{A}^n} \ge \tilde{c} B^{k-\varepsilon-\Delta_{n,k}},$$

where $\tilde{c} := \frac{1}{2}\rho(\ell)^{2n} c(\varepsilon, k, \ell, n)^{-1}$.

Proof. Define n_ν by $n_\nu := \#\left\{ \underline{x} \in \mathcal{A}^n \;\middle|\; \sum_{i=1}^{n} a_i x_i^k \equiv \nu \pmod{q} \right\}$. Then by the Cauchy-Schwarz inequality,

$$|\mathcal{A}^n| = \sum_{\nu=1}^{q} (1 \cdot n_\nu) \le \left(\sum_{\substack{\nu=1 \\ n_\nu \ne 0}}^{q} 1 \right)^{1/2} \left(\sum_{\nu=1}^{q} n_\nu^2 \right)^{1/2}.$$

For B sufficiently large, say $B \ge B_0(n, \ell)$, we have by (4.35), that $|\mathcal{A}| \ge \left(\frac{1}{2}\right)^{\frac{1}{2n}} \rho(\ell) B$. Hence, after squaring both ends of the inequality and using our lower bound on $|\mathcal{A}|$, we arrive at

$$\tfrac{1}{2}\rho(\ell)^{2n} B^{2n} \le |\mathcal{A}|^{2n} \le \left(\sum_{\substack{\nu=1 \\ n_\nu \ne 0}}^{q} 1 \right) \left(\sum_{\nu=1}^{q} n_\nu^2 \right)$$

where $\sum_{\substack{\nu=1 \\ n_\nu \ne 0}}^{q} 1$ is the number of values of ν that can be represented as $\sum_{i=1}^{n} a_i x_i^k \equiv \nu \pmod{q}$

with $\underline{x} \in \mathcal{A}^n$ and $\displaystyle\sum_{\nu=1}^{q} n_\nu^2 = \# \left\{ (\underline{x}, \underline{y}) \in \mathcal{A}^{2n} \middle| \sum_{i=1}^{n} a_i x_i^k \equiv \sum_{i=1}^{n} a_i y_i^k \pmod q \right\}$. That is,

$$\tfrac{1}{2}\rho(\ell)^{2n} B^{2n} \leq \left| S_{\mathcal{A}^n} \right| \cdot N_{\mathcal{A}^n}.$$

One now only needs to divide both sides of the inequality by $N_{\mathcal{A}^n}$ and apply the bound in (4.37). □

4.9 Small Solutions $\pmod p$ with a Small Number of Variables

Next, we use the results of the previous section to find small solutions of (1.8) with a prime modulus.

Theorem 4.9.1. *For any positive $\varepsilon < 1$, $k \geq 4$, $n > \frac{3}{2}k\log(3e/\varepsilon) + 3$, prime p, and integers a_i, $0 \leq i \leq n$ with $p \nmid a_i$, $1 \leq i \leq n$, there is a solution of (1.8) with*

$$1 \leq x_i \ll_{\varepsilon,n,k} p^{\frac{1}{k}+\varepsilon}, \qquad 1 \leq i \leq n. \tag{4.38}$$

Proof. Let $n > \frac{3}{2}k\log(3e/\varepsilon) + 3$, $m = \lfloor \frac{n}{3} \rfloor$, $B = \lfloor \left(\frac{3p}{n}\right)^{\frac{1}{k}} \rfloor$. Since $n > k$, we know by Theorem 2.6.1 that (1.8) is solvable for any odd prime p. Thus by taking the implied constant in (4.38) 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 $B \geq 1$. 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

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

and define A_2 and B_2 similarly for the second and third sets of variables.

Note that $m \geq \frac{n}{3} - 1 > \frac{1}{2}k\log(3e/\varepsilon)$, and so by (4.36) with $\delta = \frac{\varepsilon k}{3}$, $\Delta^*_{m,k} < \frac{\varepsilon k}{3}$, that is, there exists an $\varepsilon' > 0$ such that $\frac{\varepsilon k}{3} - \varepsilon'$ is a permissible exponent. Also, $B^k \leq \frac{3p}{n} \leq \frac{p}{m}$. Thus, by Corollary 4.8.2 (with the ε in the corollary taken to be ε') we obtain

$$|A_1|, |A_2|, |B_2| \geq \tilde{c} B^{k - k\varepsilon/3},$$

for some constant $\tilde{c}$ depending on ε, k, ℓ and n. Now $3^{1/k} \geq e^{1/k} \geq 1 + \frac{1}{k}$, and so for $p > nk^k$ we have

$$B \geq (3p/n)^{1/k} - 1 \geq \left(1 + \frac{1}{k}\right)(p/n)^{1/k} - 1 = (p/n)^{1/k} + \frac{1}{k}(p/n)^{1/k} - 1 > (p/n)^{1/k}.$$

