Counting solutions to diagonal congruences and Diophantine inequalities

by

Kathryn Wilson

B.S., Western Oregon University, 2017

M.S., Kansas State University, 2021

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

2025

Abstract

This dissertation will cover three results. Each result has a connection to Waring's problem and the circle method. Throughout, let p be prime, and let n, k and s be positive integers.

First, let $\Gamma^*(k, p^n)$ be the smallest positive integer s such that for any integers a_i coprime to p and integer a, the congruence

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv a \pmod{p^n}$$

is solvable in integers x_i, with $p \nmid x_i$, $1 \leq i \leq s$. We prove that for $\varepsilon > 0$,

$$\Gamma^*(k, p^n) \ll_\varepsilon k^{\frac{1}{\phi(t_1)}+\varepsilon},$$

where t_1 is the number of nonzero k-th powers mod p. The estimate is best possible aside from the possible removal of the ε.

Next, using a result of Chow, Lindqvist and Prendiville [10], we establish that for any positive integer $k \geq 4$, positive integer s such that

$$s \geq \frac{3}{2}k(\log k + \log\log k + 2 + O(\log\log k/\log k)),$$

prime p, integer a, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq s$, there exists a solution of

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k \equiv a \pmod{p}$$

with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq s$.

Lastly, we will discuss how the Bentkus–Götze–Freeman variant of the Davenport–Heilbronn circle method can be used to study $\mathbb{F}_q[t]$ solutions to inequalities of the form

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau$$

where constants $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_q((1/t))$ satisfy certain conditions. This result is a generalization of the work done by Spencer in [39] to count the number of solutions to inequalities of the form

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k) < \tau.$$

Counting solutions to diagonal congruences and Diophantine inequalities

by

Kathryn Wilson

B.S., Western Oregon University, 2017

M.S., Kansas State University, 2021

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

2025

Approved by:

Major Professor
Craig Spencer

Copyright

Abstract

This dissertation will cover three results. Each result has a connection to Waring's problem and the circle method. Throughout, let p be prime, and let n, k and s be positive integers.

First, let $\Gamma^*(k, p^n)$ be the smallest positive integer s such that for any integers a_i coprime to p and integer a, the congruence

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv a \pmod{p^n}$$

is solvable in integers x_i, with $p \nmid x_i$, $1 \leq i \leq s$. We prove that for $\varepsilon > 0$,

$$\Gamma^*(k, p^n) \ll_\varepsilon k^{\frac{1}{\phi(t_1)}+\varepsilon},$$

where t_1 is the number of nonzero k-th powers mod p. The estimate is best possible aside from the possible removal of the ε.

Next, using a result of Chow, Lindqvist and Prendiville [10], we establish that for any positive integer $k \geq 4$, positive integer s such that

$$s \geq \frac{3}{2}k(\log k + \log\log k + 2 + O(\log\log k/\log k)),$$

prime p, integer a, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq s$, there exists a solution of

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k \equiv a \pmod{p}$$

with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq s$.

Lastly, we will discuss how the Bentkus–Götze–Freeman variant of the Davenport–Heilbronn circle method can be used to study $\mathbb{F}_q[t]$ solutions to inequalities of the form

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau$$

where constants $\lambda_1, \ldots, \lambda_s \in \mathbb{F}_q((1/t))$ satisfy certain conditions. This result is a generalization of the work done by Spencer in [39] to count the number of solutions to inequalities of the form

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k) < \tau.$$

Table of Contents

List of Tables

Acknowledgments

Firstly, I would like express my sincerest thanks to my advisor Dr. Craig Spencer for his support and guidance in my time at Kansas State University. He has been a role model as both a researcher and a teacher, and I hope to one day emulate his dedication to mathematics and mathematics education. His patience and time have been invaluable to my success. I would also like to thank the members of my committee, Dr. Todd Cochrane, Dr. Chris Pinner, and Dr. Sherri Martinie for their feedback. Furthermore, I would like to extend my thanks to Dr. Todd Cochrane and Dr. Misty Ostergaard, for their help and feedback as co-authors.

I would not have been nearly as successful without the support of the Mathematics Department and my fellow graduate students. To Adriana, Stas, Garrett, Kostas, and Lailah, thank you for motivating me to aim for success. Thank you as well to Elizabeth, for uplifting me as a person and being a rock I could lean on. I am grateful that my path in life lead me to meeting all of you.

To my family, thank you for your endless support. Mom, thank you for the long phone calls. Dad, thank you for always updating me on KSU sports. Jenny, thank you for visiting me and being someone I could vent to. Tricia, thank you for being someone I could always turn to for advice and support. This would not have happened without your presence in my life.

Dedication

I dedicate this to my family. Through phone calls and cards and countless other small gestures, thank you for being by my side every step of the way.

Chapter 1

Introduction

1.1 The Hardy-Littlewood Circle Method

The Hardy-Littlewood circle method is a mathematical technique designed to count solutions to additive equations. It has been used in many areas of mathematics, most commonly in number theory. The technique was developed in the early 20^{th} century by Hardy and Littlewood to solve Waring's problem. The idea behind the circle method was originally used by Hardy and Ramanujan to count partitions (see [27]), and it is not uncommon to see the Hardy-Littlewood circle method also called the Hardy-Littlewood-Ramanujan circle method. Henceforth, the Hardy-Littlewood-Ramanujan circle method will simply be referred to as the circle method.

Waring's problem was first posed by Waring in the 18^{th} century. The problem asks how large does s needs to be for each power k such that for all $N \in \mathbb{N}$, the equation

$$x_1^k + x_2^k + \cdots + x_s^k = N, \tag{1.1}$$

has a solution where $x_i \in \mathbb{Z}$ for $1 \leq i \leq s$. In 1770, Lagrange proved that when $k = 2$, then $s = 4$ is enough variables to generate all natural numbers. Hardy and Littlewood wanted to prove a general result for the size of s for any k. Adding the condition that N be a

sufficiently large natural number, in [26] Hardy and Littlewood used the circle method to show that (1.1) is solvable when s is at least size $(k-2)2^k+5$. For the rest of this chapter, $G(k)$ will be the minimal s required such that (1.1) is solvable for sufficiently large values of N.

Efforts have been continuously made to improve upon the size of $G(k)$. In 1939, Davenport [19] established that for the specific case of $k=4$, $G(4)=16$. Vinogradov was able to show that $G(k) \leq 2k(\log k + 2\log\log k + O(\log\log\log k))$ in [41]. This was later improved by Vaughan in [40] to $G(k) \leq 2k(\log k + \log\log k + O(1))$ and by Wooley in [44] to $G(k) \leq k(\log k + \log\log k + 2 + O(\log\log k/\log k))$. In 2023 [6], Brudern and Wooley showed that $G(k) \leq \lceil k(\log k + 4.20032)\rceil$.

Hardy and Littlewood constructed the circle method using power series of the form

$$f_k(z) = \sum_{i=1}^{\infty} z^{i^k}.$$

By raising the power series to the power s, they had

$$\begin{aligned} f_k(z)^s &= \sum_{i_1=1}^{\infty} \cdots \sum_{i_s=1}^{\infty} z^{i_1^k+\cdots+i_s^k} \\ &= \sum_{N=1}^{\infty} R_{s,k}(N) z^N, \end{aligned}$$

where $R_{s,k}(N)$ is the number of ways N can be written as the sum $i_1^k+\cdots+i_s^k$. By using Cauchy's integral formula, we can find $R_{s,k}(N)$ with the integral

$$R_{s,k}(N) = \frac{1}{2\pi i}\int_C f_k(z)^s z^{-N-1} dz.$$

The circle method draws its name from the construction of this integral, which travels around the circle C centered at the origin with radius in the interval $(0,1)$.

Vinogradov later shifted the circle method to a construction using exponential sums.

Vinogradov's analysis relies on the fact that for integers m and n,

$$\int_0^1 e^{2\pi i(m-n)x} dx = \begin{cases} 1, & \text{if } m = n; \\ 0, & \text{if } m \neq n. \end{cases}$$

When considering Waring's problem, m and n can be replaced by the left and right side of (1.1). Doing so creates an integral

$$r(N) = \int_0^1 \left(\sum_{x=1}^{P} e(\alpha x^k) \right)^s e(-N\alpha) d\alpha$$

that counts solutions to (1.1) with $1 \leq x_i \leq P$ for $1 \leq i \leq s$.

To find an asymptotic formula for $r(N)$, the domain of the integral is split into subsets. Traditionally, there are two subsets named the major and minor arcs. We may appeal to Dirichlet's approximation theorem.

Theorem 1.1.1. *(Dirichlet's Approximation Theorem) Let $\alpha \in \mathbb{R}$, and suppose that $X > 1$ is a real number. Then there exist $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ with $(a, q) = 1$ and $1 \leq q \leq X$ such that*

$$\left| \alpha - \frac{a}{q} \right| \leq \frac{1}{qX}.$$

The major arcs are the union of sets of α where α is well approximated by a rational number with small denominator. The minor arcs are the complement of the major arcs on $[0, 1]$, or where α is not well approximated by a rational number with small denominator. This is only one example of a way to decompose $[0, 1]$ into the major and minor arcs when using the circle method. Ultimately, the goal of the major and minor arcs analysis is for the integral over the major arcs to provide the main contribution to the asymptotic formula. Even though the major arcs are typically a smaller set compared to the minor arcs, the integral over the minor arcs is expected to contribute to an error term instead of the main term.

1.2 Overview of Notation

The following is common notation that will be used in this manuscript. The definitions and notation provided in this section will remain consistent for every chapter. First, we define the natural numbers $\mathbb{N}$ to be the set of whole positive numbers, beginning at 1. We take $\log x$ to be the natural logarithm of x and $\phi(x)$ to be the Euler totient function of x. We write the vector $(x_1, \dots, x_n)$ as $\boldsymbol{x}$. Let A and B be sets and ℓ be a positive integer. We make use of the following sum-set and product-set notation:

$$A + B = \{a + b : a \in A, b \in B\},$$

$$AB = \{ab : a \in A, b \in B\},$$

$$\ell * A = A + A + \cdots + A, \quad (\ell\text{-times}),$$

and

$$\ell A = \{\ell a : a \in A\}.$$

Furthermore, we will make use of Vinogradov notation. For functions f and g, with g taking on only positive values, we write $f \ll g$ to mean that $|f| \leq cg$ for some positive constant c. If f only takes on positive values, we write $g \gg f$ to mean that $f \leq cg$ for some positive constant c. When we write $f \ll_\epsilon g$, we mean that the positive constant c in the expression $|f| \leq cg$ depends on ϵ. If $f \ll g$, we may also write $f(x) = O(g(x))$. We write $f \asymp g$ when both $f \ll g$ and $g \ll f$. We also write $f(x) = o(g(x))$ to mean that for functions f and g, with g taking on only positive values, for every positive constant C there exists an x_0 such that for all $x \geq x_0$, $|f| \leq Cg$.

1.3 Overview of Results

The circle method is a malleable tool that can be used to count solutions to more than just equations that look like (1.1). Chapters 2, 3, and 4 of this manuscript will each cover a

separate result for a variation of Waring's problem.

1.3.1 Diagonal Congruences Modulo a Prime Power

Hardy and Littlewood also researched the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p^n}, \tag{1.2}$$

where p is a prime. We define the Waring number $\gamma(k, p^n)$ to be the minimal s such that for any integer a, (1.2) holds for some integers x_i with $p \nmid x_i$, for some i. In [26], Hardy and Littlewood established that $\gamma(k, p^n) \leq 4k$. When p is an odd prime, Hardy and Littlewood also showed in [26] that a solution modulo p^n existed when $\gamma(k, p^n) \leq \frac{p}{p-1}k + 1$. In Chapter 2, we consider the congruence

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv a \pmod{p^n}. \tag{1.3}$$

This construction is similar to (1.2); however we have also introduced coefficients. We define for any positive integer k and prime power p^n, $\Gamma^*(k, p^n)$ to be the minimal s such that for any integer a and integers a_i with $p \nmid a_i$, $1 \leq i \leq s$, (1.3) has a solution with $p \nmid x_i$ for all i. Suppose that $k = p^e k_1$, where $k_1 | (p-1)$. Then we define $t_1 := (p-1)/k_1$.

We will prove the following theorem in Chapter 2, which is based on joint work with Todd Cochrane and Craig Spencer [14].