Thus for $p > nk^k$,

$$|A_1|, |A_2|, |B_2| \geq \tilde{c}(p/n)^{\frac{1}{k}(k - k\varepsilon/3)} = \tilde{c}(p/n)^{1-\varepsilon/3}.$$

Let $B_1 = \{1^k, 2^k, 3^k, \ldots, L^k\} \subseteq \mathbb{Z}_p$, a set with at least L/k distinct values $\pmod p$, assuming that $L \leq p$. Thus, for $p > nk^k$ and $L \leq p$,

$$\prod_{i=1}^{2} |A_i||B_i| \geq \tilde{c}^3 (p/n)^{3-\varepsilon} L/k \geq p^3,$$

provided that $L \geq k\tilde{c}^{-3}(p/n)^{\varepsilon}$. Letting L be the smallest integer satisfying this inequality, we have $L \leq p$ for p sufficiently large, and thus by Lemma 4.7.2, there exists a solution of (1.8) with

$$1 \leq x_i \leq LB \leq 2k\tilde{c}^{-3}(p/n)^{\varepsilon}(3p/n)^{1/k} = \kappa_2(\varepsilon, n, k) p^{\frac{1}{k}+\varepsilon},$$

for $1 \leq i \leq n$. □

Remark 4.9.1. An equivalent formulation of Theorem 4.9.1 may be stated as follows:

For $k \geq 4$, $n \geq k$, prime p, and integers a_i, $0 \leq i \leq n$ with $p \nmid a_i$, $1 \leq i \leq n$, there is a solution of (1.8) with

$$1 \leq x_i \ll_{\varepsilon,n,k} p^{\frac{1}{k}} + 3\exp\left(1 - \tfrac{2}{3}\tfrac{n-3}{k}\right).$$

Remark 4.9.2. By restricting the values in B_1 to smooth numbers, we can in fact obtain a solution of (1.8) with all of the variables smooth.

Letting $\varepsilon = \frac{1}{2} - \frac{1}{k}$, we see that if $n > \frac{3}{2}k \log\left(\frac{6ek}{k-2}\right) + 3$ or rather if $n > 5.23k + 3$ we obtain the following corollary.

Corollary 4.9.1. *If $k \geq 4$ and $n > 5.23k + 3$, then there exists a solution of (1.8) with $1 \leq x_i \ll \sqrt{p}$.*

4.10 Estimation of $c(n,k)$

Define

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

and

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

Then when the asymptotic formula in (4.17) is valid we have

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

For $q, k, n, \lambda_i \in \mathbb{N}, 1 \leq i \leq k$, we define

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

Theorem 4.10.1. *$S(q)$ is a multiplicative function. Furthermore,*

$$\mathfrak{S}(n,k) = \prod_{p \text{ prime}} \left(S(1) + S(p) + S(p^2) + \cdots\right).$$

Proof. Recall that

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

Write $\mathfrak{S}(n,k) = \sum\limits_{q=1}^{\infty} S(q)$. Let a, b be positive integers such that $(a,b) = 1$. Write $\underline{a} = (a,\ldots,a)$, $\underline{b} = (b,\ldots,b)$, $\underline{1} = (1,\ldots,1)$, $\underline{\alpha} = (\alpha_1,\ldots,\alpha_k)$, $\underline{\beta} = (\beta_1,\ldots,\beta_k)$, and $\underline{\lambda} = (\lambda_1,\ldots,\lambda_k)$. Let us define

$$\sum_{\underline{\alpha}=\underline{1}}^{\underline{a}} := \sum_{\alpha_1=1}^{a} \cdots \sum_{\alpha_k=1}^{a}$$

and similarly

$$\sum_{\underline{\beta}=\underline{1}}^{\underline{b}} := \sum_{\beta_1=1}^{b} \cdots \sum_{\beta_k=1}^{b}$$