Theorem 1.3.1. *For any $\varepsilon > 0$, odd prime power p^n and positive integer k with $(p-1) \nmid k$, we have*

$$\Gamma^*(k, p^n) \ll_\varepsilon k^{\frac{1}{\phi(t_1)} + \varepsilon}. \tag{1.4}$$

1.3.2 Small Solutions Modulo a Prime

When considering Waring's problem modulo p^n, we can count solutions for a general prime p and natural number n, but we can also consider specific cases. Analysis of special cases

may provide stronger results than the general case. For example, consider again the bounds on the size of s required to guarantee solutions of (1.2) established by Hardy and Littlewood in [26]. For a general prime power p^n, one requires $s \geq 4k$, but when p is restricted to be an odd prime, $s \geq \frac{p}{p-1}k+1$ suffices. In 1813, Cauchy in [8] established that when considering (1.1) modulo p, there is a solution provided $s \geq k$. In Chapter 3, we consider a congruence like (1.3) but with $n = 1$ and our solutions restricted to be of the size $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for all $1 \leq i \leq s$.

We are able to prove the following result, which is based on joint work with Todd Cochrane, Misty Ostergaard, and Craig Spencer [17].

Theorem 1.3.2. *For any positive integer $k \geq 2$, positive integer s with*

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

prime p, integer a, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq s$, there exists a solution of

$$a_1x_1^k + \cdots + a_sx_s^k \equiv a \pmod{p}. \tag{1.5}$$

with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq s$.

1.3.3 Diophantine Inequalities in Function Fields

The last result concerns Diophantine inequalities over function fields. Instead of looking for integral solutions, we instead consider solutions in $\mathbb{F}_q[t]$. Being able to translate results from the integers over to function fields actually works quite nicely, in part because we can set up the following relationships of similar objects, see Table 1.1 below. First, let $\mathbb{F}_q[t]$ denote the ring of polynomials over $\mathbb{F}_q$, let $\mathbb{F}_q(t)$ be the field of rational functions, and let $\mathbb{F}_q((1/t))$ be the completion of $\mathbb{F}_q(t)$ at the infinite place.

Real Numbers	Function Fields
$\mathbb{Z}$	$\mathbb{F}_q[t] = \mathbb{A}$
$\mathbb{Q}$	$\mathbb{F}_q(t) = \mathbb{K}$
$\mathbb{R}$	$\mathbb{F}_q((1/t)) = \mathbb{K}_\infty$

Table 1.1: *Correlation between objects in the real numbers and function fields*

Kubota in [31] considered the equation (1.1), except where N and the x_i are elements of $\mathbb{F}_q[t]$. He adapted the circle method to prove that a solution exists provided that $s \geq \max(3k+1, 2^k+1)$ and $k < \mathrm{char}(\mathbb{F}_q)$. In [33] Wooley and Liu were able to refine the condition that $k < \mathrm{char}(\mathbb{F}_q)$ to $\mathrm{char}(\mathbb{F}_q) \nmid k$ instead. For the result in Chapter 4, we use the Davenport-Heilbronn circle method to study Diophantine inequalities.

First, let p be the characteristic of $\mathbb{F}_q$, and let $k > 1$ and s be positive integers with $p \nmid k$. Let $\mathrm{Log}\, x = \max(1, \log x)$ for any positive real number x. Define $\psi(k) = \psi_q(k)$ by $\psi(k) = a_0 + a_1 + \cdots + a_n$, where k has base p expansion $k = a_0 + a_1 p + \cdots + a_n p^n$ with $0 \leq a_i \leq p-1$. We denote $B_q(k)$ by

$$B_q(k) = \begin{cases} 1, & \text{when } k \leq 2^{\psi(k)-2} \\ (1 - 2^{-\psi(k)})^{-1}, & \text{when } k > 2^{\psi(k)-2}. \end{cases}$$

Let

$$s_{q,k} = B_q(k)k(\mathrm{Log}\, k + \mathrm{Log}\, \mathrm{Log}\, k + 2 + B_q(k)\mathrm{Log}\, \mathrm{Log}\, k/\mathrm{Log}\, k).$$

For $\alpha \in \mathbb{K}_\infty \backslash \{0\}$, we can write

$$\alpha = \sum_{-\infty < i \leq n} a_i t^i,$$

where $n \in \mathbb{Z}$, each $a_i \in \mathbb{F}_q$, and $a_n \neq 0$. We define $\mathrm{ord}\, \alpha = n$. We are now able to state the main theorem of Chapter 4, which covers the content in [43].

Theorem 1.3.3. *There exists a positive absolute constant C with the following property. Suppose that k and s are natural numbers with $k > 1$,*

$$s \geq s_{q,k} + Ck\sqrt{\mathrm{Log}\, \mathrm{Log}\, k}/\mathrm{Log}\, k,$$

and $\mathrm{char}(\mathbb{F}_q) \nmid k$. *Let* τ *be some fixed integer, let* γ *be an element in* $\mathbb{K}_\infty$, *and let* $\lambda_1, \dots, \lambda_s$ *be fixed non-zero elements of* $\mathbb{K}_\infty$, *not all in* $\mathbb{F}_q(t)$*-rational ratio. Suppose also that the equation*

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0 \tag{1.6}$$

has a non-trivial solution $\mathbf{z}$ *in* $\mathbb{K}_\infty^s$. *Then, for all sufficiently large positive real numbers* P, *the number of* $\mathbb{F}_q[t]$*-solutions* $N(P, \boldsymbol{\lambda}, \gamma)$ *of*

$$\mathrm{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau$$

with $\mathrm{ord}(x_i) \leq P$ *for* $1 \leq i \leq s$ *satisfies*

$$N(P, \boldsymbol{\lambda}, \gamma) \gg q^{P(s-k)}.$$

The implicit constant may depend on s, k, q, $\boldsymbol{\lambda}$, γ, *and* τ.

Chapter 2

Diagonal Congruences Modulo a Prime Power

In this chapter, our focus will turn to diagonal congruences modulo p^n, where p is prime and n is a natural number. The contents of this chapter is joint work with Todd Cochrane and Craig Spencer, from [14]. We will show that the minimal number of variables necessary to find a solution to (1.3) is bounded by a constant multiple of a small power of k. This result improves upon previous bounds on solutions to diagonal congruences due to Alnaser, Cochrane, Ostergaard, and Spencer (see [2], [16]). Recall that we define for any positive integer k and prime power p^n, $\Gamma^*(k, p^n)$ to be the minimal s such that for any integer a and integers a_i with $p \nmid a_i$, $1 \leq i \leq s$, (1.3) has a solution with $p \nmid x_i$ for all i. Note that when $s \geq \Gamma^*(k, p^n)$, (1.3) has a solution with $p \nmid x_i$ for all i. We also define the Waring number $\gamma^*(k, p^n)$ to be the minimal s such that for any integer a, there exist integers x_i with $p \nmid x_i$, $1 \leq i \leq s$, such that (1.2) holds. To be clear, throughout this and the next chapter, upper case Γ will always refer to the general diagonal congruence (1.3), and lower case γ to the congruence (1.2). The crux of the proof is constructing a recursion relation that bounds $\Gamma^*(k, p^n)$ by a constant multiple of $\gamma^*(k, p^n)$. We then use Hensel lifting to bound $\gamma^*(k, p^n)$, concluding with a bound on $\Gamma^*(k, p^n)$.

2.1 History

Recall that $\gamma(k,p^n)$ was defined to be the minimal s such that for any integer a, there exist integers x_i with $p \nmid x_i$, for some i, such that (1.2) holds. Over two hundred years ago, Cauchy [8] proved that $\gamma(k,p) \le k+1$ for any prime p and positive integer k; see [12] for a further discussion of Waring's number for prime moduli. It was also previously noted that Hardy and Littlewood [26, p. 180, Lemma 20] established for odd p that

$$\gamma(k,p^n) \le \left\lceil \tfrac{p}{p-1}k \right\rceil .$$

It was shown in [1] that if p is odd and $t_1 > 2$, then

$$\gamma(k,p^n) \le ck^{1/2}, \tag{2.1}$$

for some absolute constant c, and that for any $\varepsilon > 0$, if $\phi(t_1) > 1/\varepsilon$ then

$$\gamma(k,p^n) \ll_\varepsilon k^\varepsilon .$$

In [13] it was shown that the constant in (2.1) can be taken to be 83 for the case of prime moduli, sharpening the result in [12].

We define $\Gamma(k,p^n)$ to be the minimal s such that for any integers a and a_i with $p \nmid a_i$, $1 \le i \le s$, (1.3) has a solution where $p \nmid x_i$ for some i. $\Gamma(k,p^n)$ plainly exists for any k and p^n, but as noted in [2], $\Gamma^*(k,p^n)$ exists if and only if $(p-1) \nmid k$. To elaborate, suppose that $(p-1) \mid k$. Then by Fermat's little theorem, $\sum_{i=1}^s a_i x_i^k$ only has one value modulo p, and we cannot guarantee that for any a, (1.3) has a solution. If we suppose that $(p-1) \nmid k$, then by Lemma 6.5 of [2], we have growth when considering sums of sets of the form $\{a_i x^k : x \in \mathbb{Z}_{p^n} \backslash \{0\}\}$. From this work, it follows that $\Gamma^*(k,p^n)$ exists. In particular, p must be odd. The focus of this chapter is $\Gamma^*(k,p^n)$, although we occasionally state results for $\Gamma(k,p^n)$ as well. We may assume that $k|\phi(p^n)$, since the group of k-th powers mod p^n is

the same as the group of $(k, \phi(p^n))$-th powers mod p^n, and write

$$k = p^e k_1, \quad \text{with } k_1|(p-1), \quad e \leq n-1, \quad t_1 := (p-1)/k_1. \tag{2.2}$$

Thus $\Gamma^*(k, p^n)$ exists if and only if $t_1 > 1$.

In [2, Theorems 2.2, 2.3] the authors established the following estimates:

$$\Gamma^*(k, p^n) = 2k\left(\tfrac{p}{p-1}\right) - 1, \qquad \text{for } t_1 = 2; \tag{2.3}$$

$$\Gamma^*(k, p^n) \leq \left\lceil \tfrac{p}{p-1}\ k \right\rceil, \qquad \text{for } t_1 > 2; \tag{2.4}$$

$$\Gamma^*(k, p^n) \leq (c \log 2k_1)^{3e+3} k^{\frac{2}{\phi(t_1)}}, \qquad \text{for } t_1 > 1; \tag{2.5}$$

while in [16, Theorem 1.2], they showed there exists a constant C such that

$$\Gamma^*(k, p^n) \leq 8k^{\frac{5}{\log_2(t_1/C)}}. \tag{2.6}$$

2.2 Statement and Proof of Result

Here we show the following improvement of (2.5) and (2.6).

Theorem 2.2.1. *For any $\varepsilon > 0$, odd prime power p^n and positive integer k with $(p-1) \nmid k$, we have*

$$\Gamma^*(k, p^n) \ll_\varepsilon k^{\frac{1}{\phi(t_1)}+\varepsilon}. \tag{2.7}$$

In particular, for any k and p^n for which $\phi(t_1) > 1/\varepsilon$ we have $\Gamma^*(k, p^n) \ll_\varepsilon k^\varepsilon$, establishing a generalization of a conjecture of Heilbronn [28] who posited that for t_1 sufficiently large relative to ε, the congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv a \pmod{p},$$

has a solution provided that $s \gg_\varepsilon k^\varepsilon$. The original conjecture was proven in [12].

The exponent $\frac{1}{\phi(t_1)} + \varepsilon$ in (2.7) is best possible aside from the possible removal of the ε (for small t_1), in view of the lower bound of Cipra [11, Theorem 4.2]: For prime $t_1 < \frac{1}{2}\log k$,

$$\Gamma^*(k,p) \geq \tfrac{1}{2.718\ldots}(t_1-1)\,k^{\frac{1}{\phi(t_1)}} - t_1 + 1 \geq \tfrac{1}{5.436\ldots}(t_1-1)\,k^{\frac{1}{\phi(t_1)}}; \tag{2.8}$$

and lower bound for general t_1, [12, Theorem 3],

$$\Gamma^*(k,p) \gg k^{\frac{1}{\phi(t_1)}}/\sqrt{\log t_1}.$$

Remark 2.2.1. *For a general positive integer q we define $\Gamma^*(k,q)$ to be the minimal s (should it exist) such that for any integers a_i with $(a_i,q)=1$, $1\leq i\leq s$, and integer a, the congruence*

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \equiv a \pmod{q} \tag{2.9}$$

is solvable in integers x_i with $(x_i,q)=1$, for all i. By the Chinese Remainder Theorem, if q has prime power factorization $q=\Pi_{i=1}^{j}p_i^{e_i}$ and $(p_i-1)\nmid k$ for all i, then

$$\Gamma^*(k,q) = \max_{1\leq i\leq j}\Gamma^*(k,p_i^{e_i}),$$

and so (2.7) provides an upper bound for $\Gamma^*(k,q)$.

2.2.1 Preliminary Lemmas

We make use of the following standard Hensel-type lifting lemma, variations of which go back to Hardy and Littlewood [26]. For a proof, see eg. [1, Lemma 1].

Lemma 2.2.1. *Let $k=p^ek_1$ with $p\nmid k_1$, $a\in\mathbb{Z}$, and $a_i\in\mathbb{Z}$, $1\leq i\leq s$.*

i) Suppose that p is odd. Then any integer solution $(x_1,\ldots,x_s)$ of the congruence

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \equiv a \pmod{p^{e+1}}, \tag{2.10}$$

with $p\nmid a_ix_i$ for some i, can be lifted to a solution of the same congruence mod p^n for any

$n \geq e+1$.

ii) For $p=2$, any solution of the congruence

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \equiv a \pmod{2^{e+2}}, \tag{2.11}$$

with $2 \nmid a_ix_i$ for some i, can be lifted to a solution of the same congruence mod 2^n for any $n \geq e+2$.

The following estimates for $\Gamma(k,p^n)$ and $\Gamma^*(k,p^n)$ are an immediate consequence.

Lemma 2.2.2. *i) For odd p, with $p^e \| k$ and $n \geq e+1$, we have $\Gamma(k,p^n) = \Gamma(k,p^{e+1})$ and $\Gamma^*(k,p^n) = \Gamma^*(k,p^{e+1})$.*

ii) For $p=2$, with $2^e \| k$ and $n \geq e+2$, we have $\Gamma(k,2^n) = \Gamma(k,2^{e+2})$ and $\Gamma^*(k,2^n) = \Gamma^*(k,2^{e+2})$.

Let $\theta(k,p^n)$ be the minimal s such that zero has a primitive representation,

$$x_1^k + x_2^k + \cdots + x_s^k \equiv 0 \pmod{p^n}, \tag{2.12}$$

with $p \nmid x_i$ for some i and $\theta^*(k,p^n)$ the same with $p \nmid x_i$ for all i.

Lemma 2.2.3. *For any odd prime power p^n, $\theta(k,p^n) = \theta^*(k,p^n)$.*

Proof. It suffices to show $\theta^*(k,p^n) \leq \theta(k,p^n)$. Say $p^e \| k$. By Lemma 2.2.2 we may assume that $n \leq e+1$. Set $s = \theta(k,p^n)$ and suppose that we have a primitive representation of 0 as in (2.12). If $p | x_i$ for some i then $p^k | x_i^k$. Since $k \geq p^e \geq e+1 \geq n$, we have $p^n | x_i^k$. Thus deleting the variable x_i yields a primitive representation of 0 in a smaller number of variables, contradicting the minimality of s. Therefore $p \nmid x_i$ for all i. □

We need the following result from [16].

Lemma 2.2.4. *[16, Lemma 6.1] Let p, k, and t_1 be as in (2.2) with $t_1 \geq 2$. Then $\theta(k,p^n) \leq p_{min}$, where p_{min} is the minimal prime divisor of t_1.*

Lemma 2.2.5. *For any k and prime power p^n for which $\gamma^*(k,p^n)$ exists, we have*

$$\gamma^*(k,p^n) \le \theta(k,p^n)\cdot\gamma(k,p^n).$$

Proof. Let A be the group of k-th powers in $\mathbb{Z}_{p^n}^*$, $A_0 = A\cup\{0\}$, $\ell = \theta(k,p^n) = \theta^*(k,p^n)$, and $s = \gamma(k,p^n)$. We claim that $s*A_0 = \mathbb{Z}_{p^n}$. Indeed, let $k = p^e k_1$ with $e \le n-1$, as in (2.2). By Lemma 2.2.1, $s = \gamma(k,p^n) = \gamma(k,p^{e+1})$, and so for any integer c there is a primitive solution to the congruence

$$x_1^k + \cdots + x_s^k \equiv c \pmod{p^{e+1}}. \tag{2.13}$$

Now, $k = p^e k_1 \ge e+1$, and so if $p|x_i$ for some i, then $x_i^k \equiv 0 \bmod p^{e+1}$. Thus x_i can be replaced by 0 in the representation of c in (2.13). The new solution $\mathbf{x}$ with all such x_i set equal to 0, can then be lifted to a primitive solution of (2.13) mod p^n in such a manner that fixes the x_i that are already 0, implying that $c \in s*A_0$.

By the preceding lemma, $\ell \le p-1$, and therefore ℓ is relatively prime to p. Then $0 \in \ell*A$, $\ell A \subseteq \ell*A$, and so $\ell A_0 \subseteq \ell*A$. Thus

$$s\ell*A = s*(\ell*A) \supseteq s*(\ell A_0) = \ell(s*A_0) = \ell\mathbb{Z}_{p^n} = \mathbb{Z}_{p^n},$$

the last equality following from the fact that $(\ell,p)=1$. Thus $\gamma^*(k,p^n) \le s\ell$. □

Finally, we need the following result, which was first proven by Heilbronn [28, Theorem 8] for the case of prime moduli. Recall from (2.2), we define $t_1(p,k) = t_1 := (p-1)/k_1$.

Lemma 2.2.6. *[1, Lemma 6] For any positive integer t there is a constant $c_1(t)$ such that for any prime power p^n and positive integer k with $t_1(p,k) = t$, we have*

$$\gamma(k,p^n) \le c_1(t)p^{n/\phi(t)}.$$

Combining Lemmas 2.2.4, 2.2.5 and 2.2.6, we obtain that for any integer $t \ge 2$, there is a

constant $c_2(t)$ such that for any prime power p^n and positive integer k with $t_1(p,k) = t$,

$$\gamma^*(k, p^n) \le \theta(k, p^n) \cdot \gamma(k, p^n) \le t \cdot c_1(t) p^{n/\phi(t)} = c_2(t) p^{n/\phi(t)}. \tag{2.14}$$

2.2.2 General Recursion Proposition

Our proof follows the method used by Dodson [22] to prove related results about a homogeneous diagonal congruence. We need the following result of Erdös and Rado [23, Theorem III], which we state in a slightly weaker form:

Lemma 2.2.7. *Let $\mathcal{S}$ be a collection of N distinct sets each of cardinality j such that $N \ge j! G^{j+1}$ for some positive integer G. Then there is a subset $\mathcal{T}$ of $\mathcal{S}$ with $|\mathcal{T}| = G$, and a fixed set U, such that for any two elements $S_1, S_2 \in \mathcal{T}$ we have $S_1 \cap S_2 = U$.*

For a fixed positive integer k and prime p with $(p-1) \nmid k$, we define $\Gamma_0^* := 0$, and for $n \in \mathbb{N}$,

$$\gamma_n^* := \gamma^*(k, p^n), \qquad \Gamma_n^* := \Gamma^*(k, p^n).$$

Recall $q = p^n$. Set

$$j := \left\lfloor \sqrt{\log_2 q} \right\rfloor, \quad r := \gamma_n^*. \tag{2.15}$$

Again, let $t_1 = (p-1)/k_1$ denote the number of k-th powers in $\mathbb{Z}_p^*$.

Proposition 2.2.1. *i) For any odd prime p and positive integer k with $t_1 \ge 3$ we have for $n \ge 1$,*

$$\Gamma_n^* \le \tfrac{1}{2} j^2 q^{\frac{1}{j}} r^{1+\frac{1}{j}} + \Gamma_{n-1}^*. \tag{2.16}$$

ii) Under the same hypotheses, for $n \ge 1$,

$$\Gamma_n^* \le 4\, q^{3/\sqrt{\log q}}\, \gamma_n^*.$$

Proof. i) Let $k = p^e k_1$ with $e \le n-1$ and $t_1 \ge 3$.

Let j, r be as given in (2.15) and set

$$s := \lfloor \tfrac{1}{2} j^2 q^{\frac{1}{j}} r^{1+\frac{1}{j}} \rfloor. \tag{2.17}$$

We claim that for $q < 512$ we have $\lceil \frac{q}{t_1} \rceil \le s$, and thus by (2.4),

$$\Gamma_n^* \le \lceil \tfrac{p}{p-1} k \rceil \le \lceil \tfrac{p}{p-1} p^{n-1} k_1 \rceil = \lceil \tfrac{q}{t_1} \rceil \le s,$$

yielding the inequality in (2.16). Indeed, if $t_1 = 3$, then by [12, Theorem 2], $r \ge \gamma^*(k,p) \ge 3$ for $p \ge 13$, and for $p = 7$, the same holds since 0 is not a sum of two nonzero squares. One can check with a computer that for $q < 512$ we have $\lceil \frac{q}{3} \rceil \le \frac{1}{2} j^2 q^{\frac{1}{j}} 3^{1+\frac{1}{j}}$, as desired. If $t_1 \ge 4$, then $r \ge 2$, and one can similarly check that $\lceil \frac{q}{4} \rceil \le \frac{1}{2} j^2 q^{\frac{1}{j}} 2^{1+\frac{1}{j}}$, for $q < 509$. Now 510 and 511 are not prime powers. For $q = 509$, a prime, and $t_1 = 4$, we have $509 = 22^2 + 5^2$ and so by [12, Theorem 2], $\gamma(k,p) \ge 22 - 1 = 21$. Thus $r \ge 21$, $j = 2$ and again $\lceil \frac{q}{4} \rceil = 128 \le s$.

Assume now that $q \ge 512$, $j \ge 3$, and let $a_1, \dots, a_s$ be integers coprime to p. Let A be the group of k-th powers in $\mathbb{Z}_q^*$. For any integers a, b coprime to p, we say that a is equivalent to b, written $a \sim b$, if as elements of $\mathbb{Z}_q$ we have $aA = bA$. This relation partitions $\mathbb{Z}_q^*$ into equivalence classes (multiplicative cosets), each of cardinality $|A| = p^{n-1-e} t_1 \ge t_1$.

Case i: Suppose that some equivalence class contains r coefficients a_i, say $a_1 \sim a_2 \sim \cdots \sim a_r$. Then there exist integers u_i coprime to p such that $a_i \equiv u_i^k a_1 \bmod q$, for $1 \le i \le r$. Setting $y_i = u_i x_i$ for $1 \le i \le r$, and $x_i = 1$ for $i > r$, we have

$$a_1 x_1^k + \cdots + a_s x_s^k \equiv a_1 (y_1^k + \cdots + y_r^k) + a_{r+1} + \cdots + a_s \pmod q.$$

Since $r = \gamma_n^*$ and $p \nmid a_1$, the right-hand side plainly represents all values mod q with $p \nmid y_i$, $1 \le i \le r$, and thus so does the left-hand side with $p \nmid x_i$, $1 \le i \le s$.

Case ii: Suppose that no set of r coefficients are equivalent, that is, each equivalence class contains at most $r - 1$ coefficients. Since each equivalence class contains at least t_1 elements, we can make a change of variables so that no coset representative appears more

than $R := \lceil \frac{r-1}{t_1} \rceil$ times among the coefficients, that is, no set of R coefficients are all equal.

Let j be as given in (2.15). For any subset $S := \{i_1, i_2, \ldots, i_j\}$ of $\{1, 2, \ldots, s\}$ of cardinality j, we consider the corresponding multiset of coefficients $\{a_{i_1}, \ldots, a_{i_j}\}$. We say two coefficients are distinct if their subscripts are distinct (even though they may have the same value.) Let $\mathcal{C}$ be the collection of all such S having the property that no sum of (any number of) distinct coefficients from $\{a_{i_1}, \ldots, a_{i_j}\}$ is zero mod q. We estimate the number $|\mathcal{C}|$ of such sets by constructing a typical element of $\mathcal{C}$. There are s choices for i_1; given i_1, at least $s - R - 1$ choices for i_2 ($i_2 \neq i_1$ and $a_{i_2} \neq -a_{i_1}$); given i_1, i_2, at least $s - 2 - 3R$ choices for i_3 ($i_3 \neq i_1, i_2$ and $a_{i_3} \neq -a_{i_1}, -a_{i_2}, -a_{i_1} - a_{i_2}$); and in general, given $i_1, \ldots, i_{\ell-1}$, at least $s - (\ell - 1) - (2^\ell - 1)R$ choices for i_ℓ. Thus

$$\begin{aligned}
|\mathcal{C}| &> \frac{s(s-1-R)(s-2-(2^2-1)R)\cdots(s-(j-1)-(2^{j-1}-1)R)}{j!} \\
&> \frac{s^j - ((1+R)+(2+(2^2-1)R)+\cdots+((j-1)+(2^{j-1}-1)R))\, s^{j-1}}{j!} \\
&= \frac{s^j - \left(\frac{j(j-1)}{2} + (2^j - j - 1)R\right) s^{j-1}}{j!} \\
&> \frac{s^j - 2^j(R+1)s^{j-1}}{j!} \\
&= \left(1 - \frac{2^j(R+1)}{s}\right)\frac{s^j}{j!}.
\end{aligned}$$

We claim that $\frac{2^j(R+1)}{s} \leq \frac{1}{2}$ and thus

$$|\mathcal{C}| > \frac{s^j}{2j!}. \tag{2.18}$$

With s as defined in (2.17), it suffices to show that

$$2^{j+2}(R+1) \leq j^2 q^{\frac{1}{j}} r^{1+\frac{1}{j}}.$$

Now, by the definition of j, $2^j \leq q^{\frac{1}{j}}$ and so it suffices to show $R + 1 \leq \frac{1}{4} j^2 r^{1+\frac{1}{j}}$. Since for $t_1 \geq 3$, $R \leq \frac{r+2}{3}$ and $j \geq 2$, the latter inequality holds for any $r \geq 2$.