Then we can write both

$$S(a) = \sum_{\substack{\underline{\alpha}=\underline{1} \\ (\alpha_1,\ldots,\alpha_k,a)=1}}^{\underline{a}} \left| a^{-1} \sum_{x=1}^{a} e_a(\underline{\alpha}\cdot(x,\ldots,x^k)) \right|^{2n}$$

and

$$S(b) = \sum_{\substack{\underline{\beta}=\underline{1} \\ (\beta_1,\ldots,\beta_k,b)=1}}^{\underline{b}} \left| b^{-1} \sum_{y=1}^{b} e_b(\underline{\beta}\cdot(y,\ldots,y^k)) \right|^{2n}.$$

Let us begin by examining the inner sums

$$\sum_{x=1}^{a} e_a(\underline{\alpha}\cdot(x,\ldots,x^k)) \qquad \text{and} \qquad \sum_{y=1}^{b} e_b(\underline{\beta}\cdot(y,\ldots,y^k)).$$

First, we note that for a polynomial function $f(x) = \sum_{i=1}^{k} \lambda_i x^i$, the sum $\sum_{x=1}^{ab} e_{ab}(f(x))$ can be reduced using the correspondence $x \longleftrightarrow bu + av$ where $1 \le u \le a$ and $1 \le v \le b$.

For a general power k of $bu + av$ we have

$$\begin{aligned}(bu+av)^k &= b^k u^k + \binom{k}{1}(bu)^{k-1}av + \cdots + \binom{k}{1}(av)^{k-1}bu + a^k v^k \\ &\equiv b^k u^k + a^k v^k \pmod{ab}.\end{aligned}$$

Thus,

$$\begin{aligned}\sum_{x=1}^{ab} e_{ab}(f(x)) &= \sum_{u=1}^{a}\sum_{v=1}^{b} e_{ab}(f(bu+av)) \\ &= \sum_{u=1}^{a}\sum_{v=1}^{b} e_{ab}\left(\sum_{i=1}^{k}\lambda_i(bu+av)^i\right) \\ &= \sum_{u=1}^{a}\sum_{v=1}^{b} e_{ab}\left(\sum_{i=1}^{k}\lambda_i(b^i u^i + a^i v^i)\right) \\ &= \sum_{u=1}^{a} e_{ab}\left(\sum_{i=1}^{k}\lambda_i b^i u^i\right)\sum_{v=1}^{b} e_{ab}\left(\sum_{i=1}^{k}\lambda_i a^i v^i\right) \\ &= \sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k}\lambda_i b^{i-1} u^i\right)\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k}\lambda_i a^{i-1} v^i\right).\end{aligned}$$

Second, we note that for $\lambda_i = b\zeta_i + a\gamma_i$ $(1 \le i \le k)$,

$$\begin{aligned}(\lambda_1,\ldots,\lambda_k,ab) = 1 &\Longleftrightarrow (\lambda_1,\ldots,\lambda_k,a) = 1 \text{ and } (\lambda_1,\ldots,\lambda_k,b) = 1 \\ &\Longleftrightarrow (b\zeta_1 + a\gamma_1,\ldots,b\zeta_k + a\gamma_k,a) = 1 \text{ and } (b\zeta_1 + a\gamma_1,\ldots,b\zeta_k + a\gamma_k,b) = 1 \\ &\Longleftrightarrow (b\zeta_1,\ldots,b\zeta_k,a) = 1 \text{ and } (a\gamma_1,\ldots,a\gamma_k,b) = 1 \\ &\Longleftrightarrow (\zeta_1,\ldots,\zeta_k,a) = 1 \text{ and } (\gamma_1,\ldots,\gamma_k,b) = 1.\end{aligned}$$

Finally,

$$\begin{aligned}
&S(ab)\\
&= \sum_{\substack{\underline{\lambda}=\underline{1}\\(\lambda_1,\ldots,\lambda_k,ab)=1}}^{\underline{ab}} \left|(ab)^{-1}\sum_{x=1}^{ab} e_{ab}\left(\sum_{i=1}^{k}(\lambda_i x^i)\right)\right|^{2n}\\
&= \sum_{\substack{\underline{\lambda}=\underline{1}\\(\lambda_1,\ldots,\lambda_k,ab)=1}}^{\underline{ab}} \left|(ab)^{-1}\sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k}(\lambda_i b^{i-1}u^i)\right)\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k}(\lambda_i a^{i-1}v^i)\right)\right|^{2n}.
\end{aligned}$$