For each set $\{i_1, \dots, i_j\}$ in $\mathcal{C}$ we form the sum $a_{i_1} + \cdots + a_{i_j} \bmod q$. By the box principle, there exists a subset $\mathcal{C}'$ of $\mathcal{C}$ of cardinality $|\mathcal{C}'| \geq |\mathcal{C}|/q$ all of whose elements have a common sum $a_{i_1} + \cdots + a_{i_j} \bmod q$. By (2.18) and Lemma 2.2.7 applied with $G = r$, if

$$\frac{s^j}{2j!q} \geq j! r^{j+1},$$

then there is a collection of r sets in $\mathcal{C}'$ having a common intersection. For $j = 3$ it suffices to have

$$s \geq 2 \cdot 3^{\frac{2}{3}} q^{\frac{1}{3}} r^{1+\frac{1}{3}},$$

which by (2.17) is the case. Using $j! < 2.56\sqrt{j}\,(j/2.718...)^j$ for $j \geq 4$, we see that it suffices to have

$$s^j \geq 2 \cdot (2.56)^2 j (j/2.718...)^{2j} q r^{j+1},$$

that is,

$$s \geq (2.718...)^{-2} (13.11j)^{1/j} j^2 q^{1/j} r^{1+\frac{1}{j}}.$$

Since $(2.718...)^{-2}(13.11j)^{1/j} < .37$ for $j \geq 4$, the latter inequality holds for s as given in (2.17).

Deleting the common elements from each of the r sets in $\mathcal{C}'$, we obtain a collection $\mathcal{C}''$ of r disjoint subsets of $\{1, 2, \dots, s\}$ of the form $\{l_1, \dots, l_{j'}\}$ for some fixed $j' \leq j$, having the property that

$$a_{l_1} + a_{l_2} + \cdots + a_{l_{j'}} \equiv b \pmod{q},$$

for some fixed integer b. Moreover, by construction, b is nonzero mod q. Label the disjoint sets $T_1, T_2, \dots, T_r$. For each set $T_i = \{l_1, \dots, l_{j'}\}$ with $1 \leq i \leq r$, we set the variables $x_{l_1}, \dots, x_{l_{j'}}$ all equal to a new variable y_i so that

$$a_{l_1} x_{l_1}^k + \cdots + a_{l_{j'}} x_{l_{j'}}^k \equiv b y_i^k \pmod{q},$$

and we set all remaining variables equal to 1. Then letting b' represent the sum of the

coefficients of variables set to 1, the diagonal form can be written as

$$a_1x_1^k + a_2x_2^k + \cdots + a_sx_s^k \equiv b(y_1^k + \cdots + y_r^k) + b' \pmod{q}. \tag{2.19}$$

Since b is nonzero mod q, and $r = \gamma_n^*$, $b(y_1^k + \cdots + y_r^k) + b'$ represents all values mod q of the form $p^{n-1}u + b'$ with $u \in \mathbb{Z}$, in such a manner that $p \nmid y_i$, $1 \le i \le r$. Thus, by (2.19), the form $\sum_{i=1}^s a_ix_i^k$ represents all such values with $p \nmid x_i$ for all i. If $q = p$, we are done. If $q = p^n$ with $n \ge 2$, then with an additional set of Γ_{n-1}^* variables (that we set aside at the start) we can represent a complete set of residues mod p^{n-1}, and thus, with the full set of $s + \Gamma_{n-1}^*$ variables, represent every value mod p^n with $p \nmid x_i$ for all i, yielding the inequality in (2.16).

ii) Let $q = p^n$, and k be a positive integer. Set $j = \lfloor \sqrt{\log_2 q} \rfloor$, $r = \gamma^*(k, q)$. By (2.4), we have for $t_1 \ge 3$,

$$r = \gamma_n^*(k, p^n) \le \left\lceil \tfrac{(k,\phi(p^n))p}{p-1} \right\rceil \le \lceil q/t_1 \rceil < q$$

and so the inequality in part (i) can be written in a slightly weaker form,

$$\Gamma_n^* \le \tfrac{1}{2}j^2q^{\frac{2}{j}}\gamma_n^* + \Gamma_{n-1}^*. \tag{2.20}$$

The quantity $j^2q^{\frac{2}{j}}\gamma_n^*$ is increasing with n, and so after repeated applications of (2.20) (and recalling $\Gamma_0^* := 0$) we obtain

$$\Gamma_n^* \le \tfrac{n}{2}j^2q^{\frac{2}{j}}\gamma_n^* < \tfrac{1}{2}\log_3(q)\lfloor\sqrt{\log_2 q}\rfloor^2 q^{\frac{2}{\lfloor\sqrt{\log_2 q}\rfloor}}\gamma_n^* < 4\,q^{\frac{3}{\sqrt{\log q}}}\,\gamma_n^*,$$

for $q \ge 3$, as one can verify by computation. □

Remark 2.2.2. *One obtains the same kind of upper bounds for* $\Gamma_n := \Gamma(k, p^n)$, *following*

the proof of Proposition 2.2.1:

$$\Gamma_n \le \tfrac{1}{2} j^2 q^{\frac{1}{j}} \gamma_n^{1+\frac{1}{j}} + \Gamma_{n-1},$$
$$\Gamma_n \le 4q^{3/\sqrt{\log q}} \gamma_n,$$

where $\Gamma_0 := 0$ *and* $\gamma_n := \gamma(k, p^n)$. *One only needs to replace "representation with all* x_i *coprime to* p*" to "representation with some* x_i *coprime to* p*", wherever this expression appears.*

Remark 2.2.3. *If the diagonal form has the additional property that no set of* $j := \lfloor \log q \rfloor$ *or fewer coefficients add up to zero mod* q*, then with* $r := \gamma^*(k, p^n)$*, we get*

$$\Gamma_n^* \le (\log q)^2 \, r^{1+\frac{1}{j}} + \Gamma_{n-1}^*,$$

eliminating the $q^{\frac{1}{\lfloor \sqrt{\log_2 q} \rfloor}}$ *factor from (2.16). Indeed, allowing any choice of* j *coefficients in the definition of* $\mathcal{C}$*,*

$$|\mathcal{C}| = \binom{s}{j} > \frac{s^j - \frac{j(j-1)}{2} s^{j-1}}{j!} > \frac{1}{2} \frac{s^j}{j!},$$

for $s > j^2$. *For* j *as chosen here,* $q^{\frac{1}{j}} \approx 2.718...$

2.2.3 Proof of Theorem 2.2.1

Lemma 2.2.8. *For any positive integer* t, $(t+1)^{1/\phi(t)} \le 3$.

Proof. For $t \ge 12$ this is a consequence of the lower bound of Rosser and Schoenfeld [35, Theorem 15]

$$\phi(t) > \frac{t}{e^\gamma \log\log t + 3/\log\log t},$$

where $\gamma = .57721...$ is Euler's constant, while for smaller t, can be verified directly using the exact value of $\phi(t)$. □

We turn to the proof of the theorem. Let ε be a fixed positive real, and k, p^n be such that $(p-1) \nmid k$. By Lemma 2.2.1, we may assume that $k = p^{n-1} k_1$, with $k_1 | (p-1)$, $t_1 = \frac{p-1}{k_1} > 1$.

If $t_1 = 2$ then the result follows from (2.3) and so we may assume $t_1 \geq 3$. Let C be the constant in (2.6). If $t_1 > C\,2^{5/\varepsilon}$, then by (2.6), $\Gamma^*(k, p^n) \leq 8k^\varepsilon$, and the theorem holds.

Suppose now that $t_1 \leq C\,2^{5/\varepsilon}$. Then, by (2.14), setting

$$c_2^*(\varepsilon) := \max_{t \leq C\,2^{5/\varepsilon}} c_2(t),$$

we obtain

$$\gamma^*(k, p^n) \leq c_2(t_1) p^{n/\phi(t_1)} \leq c_2^*(\varepsilon)\, p^{n/\phi(t_1)}. \tag{2.21}$$

Now, $p^n = p^{n-1}(k_1 t_1 + 1) \leq k(t_1 + 1)$, and so by Lemma 2.2.8,

$$p^{n/\phi(t_1)} \leq k^{1/\phi(t_1)}(t_1 + 1)^{1/\phi(t_1)} \leq 3k^{1/\phi(t_1)}.$$

Inserting this into (2.21), yields

$$\gamma_n^* := \gamma^*(k, p^n) \leq 3\, c_2^*(\varepsilon) k^{\frac{1}{\phi(t_1)}}. \tag{2.22}$$

Since $t_1 \leq C\,2^{5/\varepsilon}$, it follows that

$$q = p^n = k t_1 \tfrac{p}{p-1} \leq c_\varepsilon k,$$

for some constant c_ε depending only on ε. Then, by Proposition 2.2.1 (ii), we have

$$\Gamma_n^* \leq 4\, q^{3/\sqrt{\log q}}\, \gamma_n^* \ll_\varepsilon k^{3/\sqrt{\log c_\varepsilon k}}\, \gamma_n^*.$$

Thus, if $k > c_\varepsilon^{-1} e^{9/\varepsilon^2}$, then $\Gamma_n^* \ll_\varepsilon k^\varepsilon \gamma_n^*$, which combined with (2.22) yields

$$\Gamma_n^* \ll_\varepsilon k^{\frac{1}{\phi(t_1)} + \varepsilon}.$$

If $k \leq c_\varepsilon^{-1} e^{9/\varepsilon^2}$ then the uniform bound $\Gamma_n^* \leq \lceil \frac{p}{p-1} k \rceil$ for $t_1 \geq 3$, yields $\Gamma_n^* \ll_\varepsilon 1$.

Chapter 3

Small Solutions Modulo a Prime

We once again consider solutions of diagonal congruences like (1.5). In this chapter we seek solutions with $1 \leq x_i \ll p^{\frac{1}{k}}$ for all i. This chapter is based on joint work done with Todd Cochrane, Misty Ostergaard, and Craig Spencer in [17]. In [15], Cochrane, Ostergaard, and Spencer were able to obtain solutions to (1.5) with $1 \leq x_i \ll p^{\frac{1}{k}}$ for $1 \leq i \leq s$ when $s \geq \frac{3}{2}(k^2+k+2)$. We will lower the required number of variables needed to obtain solutions to (1.5) of size $1 \leq x_i \ll p^{\frac{1}{k}}$ for $1 \leq i \leq s$. The improvement on the bound for the number of variables required uses techniques of smooth numbers, and follows from a result of Chow, Lindqvist, and Prendiville in [10]. Of note, by looking at the congruence $\sum_{i=1}^{s} x_i^k \equiv \frac{p-1}{2} \mod p$, we see the requirement that $1 \leq x_i \ll p^{\frac{1}{k}}$ for $1 \leq i \leq s$ is optimal.

3.1 History

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

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k \equiv 0 \pmod{p} \tag{3.1}$$

where the a_i, $1 \leq i \leq s$, are integers and p is prime, Schmidt in [37] found that when k is odd, $\epsilon > 0$, and s is sufficiently large, (3.1) has a solution with

$$\max_i |x_i| \leq p^{\epsilon}.$$

Later, Schmidt in [38] showed that for $a_i \in \mathbb{Z}$, $1 \leq i \leq s$, p a prime, odd $k \geq 3$, $\epsilon > 0$, and a constant $c(k)$ depending only on k, (3.1) has a solution with

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

Baker in [3] found that for a natural number m, $\epsilon > 0$, and integers a_i, $1 \leq i \leq s$, a non-zero solution to the congruence

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k \equiv 0 \pmod{m} \tag{3.2}$$

can be found with

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

In the case of $k = 3$, Dietmann in [21] showed that (3.2) has a solution satisfying

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

In [4, Lemma 10.1], Baker further refined his bound on solutions to homogeneous congruences with a composite modulus by proving that for a natural number m, $\epsilon > 0$, integers a_i, $1 \leq i \leq s$, and $s \geq C(k, \epsilon)$ where $C(k, \epsilon)$ is a constant, (3.2) has a solution with

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

3.2 Statement and Proof of Result

This chapter uses smooth numbers and a result from the work of Chow, Lindqvist and Prendiville [10] to lower the number of variables needed to establish a solution for (1.5) with $1 \leq x_i \ll p^{\frac{1}{k}}$ for $1 \leq i \leq s$. Using this result we are able to reduce the number of variables needed from $s \geq \frac{3}{2}(k^2+k+2)$ to

$$s \geq \frac{3}{2}k(\log\, k + \log\, \log\, k + 2 + O(\log\, \log\, k/\log\, k)).$$

Theorem 3.2.1. *For any positive integer $k \geq 2$, positive integer s with*

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

prime p, integer a, and integers a_i, with $p \nmid a_i$ for $1 \leq i \leq s$, there exists a solution of (1.5) with $1 \leq x_i \ll_k p^{\frac{1}{k}}$ for $1 \leq i \leq s$.

3.2.1 Counts on Smooth Numbers

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

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

which we call the set of B^η-smooth numbers. Now we are able to state the following theorem, shown by Chow, Lindqvist, and Prendiville in [10].

Lemma 3.2.1 ([10], Theorem B.1)**.** *Let $c_1, \ldots, c_s \in \mathbb{Z}\backslash\{0\}$ with $\sum_{i\in I} c_i = 0$ for some non-empty subset I of $\{1, 2, \ldots, s\}$. Then, for $k \geq 2$, there exists a positive real number $\eta_0(k)$ and positive integers $s_0(k)$ and $N_0(\boldsymbol{c}, \eta, k)$ such that for $0 < \eta \leq \eta_0(k)$, $s \geq s_0(k)$ and*

$N \geq N_0(\boldsymbol{c}, \eta, k)$, *we have*

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

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

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

Let

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

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

and

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

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

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

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

which was established by Ramaswami in [34].

Let $\eta_0(k)$ and $s_0(k)$ be defined as in Lemma 3.2.1. We define $e_p(x) := e^{\frac{2\pi i x}{p}}$. We can now prove the following lemma.

Lemma 3.2.2. *For any positive integers* k *and* s *and prime* p *with* $k \geq 2$, $0 < \eta \leq \eta_0(k)$, $2s \geq s_0(k)$, $sB^k \leq p$, *and integers* a_i *with* $(a_i, p) = 1$, $1 \leq i \leq s$, *we have* $|S_{\mathcal{A}^s}| \gg_{k,s,\eta} B^k$.

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

Cauchy-Schwarz inequality, we see that

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

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

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

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

We notice that

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

counts the number of solutions to the congruence

$$a_i(x_1^k + \cdots + x_s^k) \equiv a_i(y_1^k + \cdots + y_s^k) \pmod p.$$

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

$$x_1^k + \cdots + x_s^k \equiv y_1^k + \cdots + y_s^k \pmod p. \tag{3.3}$$

In conclusion, $N_{\mathcal{A}^s} \leq \tilde{N}_{\mathcal{A}^s}$. Since $sB^k \leq p$, any solution of (3.3) with $1 \leq x_i, y_i \leq B$ is a solution to

$$x_1^k + \cdots + x_s^k = y_1^k + \cdots + y_s^k.$$

Thus, we have by Lemma 3.2.1 that $\tilde{N}_{\mathcal{A}^s} \ll_{k,s,\eta} B^{2s-k}$, so $N_{\mathcal{A}^s} \ll_{k,s,\eta} B^{2s-k}$. For B sufficiently large, we have that $|\mathcal{A}| > \frac{1}{2}\rho\left(\frac{1}{\eta}\right) B$. Therefore, we find that $|S_{\mathcal{A}^s}| \gg_{k,s,\eta} B^k$. □

We now recall two lemmas from [15]. The first lemma follows from the Cauchy-Davenport Theorem [8, 18], and the second is a direct result of work of Sárközy [36, Corollary A]. Recall that for prime p and positive integer k, we define $\Gamma(k,p)$ to be the minimal positive integer s such that for any integers a_i with $p \nmid a_i$, $1 \leq i \leq s$, and integer a,

$$a_1 x_1^k + a_2 x_2^k + \cdots + a_s x_s^k \equiv a \pmod{p}$$

has a solution.

Lemma 3.2.3 ([15], Lemma 8.1)**.** *For any prime p and positive integer k, we have $\Gamma(k,p) \leq k$.*

Lemma 3.2.4 ([15], Lemma 8.3)**.** *If A_1, A_2, A_3, and B_1 are subsets of $\mathbb{Z}_p$ with $|A_1||A_2||A_3||B_1| > p^3$, then $A_1B_1 + A_2 + A_3 = \mathbb{Z}_p$.*

We now have all of the necessary tools to prove Theorem 3.2.1.

3.2.2 Proof of Theorem 3.2.1

Let k be a positive integer and $s_0(k)$, $\eta_0(k)$ and N_0 be as defined in Lemma 3.2.1. We may assume that $s = 3\left\lceil \frac{s_0(k)}{2} \right\rceil$ by setting $s - 3\left\lceil \frac{s_0(k)}{2} \right\rceil$ variables equal to arbitrary values in their specified intervals if $s > 3\left\lceil \frac{s_0(k)}{2} \right\rceil$. Let $0 < \eta \leq \eta_0(k)$, p be prime, and a, a_i be integers such that $p \nmid a_i$ for $1 \leq i \leq s$.

Set $B = \left\lfloor \left(\frac{3p}{s}\right)^{\frac{1}{k}} \right\rfloor$ and define $m = \left\lceil \frac{s_0(k)}{2} \right\rceil$. If p is less than the implied constant in $1 \leq x_i \ll_k p^{\frac{1}{k}}$, then the x_i are any element of the complete residue system modulo p. By Lemma 3.2.3, we have that (1.5) is solvable. Thus, we may assume that p is larger than any

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

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

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

and define A_2 and A_3 similarly for the variables $x_{m+1}, \ldots, x_{2m}$ and $x_{2m+1}, \ldots, x_{3m}$, respectively. We now apply Lemma 3.2.2 with s replaced by m, checking that $mB^k \leq p$ and $2m \geq s_0(k)$. Since $mB^k \leq p$, it follows from Lemma 3.2.2 that there exists a positive constant $c_0(k, \eta)$ with $|A_i| \geq c_0(k, \eta)p$ for $1 \leq i \leq 3$.

We set

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

and take p to be sufficiently large so that $p > L$. Furthermore, we set $D = \{1^k, 2^k, 3^k, \ldots, L^k\} \subseteq \mathbb{Z}_p$. Note that there are at least L/k distinct values mod p in the set D. Thus,

$$|A_1||A_2||A_3||D| > p^3.$$

Therefore, by Lemma 3.2.4, $A_1 D + A_2 + A_3 = \mathbb{Z}_p$. It follows that for any integer a, there exists a solution of (1.5) with

$$1 \leq x_i \leq LB \ll_k p^{\frac{1}{k}}.$$

Chapter 4

Diophantine Inequalities in Function Fields

This chapter moves away from congruences, and instead considers Diophantine inequalities. Instead of integer solutions we want to find polynomial solutions in the function field setting. The work in this chapter is based on [43]. Let $\lambda_i, \ldots, \lambda_s \in \mathbb{F}_q((1/t))$ and $\tau \in \mathbb{Z}$. For $\alpha \in \mathbb{F}_q((1/t))\backslash\{0\}$, we can express α as

$$\alpha = \sum_{-\infty < i \leq n} a_i t^i$$

where $a_i \in \mathbb{F}_q$ and $a_n \neq 0$. We then define $\operatorname{ord} \alpha = n$. We find an asymptotic for the number of solutions of

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau \tag{4.1}$$

where $x_1, \ldots, x_s \in \mathbb{F}_q[t]$ and $\deg x_i \leq m$ for all $1 \leq i \leq s$, using the same method established by Spencer in [39]. We follow a specific form of the circle method, the Bentkus-Götze-Freeman variant of the Davenport-Heilbronn method. We will consider one major arc, one minor arc, and a third trivial arc. The trivial arc provides no contribution to the asymptotic formula.

4.1 History

In [31], Kubota considered Waring's problem in $\mathbb{F}_q[t]$ by modifying the Hardy-Littlewood circle method. He counted solutions to the equation

$$x_1^k + \cdots + x_s^k = N \tag{4.2}$$

where $N, x_1, \ldots, x_s \in \mathbb{F}_q[t]$. The work of Kubota required that $k < \text{char}(\mathbb{F}_q)$ in the analysis of the minor arcs, due to his use of Weyl differencing. Carr was able to improve the bound to $s \geq 2k(k-1)\log 2 + 2k + 3$ in [7] using Vinogradov's mean value theorem, but still required that $k < \text{char}(\mathbb{F}_q)$. In [33] by Wooley and Liu, the $k < \text{char}(\mathbb{F}_q)$ condition was overcome through the use of sieve methods. Instead, they had the condition that $\text{char}(\mathbb{F}_q) \nmid k$.

The Davenport–Heilbronn method was developed to study the number of integral solutions to Diophantine inequalities of the form

$$|\lambda_1 x_1^k + \cdots + \lambda_s x_s^k| < \tau \tag{4.3}$$

where k and s are positive integers with $k > 1$, τ is a fixed positive real number, and $\lambda_1, \ldots, \lambda_s$ are non-zero real numbers not all in rational ratio. The number of solutions to (4.3) such that $\mathbf{x} \in [-P, P]^s \cap \mathbb{Z}^s$ is denoted by $N_0(P, \boldsymbol{\lambda})$. The condition that the λ_i $(1 \leq i \leq s)$ do not all have the same sign is added in the case that k is even, to guarantee the existence of a real solution. The method was constructed by Davenport and Heilbronn in [20]. In the aforementioned paper, they showed that for $s > 2^k$ and $(P_n)_{n=1}^{\infty}$ a sequence increasing to infinity that depends on $\boldsymbol{\lambda}$,

$$N_0(P_n, \boldsymbol{\lambda}) \gg P_n^{s-k}.$$

In 2001, Hsu in [30] used the Davenport–Heilbronn method in function fields to study the number of solutions of

$$\text{ord}(\lambda_1 p_1^k + \cdots + \lambda_s p_s^k) < \tau$$

where each p_i is a monic irreducible polynomial in $\mathbb{F}_q[t]$, the λ_i satisfy appropriate conditions,

$k < \mathrm{char}(\mathbb{F}_q)$, and

$$s \geq \begin{cases} 2^k + 1, & \text{when } 2 \leq k \leq 11; \\ 2[2k^2 \log\, k + k^2 \log\, \log\, k + 2k^2 - 2k] + 1, & \text{when } k \geq 11. \end{cases}$$

This broadened in scope the previous work Hsu had done on counting solutions in the linear case with three monic irreducible polynomials (see [29]). In 2008, Spencer (see [39]) continued the study of such methods to count solutions of Diophantine inequalities in the function field setting by developing the Bentkus–Götze–Freeman variant of the Davenport–Heilbronn circle method for function fields.

The Bentkus–Götze–Freeman variant of the Davenport–Heilbronn method was developed over 50 years after the paper in which Davenport and Heilbronn first presented their method. The variant established an asymptotic lower bound and asymptotic formula for $N_0(P, \boldsymbol{\lambda})$, for all sufficiently large values of P (see [5], [24], [25], [45]). For

$$s \geq k(\log\, k + \log\, \log\, k + O(1)),$$

an asymptotic lower bound for $N_0(P, \boldsymbol{\lambda})$ was established, and for

$$s \geq k^2(\log\, k + \log\, \log\, k + 2 + o(1)),$$

an asymptotic formula for $N_0(P, \boldsymbol{\lambda})$ was established. Spencer used the Bentkus–Götze–Freeman variant of the Davenport–Heilbronn circle method for function fields to provide an asymptotic lower bound for all sufficiently large positive numbers P on the number of $\mathbb{F}_q[t]$ solutions to

$$\mathrm{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k) < \tau$$

in $\mathbb{F}_q((1/t))$ with $\mathrm{ord}(x_i) \leq P$ for $1 \leq i \leq s$. Here, τ is a real number, and s is sufficiently large in terms of k and q. In this chapter, we follow much of the same methodology while

considering the inequality

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau$$

where γ is an element of $\mathbb{F}_q((1/t))$.

4.2 Definitions and Notation

First, we establish some basic notation. Let p be the characteristic of $\mathbb{F}_q$. Let $\mathbb{A} = \mathbb{F}_q[t]$ denote the ring of polynomials over $\mathbb{F}_q$, let $\mathbb{K} = \mathbb{F}_q(t)$, and let $\mathbb{K}_\infty = \mathbb{F}_q((1/t))$ be the completion of $\mathbb{K}$ at the infinite place. If $\alpha \in \mathbb{K}_\infty \backslash \{0\}$, it can be expressed as

$$\alpha = \sum_{-\infty < i \leq n} a_i t^i,$$

where $n \in \mathbb{Z}$, each $a_i \in \mathbb{F}_q$, and $a_n \neq 0$. In this case, we define $\operatorname{ord} \alpha = n$ and $\operatorname{lead} \alpha = a_n$, and if α is a polynomial, then $\operatorname{ord} \alpha = \deg \alpha$. We set $\operatorname{ord} 0 = -\infty$ and let $\operatorname{res} \alpha$ be the coefficient of t^{-1}.