Making the substitution $\lambda_i = b\zeta_i + a\gamma_i$, we reach

$$\begin{aligned}
S(ab) &= \sum_{\substack{\underline{\zeta}=\underline{1}\\(\zeta_1,\ldots,\zeta_k,a)=1\\(\gamma_1,\ldots,\gamma_k,b)=1}}^{\underline{a}}\sum_{\underline{\gamma}=\underline{1}}^{\underline{b}} \left|(ab)^{-1}\sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k}((b\zeta_i+a\gamma_i)b^{i-1}u^i)\right)\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k}((b\zeta_i+a\gamma_i)a^{i-1}v^i)\right)\right|^{2n}\\
&= \sum_{\substack{\underline{\zeta}=\underline{1}\\(\zeta_1,\ldots,\zeta_k,a)=1\\(\gamma_1,\ldots,\gamma_k,b)=1}}^{\underline{a}}\sum_{\underline{\gamma}=\underline{1}}^{\underline{b}} \left|(ab)^{-1}\sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k}(\zeta_i b^i u^i + ab^{i-1}\gamma_i u^i)\right)\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k}(ba^{i-1}\zeta_i v^i + a^i\gamma_i v^i)\right)\right|^{2n}\\
&= \sum_{\substack{\underline{\zeta}=\underline{1}\\(\zeta_1,\ldots,\zeta_k,a)=1\\(\gamma_1,\ldots,\gamma_k,b)=1}}^{\underline{a}}\sum_{\underline{\gamma}=\underline{1}}^{\underline{b}} \left|(ab)^{-1}\sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k} b^i\zeta_i u^i\right)\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k} a^i\gamma_i v^i\right)\right|^{2n}\\
&= \sum_{\substack{\underline{\zeta}=\underline{1}\\(\zeta_1,\ldots,\zeta_k,a)=1}}^{\underline{a}} \left|a^{-1}\sum_{u=1}^{a} e_{a}\left(\sum_{i=1}^{k} b^i\zeta_i u^i\right)\right|^{2n} \sum_{\substack{\underline{\gamma}=\underline{1}\\(\gamma_1,\ldots,\gamma_k,b)=1}}^{\underline{b}} \left|b^{-1}\sum_{v=1}^{b} e_{b}\left(\sum_{i=1}^{k} a^i\gamma_i v^i\right)\right|^{2n}\\
&= \left(\sum_{\substack{\underline{\alpha}=\underline{1}\\(\alpha_1,\ldots,\alpha_k,a)=1}}^{\underline{a}} \left|a^{-1}\sum_{x=1}^{a} e_{a}\left(\sum_{i=1}^{k} \alpha_i x^i\right)\right|^{2n}\right)\left(\sum_{\substack{\underline{\beta}=\underline{1}\\(\beta_1,\ldots,\beta_k,b)=1}}^{\underline{b}} \left|b^{-1}\sum_{y=1}^{b} e_{b}\left(\sum_{i=1}^{k} \beta_i y^i\right)\right|^{2n}\right)\\
&= S(a)S(b),
\end{aligned}$$

where the penultimate equality is due to the substitution $b^i\zeta_i = \alpha_i$ and $a^i\gamma_i = \beta_i$ for each

$1 \leq i \leq k$. Thus, $S(q)$ is a multiplicative function, implying that

$$\mathfrak{S}(n,k) = \prod_{p \text{ prime}} \left(S(1) + S(p) + S(p^2) + \cdots\right).$$

□

For integers $\lambda_i \in \mathbb{Z}, 0 \leq i \leq k$, let $f(x) = \lambda_0 + \lambda_1 x + \cdots + \lambda_k x^k$ and

$$S(f,q) := \sum_{x=1}^{q} e_q \left(\lambda_0 + \lambda_1 x + \cdots + \lambda_k x^k\right).$$

Currently, the best upper bounds known for $S(f,q)$ are

$$|S(f,q)| \leq e^{k + O(\frac{k}{\log k})} q^{1-\frac{1}{k}},$$

if $(\lambda_1, \ldots, \lambda_k, q) = 1$, due to Stečkin [30], and

$$|S(f,q)| \leq e^{1.74k} q^{1-\frac{1}{k}}, \tag{4.39}$$

if $(\lambda_1, \ldots, \lambda_k, q) = 1$ and $k \geq 3$, due to Qi and Ding [23].