There is a non-Archimedean valuation on $\mathbb{K}_\infty$ defined by $|\alpha| = \langle \alpha \rangle = q^{\operatorname{ord} \alpha}$. If u is a real number, let $\hat{u} = q^u$. We now rewrite

$$\operatorname{ord}(\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma) < \tau$$

as

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma \rangle < \hat{\tau}.$$

Here $k > 1$ and s are positive integers with $p \nmid k$.

To produce the results found in Theorem 1.3.3, we utilize the Davenport–Heilbron method for function fields. Let $e_q : \mathbb{F}_q \to \mathbb{C}^\times$ be defined by $e_q(a) = e^{2\pi i \operatorname{tr}(a)/p}$ where $\operatorname{tr} : \mathbb{F}_q \to \mathbb{F}_p$ is the trace map. We define $e : \mathbb{K}_\infty \to \mathbb{C}^\times$ by $e(\alpha) = e_q(\operatorname{res} \alpha)$. Let $\mathbb{T}$ be a compact additive subgroup of $\mathbb{K}_\infty$ defined as $\mathbb{T} = \{\alpha : \operatorname{ord} \alpha < 0\}$. We normalize a Haar measure on $\mathbb{K}_\infty$ so

that

$$\int_{\mathbb{T}} d\alpha = 1.$$

Like in [30], define the function $\chi_\tau : \mathbb{K}_\infty \to \mathbb{R}$ by

$$\chi_\tau(\alpha) = \begin{cases} \hat{\tau}, & \text{when } \langle \alpha \rangle < \hat{\tau}^{-1}; \\ 0, & \text{when } \langle \alpha \rangle \geq \hat{\tau}^{-1}. \end{cases}$$

Then as in Lemma 2.2 of [30], we construct an indicator function:

$$\int_{\mathbb{K}_\infty} e(\alpha\beta)\chi_\tau(\alpha)d\alpha = \begin{cases} 1, & \text{when } \langle \beta \rangle < \hat{\tau}; \\ 0, & \text{when } \langle \beta \rangle \geq \hat{\tau}. \end{cases}$$

We define the set of *R-smooth polynomials* $\mathcal{A}'(P, R)$ as

$$\mathcal{A}'(P, R) = \{x \in \mathbb{A} : \langle x \rangle \leq \hat{P}; \omega \text{ irreducible and } \omega \mid x \Rightarrow \langle \omega \rangle \leq \hat{R}\},$$

where $R \leq P$ for some real numbers P and R. Whenever R is used in the remainder of the chapter, we take $R = \eta P$, and when R occurs in a statement, we are asserting that there exists a positive number η_0 such that the statement holds for all $0 < \eta \leq \eta_0$. Denote

$$F(\alpha) = F(\alpha; P) = \sum_{\langle x \rangle \leq \hat{P}} e(\alpha x^k)$$

and

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

Note that by our definition of $e(\alpha)$, when $\alpha \in \mathbb{K}_\infty$ and $g \in \mathbb{A}$ we have that $f(\alpha + g) = f(\alpha)$. Set $F_i(\alpha) = F(\lambda_i \alpha)$ for $1 \leq i \leq s$ and $f_j(\alpha) = f(\lambda_j \alpha)$ for $3 \leq j \leq s$. We now have that the integral

$$\int_{\mathbb{K}_\infty} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)e(-\alpha\gamma)\chi_\tau(\alpha)d\alpha$$

counts the number of solutions $\mathbf{x} \in \mathbb{A}^s$ of

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma \rangle < \hat{\tau}$$

where $\langle x_i \rangle \leq \hat{P}$ for $i = 1, 2$ and $x_j \in \mathcal{A}'(P, R)$ for $3 \leq j \leq s$.

We say that a positive number $u > 2k - 2$ is *accessible to the exponent* k when there exists a positive number δ for which

$$\int_{\mathfrak{n}} |F(\alpha; P)^2 f(\alpha; P, R)^u| d\alpha \ll \hat{P}^{u+2-k-\delta},$$

where $\mathfrak{n}$ denotes the set of $\alpha \in \mathbb{T}$ such that for a and g in $\mathbb{A}$, when $\langle g\alpha - a \rangle < \hat{P}^{1-k}$ and $g \neq 0$, then $\langle g \rangle > \hat{P}$.

4.3 Statement and Proof of Result

Recall $k > 1$ and s are positive integers with $p \nmid k$. Like in Section 1.3.3, let $\operatorname{Log} x = \max(1, \log x)$ for any positive real number x. Define $\psi(k) = \psi_q(k)$ by $\psi(k) = a_0 + a_1 + \cdots + a_n$, where k has base-p expansion $k = a_0 + a_1 p + \cdots + a_n p^n$ with $0 \leq a_i \leq p - 1$. We denote $B_q(k)$ by

$$B_q(k) = \begin{cases} 1, & \text{when } k \leq 2^{\psi(k)-2}; \\ (1 - 2^{-\psi(k)})^{-1}, & \text{when } k > 2^{\psi(k)-2}. \end{cases}$$

Let

$$s_{q,k} = B_q(k) k (\operatorname{Log} k + \operatorname{Log} \operatorname{Log} k + 2 + B_q(k) \operatorname{Log} \operatorname{Log} k / \operatorname{Log} k).$$

We now restate our generalization of [39, Theorem 1.1].

Theorem 4.3.1. *There exists a positive absolute constant C with the following property. Suppose that k and s are natural numbers with $k > 1$,*

$$s \geq s_{q,k} + Ck\sqrt{\operatorname{Log} \operatorname{Log} k} / \operatorname{Log} k,$$

and $\mathrm{char}(\mathbb{F}_q) \nmid k$. *Let* τ *be some fixed integer, let* γ *be an element in* $\mathbb{K}_\infty$, *and let* $\lambda_1, \dots, \lambda_s$ *be fixed non-zero elements of* $\mathbb{K}_\infty$, *not all in* $\mathbb{F}_q(t)$*-rational ratio. Suppose also that the equation*

$$\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0 \tag{4.4}$$

has a non-trivial solution $\mathbf{z}$ *in* $\mathbb{K}_\infty^s$. *Then, for all sufficiently large positive real numbers* P, *the number of* $\mathbb{F}_q[t]$*-solutions* $N(P, \boldsymbol{\lambda}, \gamma)$ *of*

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma \rangle < \hat{\tau}$$

with $\langle x_i \rangle \leq \hat{P}$ *for* $1 \leq i \leq s$ *satisfies*

$$N(P, \boldsymbol{\lambda}, \gamma) \gg \hat{P}^{s-k}.$$

The implicit constant may depend on s, k, q, $\boldsymbol{\lambda}$, γ, *and* τ.

Stemming from results of Chevalley and Weil (see [9] and [42], respectively) and discussion in [39], the following conditions on s, k, and q provide cases where a non-trivial solution to (4.4) exists in $\mathbb{K}_\infty^s$.

Proposition 4.3.1. *Suppose that* $\mathrm{char}(\mathbb{F}_q) \nmid k$ *and let* $\lambda_1, \dots, \lambda_s$ *be non-zero elements of* $\mathbb{K}_\infty$. *The equation* $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ *has a non-trivial solution* $\mathbf{z} \in \mathbb{K}_\infty^s$ *whenever one of the following three conditions are met:*

(1) $s \geq k^2 + 1$,

(2) $q > k^4$ *and* $s \geq 2k + 1$,

(3) $(k, q-1) = 1$ *and* $s \geq k + 1$.

By Theorem 9.4, Corollary 13.3, and Lemma 14.1 of [33], Theorem 4.3.1 is the consequence of the following theorem.

Theorem 4.3.2. *Suppose that* k *and* s *are natural numbers with* $k > 1$ *and* $\mathrm{char}(\mathbb{F}_q) \nmid k$. *Assume that* $u > 2k-2$ *is accessible to the exponent* k *and that* $s \geq u+5$. *Let* τ *be some fixed*

integer, let γ be a non-zero element in $\mathbb{K}_\infty$, and let $\lambda_1, \dots, \lambda_s$ be fixed non-zero elements of $\mathbb{K}_\infty$, not all in $\mathbb{F}_q(t)$-rational ratio. Suppose also that the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. Then, for all sufficiently large positive real numbers P, the number of $\mathbb{F}_q[t]$-solutions $N(P, \boldsymbol{\lambda}, \gamma)$ of

$$\langle \lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma \rangle < \hat{\tau}$$

with $\langle x_i \rangle \leq P$ for $1 \leq i \leq s$ satisfies

$$N(P, \boldsymbol{\lambda}, \gamma) \gg \hat{P}^{s-k}.$$

The implicit constant may depend on s, k, q, $\boldsymbol{\lambda}$, γ, and τ.

Following the Davenport–Heilbronn method, we split the region $\mathbb{K}_\infty$ into three arcs. First, set $S_1(P) = (\operatorname{Log} \hat{P})^{1/8}$. Define the major arc by

$$\mathfrak{M} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle < S_1(P) \hat{P}^{-k}\},$$

the minor arc by

$$\mathfrak{m} = \{\alpha \in \mathbb{K}_\infty : S_1(P) \hat{P}^{-k} \leq \langle \alpha \rangle < \hat{\tau}^{-1}\},$$

and the trivial arc by

$$\mathfrak{t} = \{\alpha \in \mathbb{K}_\infty : \langle \alpha \rangle \geq \hat{\tau}^{-1}\}.$$

The trivial arcs provide no contribution to the bound, as

$$\int_{\langle \alpha \rangle \geq \hat{\tau}^{-1}} F_1(\alpha) F_2(\alpha) f_3(\alpha) \cdots f_s(\alpha) e(-\alpha\gamma) \chi_\tau(\alpha) d\alpha = 0.$$

Thus, for Theorem 4.3.2 to hold we want

$$\int_{\mathfrak{m}} F_1(\alpha) F_2(\alpha) f_3(\alpha) \cdots f_s(\alpha) e(-\alpha\gamma) \chi_\tau(\alpha) d\alpha = o(\hat{P}^{s-k})$$

and

$$\int_{\mathfrak{M}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)e(-\alpha\gamma)\chi_\tau(\alpha)d\alpha \gg \hat{P}^{s-k}$$

for sufficiently large values of P.

4.3.1 The Minor Arc

To establish the desired bound on the minor arcs, we need an appropriate Weyl-type estimate and a suitable mean value estimate for $f(\alpha)$. We will closely follow the analysis provided in Sections 3 and 4 of [39], with a slight difference in the proof of one of the lemmas.

The machinery provided by Lemma 4.1 of [39] will still be used to establish a mean value estimate for $f(\alpha)$, without any changes. However, our discussion of the Weyl-type estimate will slightly diverge from what is given by Section 3 of [39]. In [39], the proof of Lemma 3.1 cites a result from a preprint that never appeared in the literature. We will provide a proof analogous to Lemma 3.1 of [39] using a result that does currently exist in the literature.

We will first provide definitions for terms that are used in the statement of the result we will cite. Let $\mathcal{K}$ be a finite set of positive integers. We define the *shadow* of $\mathcal{K}$ to be

$$S(\mathcal{K}) = \left\{ j \in \mathbb{Z}^+ : p \nmid \binom{r}{j} \text{ for some } r \in \mathcal{K} \right\},$$

where we adopt the convention that if $j > r$, $\binom{r}{j} = 0$. We can then construct

$$\mathcal{K}^* = \{k \in \mathcal{K} : p \nmid k \text{ and } p^v k \notin S(\mathcal{K}) \text{ for any } v \in \mathbb{Z}^+\}.$$

In [32], a partial ordering $\preceq_p$ on $\mathbb{N}$ is established. Given $n, m \in \mathbb{N}$, we write $m \preceq_p n$ provided that $p \nmid \binom{m}{n}$. We are now able to state the result we will use in proving Lemma 3.1, which is Theorem 3.1 from [32].