Theorem 4.10.2. *(i) For $n \geq (k^2+k+2)/2$ and $k \geq 2$, we have*

$$\mathfrak{S}(n,k) \leq \left(1 + \tfrac{k}{2}\right) e^{1.74(k^3+k^2+2k)}.$$

(ii) For all n we have $\mathfrak{S}(n,k) \geq e^{\frac{\log 6}{30}(k+1)(k+4)}$.

Proof. (i) Using the upper bound on $S(f,q)$ in (4.39), we have that

$$\begin{aligned}
\mathfrak{S}(n,k) &= \sum_{q=1}^{\infty} \sum_{\substack{\lambda_1=1 \\ (\lambda_1,\ldots,\lambda_k,q)=1}}^{q} \cdots \sum_{\lambda_k=1}^{q} \left| q^{-1} \sum_{x=1}^{q} e_q\left(\lambda_1 x + \cdots + \lambda_k x^k\right) \right|^{2n} \\
&\le \sum_{q=1}^{\infty} \sum_{\substack{\lambda_1=1 \\ (\lambda_1,\ldots,\lambda_k,q)=1}}^{q} \cdots \sum_{\lambda_k=1}^{q} \left| q^{-1} e^{1.74k} q^{1-\frac{1}{k}} \right|^{2n} \\
&= \sum_{q=1}^{\infty} \sum_{\substack{\lambda_1=1 \\ (\lambda_1,\ldots,\lambda_k,q)=1}}^{q} \cdots \sum_{\lambda_k=1}^{q} e^{3.48kn} q^{-\frac{2n}{k}} \\
&\le e^{3.48kn} \sum_{q=1}^{\infty} q^{k-\frac{2n}{k}}.
\end{aligned}$$

For $n > \frac{k^2+k}{2}$, or equivalently $k - \frac{2n}{k} < -1$, the sum $\sum_{q=1}^{\infty} q^{k-\frac{2n}{k}}$ is a convergent series. Furthermore, for such an n,

$$\sum_{q=1}^{\infty} q^{k-\frac{2n}{k}} \le 1 + \int_{q=1}^{\infty} q^{\frac{k^2-2n}{k}} dq = 1 + \frac{k}{2n-(k^2+k)} \le 1 + \frac{k}{2},$$

and so

$$\mathfrak{S}(n,k) \le e^{3.48kn} \sum_{q=1}^{\infty} q^{k-\frac{2n}{k}} \le \left(1+\tfrac{k}{2}\right) e^{3.48kn}.$$

Since $\mathfrak{S}(n,k)$ is decreasing as a function of n, for $n \ge \frac{k^2+k+2}{2}$,

$$\mathfrak{S}(n,k) \le \mathfrak{S}\left(\tfrac{k^2+k+2}{2}, k\right) \le \left(1+\tfrac{k}{2}\right) e^{1.74(k^3+k^2+2k)}.$$

(ii) Suppose that $p < (k+4)/3$. We shall derive a lower bound on

$$S(p) = \sum_{\substack{\lambda_1=1 \\ (\lambda_1,\ldots,\lambda_k,p)=1}}^{p} \cdots \sum_{\lambda_k=1}^{p} \left| p^{-1} \sum_{x=1}^{p} e_p\left(\lambda_1 x + \cdots + \lambda_k x^k\right) \right|^{2n}$$

for such p. For $p \nmid x$ we have

$$\sum_{i=1}^{k} \lambda_i x^i \equiv \sum_{\ell=0}^{p-2} \left(\sum_{\substack{i=1 \\ i \equiv \ell \pmod{p-1}}}^{k} \lambda_i \right) x^\ell \pmod{p}$$

by Fermat's Little Theorem. Let n_ℓ be the number of i with $i \equiv \ell \pmod{p-1}$ and $1 \le i \le k$; namely, $n_\ell = \lfloor \frac{k-\ell}{p-1} \rfloor$. Note that since $p < (k+4)/3$ we have $n_\ell \ge \lfloor \frac{3p-4-\ell}{p-1} \rfloor \ge \lfloor \frac{3p-4-p+2}{p-1} \rfloor = 2$ for all ℓ.

In the case when $p = 2$, the above sum yields only the constant term x^0. Thus there are $p^{n_0} - 1 = 2^k - 1$ choices for the λ_i with $i \equiv 0 \pmod{1}$ and $(\lambda_1, \lambda_2, \ldots, \lambda_k, 2) = 1$ for which the polynomial above is identically a constant.

Now let us consider the case when $p > 2$. The above polynomial is identically a constant if for $\ell \ge 1$, each sum over i is $0 \pmod{p}$. For a given $\ell \ge 1$ there are $p^{n_\ell - 1} - 1$ choices for the λ_i with $i \equiv \ell \pmod{p-1}$ where $(\lambda_\ell, \lambda_{\ell+p-1}, \ldots, \lambda_{\ell+(n_\ell-1)(p-1)}, p) = 1$ and $\sum_{\substack{i=1 \\ i \equiv \ell \pmod{p-1}}}^{k} \lambda_i \equiv 0 \pmod{p}$. Thus, there are at least

$$\begin{aligned} p^{n_0} \prod_{\ell=1}^{p-2} (p^{n_\ell - 1} - 1) &= p^{n_0} \prod_{\ell=1}^{p-2} \left(1 - \frac{1}{p^{n_\ell - 1}}\right) \prod_{\ell=1}^{p-2} p^{n_\ell - 1} \\ &> \left(1 - \tfrac{1}{p}\right)^{p-2} p^{-p+2+\sum_{\ell=0}^{p-2} n_\ell} \\ &\ge e^{-1} p^{k-p+2}, \end{aligned}$$

choices of the λ_i with $(\lambda_1, \ldots, \lambda_k, p) = 1$ that make the polynomial identically a constant, noting that for $\ell = 0$ the λ_i can be arbitrarily selected. Each such choice of the λ_i gives a contribution of 1 to the sum $S(p)$, and so $S(p) \ge e^{-1} p^{k-p+2}$. By Theorem 4.10.1, we have that

$$\mathfrak{S}(n,k) = \prod_{p \,\text{prime}} \left(S(1) + S(p) + S(p^2) + \ldots \right).$$

Thus

$$\mathfrak{S}(n,k) \geq \prod_{p<(k+4)/3} S(p) \geq \prod_{p<(k+4)/3} e^{-1}p^{k-p+2}.$$

Taking the logarithm of both sides we get, for $k \geq 8$,

$$\begin{aligned}
\log \mathfrak{S}(n,k) &\geq \sum_{p<(k+4)/3} ((k-p+2)\log p - 1) \\
&\geq \sum_{p<(k+4)/3} \left(k - \frac{k+4}{3} + 2\right) \log p \\
&= \frac{2}{3}(k+1) \sum_{p<(k+4)/3} \log p. \qquad (4.40)
\end{aligned}$$

By a result of Rosser and Schoenfeld [25], for $x \geq 41$,

$$\Theta(x) = \sum_{p \leq x} \log p > x \left(1 - \frac{1}{\log x}\right).$$

Applying this bound in (4.40), for $(k+4)/3 \geq 41$, we obtain that

$$\log \mathfrak{S}(n,k) > \frac{2}{3}(k+1)\left(\frac{k+4}{3}\right)\left(1 - \frac{1}{\log((k+4)/3)}\right).$$

Noting that for $(k+4)/3 \geq 41$,

$$1 - \frac{1}{\log((k+4)/3)} > 1 - \frac{1}{\log 41} > 0.73,$$

we conclude that

$$\log \mathfrak{S}(n,k) > \left(\frac{2}{9}\right)(k+1)(k+4)\left(\frac{73}{100}\right) = \left(\frac{73}{450}\right)(k+1)(k+4) > \left(\frac{\log 6}{30}\right)(k+1)(k+4).$$

Finally, we can exponentiate both sides to get the result of the theorem for $(k+4)/3 \geq 41$. For $(k+4)/3 \leq 41$, one can numerically check that the result of the theorem holds.

□

Bibliography

[1] A. Alnaser and T. Cochrane, *Waring's number mod m*, J. Number Theory 128 (2008), no. 9, 2582–2590.

[2] Tom M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[3] G. I. Arkhipov, V. N. Chubarikov, and A. A. Karatsuba, Trigonometric Sums in Number Theory and Analysis, de Gruyter Exp. in Math. 39 (Walter de Gruyter, Berlin, 2004).