Theorem 4.3.3. *Fix q and a finite set $\mathcal{K} \subset \mathbb{Z}^+$. There exist positive constants ξ and C, depending only on $\mathcal{K}$ and q, such that the following holds. Let $\epsilon > 0$ and let M be sufficiently large in terms of $\mathcal{K}$, ϵ, and q. Suppose that $h(x) = \sum_{r \in \mathcal{K} \cup \{0\}} \alpha_r x^r$ is a polynomial with*

coefficients in $\mathbb{K}_\infty$ *satisfying the bound*

$$\left| \sum_{\langle x \rangle < \hat{M}} e(h(x)) \right| \geq q^{M-\sigma}, \tag{4.5}$$

for some positive number σ *with* $\sigma \leq \xi M$*. Then for each maximal* $k \in \mathcal{K}^*$*, with respect to the partial ordering* $\preceq_p$*, there exist* $a \in \mathbb{F}_q[t]$ *and monic* $g \in \mathbb{F}_q[t]$ *having the property that*

$$\operatorname{ord}(g\alpha_k - a) < -kM + \epsilon M + C\sigma \quad \textit{and} \quad \operatorname{ord} g \leq \epsilon M + C\sigma.$$

For the purpose of this chapter, we set $\mathcal{K} = \{k\}$, $h(x) = \alpha x^k$, $M = P + 1$, $\epsilon = 1/4$, and $\sigma = \min\{P/(4C), \xi P\}$. Furthermore, we have that $\{k\} \subseteq S(\mathcal{K}) \subseteq \{1, \ldots, k\}$ and $\mathcal{K}^* = \{k\}$, since $p \nmid k$ and $p^v k > k$ for all $v \in \mathbb{Z}^+$. Note that k is trivially maximal in $\mathcal{K}^*$ with respect to the partial ordering $\preceq_p$. Thus, if (4.5) holds and P is sufficiently large in terms of k and q, it follows that there exists $a \in \mathbb{F}_q[t]$ and monic $g \in \mathbb{F}_q[t]$ satisfying

$$\operatorname{ord}(g\alpha - a) < -k(P+1) + \epsilon(P+1) + C\sigma < (3/4 - k)P$$

and

$$\operatorname{ord} g \leq \epsilon(P+1) + C\sigma \leq 3P/4.$$

Let $\mathfrak{n}_*$ denote the set of $\alpha \in \mathbb{T}$ such that, for a and monic g in $\mathbb{A}$ satisfying $\operatorname{ord}(g\alpha - a) < (3/4 - k)P$, we have $\operatorname{ord} g > 3P/4$. By the contrapositive of Theorem 4.3.3, there exists a small positive constant $\nu = \nu(q, k)$ such that

$$\sup_{\alpha \in \mathfrak{n}_*} |F(\alpha; P)| \ll \hat{P}^{1-\nu}.$$

We adapt the proof of Lemma 3.1 of [39] using the set $\mathfrak{n}_*$ defined above.

Lemma 4.3.1. *There is a positive constant* c*, depending at most on* k *and* q*, with the following property. Suppose that* P *is a real number, sufficiently large in terms of* k *and* q*.*

Suppose that δ is a positive number with $\hat{P}^{-\nu/2} < \delta \leq 1$. Then, whenever $|F(\alpha)| \geq \delta\hat{P}$, there exist a and g in $\mathbb{A}$ such that $(a, g) = 1$, $1 \leq \langle g \rangle \leq c\delta^{-k}$ and $\langle g\alpha - a \rangle \leq \delta^{-k}\hat{P}^{-k}$.

Proof. Suppose there exists an $\alpha \in \mathbb{K}_\infty$ such that $|F(\alpha)| \geq \delta\hat{P}$, where δ is a positive number with $\hat{P}^{-\nu/2} < \delta \leq 1$. It follows from Lemma 3 of [31], that for all $\alpha \in \mathbb{T}$, there exist unique a and g in $\mathbb{A}$, where $(a, g) = 1$, g is monic, $\langle a \rangle < \langle g \rangle \leq \hat{P}^{k-3/4}$ and $\langle g\alpha - a \rangle < \hat{P}^{-k+3/4}$.

Suppose that $\langle g \rangle > \hat{P}^{3/4}$. Thus, $\alpha \in \mathfrak{n}_*$, and $|F(\alpha)| \ll \hat{P}^{1-\nu}$. Taking P sufficiently large,

$$|F(\alpha)| < \frac{1}{2}\hat{P}^{1-\nu/2} \leq \frac{1}{2}\delta\hat{P}.$$

This contradicts our assumption on the size of $|F(\alpha)|$; thus we assume that $\langle g \rangle \leq \hat{P}^{3/4}$.

By Lemma 4.1 of [33], there exists a positive constant c such that

$$\Big|F(\alpha)\Big| \leq c^{1/k}\hat{P}(\langle g \rangle + \hat{P}^k\langle g\alpha - a \rangle)^{-1/k}.$$

By assumption, we have that $|F(\alpha)| \geq \delta\hat{P}$; thus,

$$\langle g \rangle + \hat{P}^k\langle g\alpha - a \rangle \leq c\delta^{-k}.$$

The result follows. □

The following are Lemma 3.2 and Lemma 3.3 of [39], respectively.

Lemma 4.3.2. *Suppose that S is a fixed real number with $0 < S < \hat{\tau}^{-1}$. Then one has*

$$\lim_{P\to\infty} \sup_{S\leq\langle\alpha\rangle<\hat{\tau}^{-1}} |F_1(\alpha)F_2(\alpha)| = 0.$$

Lemma 4.3.3. *Suppose that $S(P)$ is a function on $(0, \infty)$ that increases monotonically to infinity and satisfies $1 \leq S(P) \leq \hat{P}$. Then there exists a function $T(P)$ on $(0, \infty)$ depending only on λ_1, λ_2, k, q, τ, and $S(P)$, that increases monotonically to infinity, satisfies*

$1 \leq T(P) \leq S(P)$ *and satisfies the property that*

$$\sup_{S(P)\hat{P}^{-k} \leq \langle \alpha \rangle < \hat{\tau}^{-1}} |F_1(\alpha)F_2(\alpha)| \ll \hat{P}^2 T(P)^{-\nu/(2k)}.$$

We have now established a Weyl-type estimate that can provide our desired bound on the minor arc.

Lemma 4.3.4. *Suppose that $u > 2k-2$ is accessible to the exponent k and that $s \geq u+5$. One has*

$$\int_{\mathfrak{m}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)e(-\alpha\gamma)\chi_\tau(\alpha)d\alpha = o(\hat{P}^{s-k}).$$

Proof. Let $v = \lfloor s/2 \rfloor - 2$. By the triangle inequality,

$$\int_{\mathfrak{m}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)e(-\alpha\gamma)\chi_\tau(\alpha)d\alpha \ll \int_{\mathfrak{m}} |F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)|\chi_\tau(\alpha)d\alpha,$$

By Hölder's inequality, we see that

$$\int_{\mathfrak{m}} |F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)|\chi_\tau(\alpha)d\alpha \ll \left(\sup_{\alpha\in\mathfrak{m}} |F_1(\alpha)F_2(\alpha)|\right) \prod_{i=3}^{s} \left(\int_{\langle\alpha\rangle<\hat{\tau}^{-1}} |f_i(\alpha)|^{s-2}d\alpha\right)^{1/(s-2)}.$$

By Lemma 4.1 of [39], we have

$$\int_{\mathbb{T}} |f(\alpha)|^{s-2}d\alpha \ll \hat{P}^{s-2-k}.$$

Using a change of variables, we have that

$$\begin{aligned}
\int_{\langle\alpha\rangle<\hat{\tau}^{-1}} |f_i(\alpha)|^{s-2}d\alpha &= \langle\lambda_i\rangle^{-1} \int_{\langle\alpha\rangle<\langle\lambda_i\rangle\hat{\tau}^{-1}} |f(\alpha)|^{s-2}d\alpha \\
&\ll \sum_{\substack{x\in\mathbb{A} \\ \langle x\rangle<\langle\lambda_i\rangle\hat{\tau}^{-1}}} \int_{\langle\alpha-x\rangle<1} |f(\alpha)|^{s-2}d\alpha \\
&= \sum_{\substack{x\in\mathbb{A} \\ \langle x\rangle<\langle\lambda_i\rangle\hat{\tau}^{-1}}} \int_{\mathbb{T}} |f(\alpha)|^{s-2}d\alpha
\end{aligned}$$

$$\ll \hat{P}^{s-2-k}.$$

Next, we use Lemma 4.3.3 with $S(P) = S_1(P)$ to bound the contribution from the supremum by

$$\sup_{\alpha \in \mathfrak{m}} |F_1(\alpha)F_2(\alpha)| = o(\hat{P}^2).$$

The conclusion of the lemma follows. □

4.3.2 The Major Arc

First, define

$$\mathcal{F}(\alpha) = F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)$$

and

$$\mathcal{G}(\alpha) = F_1(\alpha)\cdots F_s(\alpha).$$

For the major arcs, we want to compare

$$\hat{\tau}\int_{\mathfrak{M}} \mathcal{F}(\alpha)e(-\alpha\gamma)d\alpha$$

to the singular integral

$$J_{s,k} = \int_{\langle\alpha\rangle < \hat{P}^{s-k}} \mathcal{G}(\alpha)e(-\alpha\gamma)d\alpha.$$

The following lemma uses the Dickman function, $\rho(u)$, which is the continuous function on the real numbers that is uniquely defined by the differential equation $u\rho'(u) = -\rho(u-1)$, with the initial condition that $\rho(u) = 1$ for $u \in [0, 1]$.

Lemma 4.3.5. *Suppose that $s \geq k+1$. One has*

$$\int_{\mathfrak{M}} \mathcal{F}(\alpha)e(-\alpha\gamma)d\alpha - \rho(P/R)^{s-2}J_{s,k} \ll \hat{P}^{s-k}(\operatorname{Log}\hat{P})^{-1/(8k)}.$$

Proof. Set $P \geq 1$ large enough so that $2P/\log(2P) < R < P - \log(P)$. From [33] and [39],

we have that

$$\mathcal{F}(\alpha)e(-\alpha\gamma) - \rho(P/R)^{s-k}\mathcal{G}(\alpha)e(-\alpha\gamma) \ll \hat{P}^s(\operatorname{Log}\hat{P})^{-3/8}$$

for $\alpha \in \mathfrak{M}$. It follows by the triangle inequality that

$$\begin{aligned}\int_{\mathfrak{M}} \mathcal{F}(\alpha)e(-\alpha\gamma)d\alpha - \rho(P/R)^{s-2}\int_{\mathfrak{M}} \mathcal{G}(\alpha)e(-\alpha\gamma)d\alpha &\ll \operatorname{meas}(\mathfrak{M})\hat{P}^s(\operatorname{Log}\hat{P})^{-3/8} \\ &\ll \hat{P}^{s-k}(\operatorname{Log}\hat{P})^{-1/4}.\end{aligned} \tag{4.6}$$

Furthermore, Lemma 4.1 in [33] provides the bound

$$F_i(\alpha) \ll \hat{P}(1+\hat{P}^k\langle\alpha\rangle)^{-1/k}.$$

Thus,

$$\begin{aligned}\int_{\mathfrak{M}} \mathcal{G}(\alpha)e(-\alpha\gamma)d\alpha - J_{s,k} &\ll \int_{\mathfrak{T}} \Big|\mathcal{G}(\alpha)\Big|\Big|e(-\alpha\gamma)\Big|d\alpha \\ &\ll \hat{P}^s\int_{\mathfrak{T}}(1+\hat{P}^k\langle\alpha\rangle)^{-s/k}d\alpha,\end{aligned}$$

where $\mathfrak{T} = \{\alpha \in \mathbb{K}_\infty : S_1(P)\hat{P}^{-k} \leq \langle\alpha\rangle\}$.