[4] R. C. Baker, *Small Solutions of Congruences*, Mathematika 30 (1983), 164–188.

[5] R. C. Baker, Diophantine Inequalities, London Math. Soc. Monographs, Clarendon Press, Oxford, 1986.

[6] R. Balasubramanian, J.-M. Deshouillers, and F. Dress, *Problème de Waring pour les bicarrés. I. Schéme de la solution*, C. R. Acad. Sci. Paris Sér. I Math. 303 (1986), no. 4, 85–88.

[7] R. Balasubramanian, J.-M. Deshouillers, and F. Dress, *Problème de Waring pour les bicarrés. II. Résultats auxiliaires pour le théorème asymptotique*, C. R. Acad. Sci. Paris Sér. I Math. 303 (1986), no. 5, 161–163.

[8] J. Bourgain, C. Demeter, and L. Guth, *Proof of the Main Conjecture in Vinogradov's Mean Value Theorem for Degrees Higher Than Three*, arXiv:1512.01565v2 (2016). (To appear in Ann. of Math.)

[9] Chowla, *On Waring's problem* $\pmod{p}$, Proc. Indian Nat. Acad. Sci. A 13 (1943), 195–220.

[10] T. Cochrane, *Small Solutions of Congruences*, Ph.D. Thesis, University of Michigan, 1984, 1–106.

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

[12] T. Cochrane and C. Pinner, *An improved Mordell type bound for exponential sums*, Proc. Amer. Math. Soc. 133 (2005), no. 2, 313–320.

[13] 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 (1998), no. 2, 175–182.

[14] T. Cochrane and Z. Zheng, *On upper bounds of Chalk and Hua for exponential sums*, Proc. Amer. Math. Soc. 129, no. 9, (2001), 2505–2516.

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

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

[17] G. H. Hardy and J. E. Littlewood, *Some problems of "Partitio Numerorum", IV: The singular series in Waring's problem and the value of the number* $G(k)$, Math. Zeitschrift 12 (1922), 161–188.

[18] D. Hart and A. Iosevich, *Sums and products in finite fields: an integral geometric viewpoint,* Radon transforms, geometry, and wavelets, 129–135, Contemp. Math., 464, Amer. Math. Soc., Providence, RI, 2008.

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

[20] 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.

[21] A. Kempner, *Bemerkungen zum Waringschen Problem*, Math. Ann. 72 (1912), no. 3, 387–399.

[22] 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.

[23] M. Qi and P. Ding, *Estimate of complete trigonometric sums*, Kexue Tongbao 29 (1984), 1567-1569.

[24] 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.

[25] J. Barkley Rosser and L. Schoenfeld, *Approximate Formulas For Some Functions of Prime Numbers*, Illinois J. Math. 6 (1962), no. 1, 64–94.

[26] A. Sárközy, *On products and shifted products of residues modulo p*, Integers: Electron. J. Combin. Numb. Theory 8(2) (2008), A9, 18.

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

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

[29] 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.

[30] S. B. Stečkin, *Estimate of a complete rational trigonometric sum*, Proc. Steklov Inst. 143 (1977), 188–220, English translation, A.M.S. Issue 1 (1980), 201–220.

[31] R. S. Steiner, *Effective Vinogradov's Mean Value Theorem Via Efficient Boxing*, 2016. arXiv:1603.02536v1.

[32] T. Tao and V. H. Vu, Additive Combinatorics, Cambridge University Press, no. 105, Cambridge, UK, 2010.

[33] A. Weil, *Number of solutions of equations in finite fields*, Bull. Amer. Math. Soc. 55 (1949), 497–508.

[34] A. Wieferich, *Beweis des Satzes, daß sich eine jede ganze Zahl als Summe von höchstens neun positiven Kuben darstellen läßt*, Math. Ann. (1) 66 (1909), 95–101.

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

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

[37] T. D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Ann. of Math. (2) 175 (2012), no. 3, 1575–1627.

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

[39] T. D. Wooley, *Translation invariance, exponential sums, and Waring's problem*, arXiv:1404.3508 (2014), 1–25.

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

[41] T. D. Wooley, *The cubic case of the mean conjecture in Vinogradov's mean value theorem*, arXiv 1401.3150.