We note that if we have $\beta \in \mathbb{K}_\infty$ and $n \in \mathbb{Z}$, then

$$\int_{\operatorname{ord}(\alpha-\beta)<-n} d\alpha = q^{-n}.$$

Thus, if we consider the set of $\alpha \in \mathbb{T}$ with $\langle\alpha\rangle = q^\ell$, the measure of that set cannot be more than $q^{\ell+1}$. Set $V = \log_q(S_1(P))$. From the construction of our set $\mathfrak{T}$ and our hypothesis $s \geq k+1$, we have that

$$\begin{aligned}\int_{\mathfrak{M}} \mathcal{G}(\alpha)e(-\alpha\gamma)d\alpha - J_{s,k} &\ll \hat{P}^s\int_{\mathfrak{T}}(1+\hat{P}^k\langle\alpha\rangle)^{-s/k}d\alpha \\ &\ll \hat{P}^s\sum_{V-kP\leq\ell} q^{\ell+1}(1+q^{kP+\ell})^{-s/k}\end{aligned}$$

$$
\begin{aligned}
&\ll \hat{P}^s \sum_{V-kP\le \ell} q^{\ell}(q^{kP+\ell})^{-s/k} \\
&= \hat{P}^s \sum_{V-kP\le \ell} q^{\ell(1-s/k)-sP} \\
&\ll \hat{P}^s q^{(V-kP)(1-s/k)} q^{-sP} \\
&= \hat{P}^{s-k}\hat{V}^{1-s/k} \\
&= \hat{P}^{s-k}(\operatorname{Log}\hat{P})^{-1/(8k)}.
\end{aligned}
$$

Combining the bound above with (4.6) completes the lemma. □

Lemma 4.3.6. *Let $s \ge k+1$, and suppose that the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. For sufficiently large values of P, one has $J_{s,k} \gg \hat{P}^{s-k}$.*

Proof. By Lemma 1 of [31], we have

$$
J_{s,k} = \int_{\langle\alpha\rangle<\hat{P}^{1-k}} \mathcal{G}(\alpha)e(\alpha\gamma)d\alpha = \hat{P}^{1-k}W, \tag{4.7}
$$

where W denotes the number of s-tuples $(x_1,\dots,x_s)\in\mathbb{A}^s$ with

$$
\langle\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma\rangle < \hat{P}^{k-1} \tag{4.8}
$$

and $\langle x_i\rangle \le \hat{P}$ for $1\le i\le s$. As in [39], choose r such that $\langle\lambda_r z_r^k\rangle$ is maximal. Let $d = \operatorname{ord}\lambda_r$ and $w = \operatorname{lead}\lambda_r$. For $1\le i\le s$, we define a_i by

$$
a_i = \begin{cases} \operatorname{lead} z_i, & \text{when } \langle\lambda_i z_i^k\rangle = \langle\lambda_r z_r^k\rangle; \\ 0, & \text{otherwise,} \end{cases}
$$

and m_i as

$$
m_i = \left\lfloor \frac{d - \operatorname{ord}\lambda_i + k\cdot\operatorname{ord} z_r}{k} \right\rfloor.
$$

Let $n = \lfloor P\rfloor - \max\limits_{1\le i\le s} m_i - \max\left(0, \left\lceil \dfrac{d}{k-1}\right\rceil\right)$, and suppose that P is large enough so that

$n + m_i > 0$ for $1 \leq i \leq s$ and $d + k(n + m_r) > \operatorname{ord} \gamma$. For $1 \leq i \leq s$, write $x_i \in \mathbb{A}$ as $x_i = a_i t^{n+m_i} + y_i$, where $y_i \in \mathbb{A}$ and $\operatorname{ord} y_i < n + m_i$. Let

$$x_r = a_r t^{n+m_r} + b_{n+m_r-1} t^{n+m_r-1} + \cdots + b_0,$$

where each $b_i \in \mathbb{F}_q$. We define $c_l \in \mathbb{F}_q$ via the relation

$$\lambda_1 x_1^k + \cdots + \lambda_s x_s^k - \gamma = \sum_{l=-\infty}^{\infty} c_l t^l.$$

Thus, (4.8) holds when $c_l = 0$ for all $l \geq (k-1)P$. We note that $c_l = 0$ for all $l > d+k(n+m_r)$ via the relation

$$\operatorname{ord} \lambda_i + k(n + m_i) \leq d + k(n + m_r).$$

Also, the coefficient $c_{d+k(n+m_r)} = 0$ by the definition for a_i, the construction of the x_i, and our hypothesis.

We consider what occurs when

$$d + (k - 1)(n + m_r) \leq l < d + k(n + m_r).$$

From our construction of the x_i, we have

$$c_l = kwa_r^{k-1} b_{l-d-(k-1)(n+m_r)} + h_l,$$

where h_l is an element of $\mathbb{F}_q$ depending at most on $\boldsymbol{\lambda}$, $\mathbf{a}$, γ, b_i with $i > l-d-(k-1)(n+m_r)$, and y_j with $j \neq r$.

For $j \neq r$, let y_j be arbitrarily selected. Note that $kwa_r^{k-1} \neq 0$. We can choose b_{n+m_r-1} so that $c_{d+k(n+m_r)-1} = 0$, and similarly we can then select b_{n+m_r-2} so that $c_{d+k(n+m_r)-2} = 0$. Continuing in this manner, we can choose x_r such that $c_l = 0$ for all $l \geq d + (k-1)(n+m_r)$.

From our construction of n,

$$\begin{aligned} d + (k-1)(n+m_r) &\leq (k-1)(\lfloor P \rfloor - \max_{1\leq i\leq s} m_i + m_r) \\ &\leq (k-1)P. \end{aligned}$$

Then, due to the y_j being arbitrarily selected for $j \neq r$, $W \gg \hat{P}^{s-1}$ for P sufficiently large. In summary, by (4.7), $J_{s,k} \gg \hat{P}^{s-k}$. □

Combining the results of the previous lemmas gives us the following:

Lemma 4.3.7. *Let $s \geq k+1$, and suppose that the equation $\lambda_1 z_1^k + \cdots + \lambda_s z_s^k = 0$ has a non-trivial solution $\mathbf{z}$ in $\mathbb{K}_\infty^s$. For sufficiently large values of P, one has*

$$\int_{\mathfrak{M}} F_1(\alpha)F_2(\alpha)f_3(\alpha)\cdots f_s(\alpha)e(-\gamma\alpha)\chi_\tau(\alpha)d\alpha \gg \hat{P}^{s-k}.$$

Theorem 4.3.2 now follows by Lemma 4.3.4 and Lemma 4.3.7.

Bibliography

[1] A. Alnaser and T. Cochrane. Waring's number mod m. *J. Number Theory*, 128(9): 2582–2590, 2008. ISSN 0022-314X,1096-1658. doi: 10.1016/j.jnt.2008.03.006. URL https://doi.org/10.1016/j.jnt.2008.03.006.

[2] A. Alnaser, T. Cochrane, M. Ostergaard, and C. Spencer. Waring numbers for diagonal congruences. *Rocky Mountain J. Math.*, 50(3):825–838, 2020. ISSN 0035-7596,1945-3795. doi: 10.1216/rmj.2020.50.825. URL https://doi.org/10.1216/rmj.2020.50.825.

[3] R. C. Baker. Small solutions of congruences. *Mathematika*, 30(2):164–188, 1983. doi: https://doi.org/10.1112/S0025579300010512. URL https://londmathsoc.onlinelibrary.wiley.com/doi/abs/10.1112/S0025579300010512.

[4] R. C. Baker. *Diophantine inequalities*, volume 1 of *London Mathematical Society Monographs. New Series*. The Clarendon Press, Oxford University Press, New York, 1986. ISBN 0-19-853545-7. Oxford Science Publications.

[5] V. Bentkus and F. Götze. Lattice point problems and distribution of values of quadratic forms. *Ann. of Math. (2)*, 150(3):977–1027, 1999. ISSN 0003-486X,1939-8980. doi: 10.2307/121060. URL https://doi.org/10.2307/121060.

[6] J. Brüdern and T. D. Wooley. On Waring's problem for larger powers. *J. Reine Angew. Math.*, 805:115–142, 2023. ISSN 0075-4102,1435-5345. doi: 10.1515/crelle-2023-0072. URL https://doi.org/10.1515/crelle-2023-0072.

[7] M. Car. Le problème de Waring pour l'anneau des polynômes sur un corps fini. In *Séminaire de Théorie des Nombres, 1972–1973 (Univ. Bordeaux I, Talence)*, pages Exp.

No. 6, 13. Centre National de Recherche Scientifique, Laboratoire de Théorie des Nombres, Talence, 1973.

[8] A. Cauchy. Recherches sur les nombres. *J. École Polytech.*, 9:99–116, 1813.

[9] C. Chevalley. Démonstration d'une hypothèse de M. Artin. *Abh. Math. Sem. Univ. Hamburg*, 11(1):73–75, 1935. ISSN 0025-5858,1865-8784. doi: 10.1007/BF02940714. URL https://doi.org/10.1007/BF02940714.

[10] S. Chow, S. Lindqvist, and S. Prendiville. Rado's criterion over squares and higher powers. *J. Eur. Math. Soc. (JEMS)*, 23(6):1925–1997, 2021. ISSN 1435-9855,1435-9863. doi: 10.4171/JEMS/1047. URL https://doi.org/10.4171/JEMS/1047.

[11] J. A. Cipra. *Waring's number in finite fields*. ProQuest LLC, Ann Arbor, MI, 2010. ISBN 978-1124-04000-4. URL http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:3408116. Thesis (Ph.D.)–Kansas State University.

[12] J. A. Cipra, T. Cochrane, and C. Pinner. Heilbronn's conjecture on Waring's number (mod p). *J. Number Theory*, 125(2):289–297, 2007. ISSN 0022-314X,1096-1658. doi: 10.1016/j.jnt.2006.12.001. URL https://doi.org/10.1016/j.jnt.2006.12.001.

[13] T. Cochrane and C. Pinner. Sum-product estimates applied to Waring's problem mod p. *Integers*, 8:A46, 18, 2008. ISSN 1553-1732.

[14] T. Cochrane, C. Spencer, and K. Wilson. Waring numbers for diagonal congruences, II. (submitted).

[15] T. Cochrane, M. Ostergaard, and C. Spencer. Solutions to diagonal congruences with variables restricted to a box. *Mathematika*, 64(2):430–444, 2018. ISSN 0025-5793,2041-7942. doi: 10.1112/S0025579318000025. URL https://doi.org/10.1112/S0025579318000025.

[16] T. Cochrane, M. Ostergaard, and C. Spencer. Homogeneous additive congruences. *Rocky Mountain J. Math.*, 52(4):1295–1317, 2022. ISSN 0035-7596,1945-3795. doi: 10.1216/rmj.2022.52.1295. URL https://doi.org/10.1216/rmj.2022.52.1295.

[17] T. Cochrane, M. Ostergaard, C. Spencer, and K. Wilson. A note on small solutions of diagonal congruences. pre-print, 2025.

[18] H. Davenport. On the Addition of Residue Classes. *J. London Math. Soc.*, 10(1): 30–32, 1935. ISSN 0024-6107,1469-7750. doi: 10.1112/jlms/s1-10.37.30. URL https://doi.org/10.1112/jlms/s1-10.37.30.

[19] H. Davenport. On Waring's problem for fourth powers. *Ann. of Math. (2)*, 40:731–747, 1939. ISSN 0003-486X. doi: 10.2307/1968889. URL https://doi.org/10.2307/1968889.

[20] H. Davenport and H. Heilbronn. On indefinite quadratic forms in five variables. *J. London Math. Soc.*, 21:185–193, 1946. ISSN 0024-6107,1469-7750. doi: 10.1112/jlms/s1-21.3.185. URL https://doi.org/10.1112/jlms/s1-21.3.185.

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

[22] M. Dodson. Homogeneous additive congruences. *Philos. Trans. Roy. Soc. London Ser. A*, 261:163–210, 1967. ISSN 0080-4614. doi: 10.1098/rsta.1967.0002. URL https://doi.org/10.1098/rsta.1967.0002.

[23] P. Erdös and R. Rado. Intersection theorems for systems of sets. *J. London Math. Soc.*, 35:85–90, 1960. ISSN 0024-6107,1469-7750. doi: 10.1112/jlms/s1-35.1.85. URL https://doi.org/10.1112/jlms/s1-35.1.85.

[24] D. E. Freeman. Asymptotic lower bounds for Diophantine inequalities. *Mathematika*, 47 (1-2):127–159, 2000. ISSN 0025-5793. doi: 10.1112/S0025579300015771. URL https://doi.org/10.1112/S0025579300015771.

[25] D. E. Freeman. Asymptotic lower bounds and formulas for Diophantine inequalities. In *Number theory for the millennium, II (Urbana, IL, 2000)*, pages 57–74. A K Peters, Natick, MA, 2002. ISBN 1-56881-146-2.

[26] 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. Z.*, 12 (1):161–188, 1922. ISSN 0025-5874,1432-1823. doi: 10.1007/BF01482074. URL https://doi.org/10.1007/BF01482074.

[27] G. H. Hardy and S. Ramanujan. Asymptotic Formulaae in Combinatory Analysis. *Proc. London Math. Soc. (2)*, 17:75–115, 1918. ISSN 0024-6115. doi: 10.1112/plms/s2-17.1.75. URL https://doi.org/10.1112/plms/s2-17.1.75.

[28] H. Heilbronn. Lecture notes on additive number theory mod p. *California Institute of Technology*, 169:170, 1964.

[29] C.-N. Hsu. Diophantine inequalities for polynomial rings. *J. Number Theory*, 78(1): 46–61, 1999.

[30] C.-N. Hsu. Diophantine inequalities for the non-Archimedean line $\mathbb{F}_q((1/T))$. *Acta Arith.*, 97(3):253–267, 2001. ISSN 0065-1036,1730-6264. doi: 10.4064/aa97-3-5. URL https://doi.org/10.4064/aa97-3-5.

[31] R. M. Kubota. Waring's problem for $\mathbf{F}_q[x]$. *Dissertationes Math. (Rozprawy Mat.)*, 117: 60, 1974. ISSN 0012-3862.

[32] T. H. Lê, Y.-R. Liu, and T. D. Wooley. Equidistribution of polynomial sequences in function fields, with applications, 2023. arXiv:1311.0892.

[33] Y.-R. Liu and T. D. Wooley. Waring's problem in function fields. *J. Reine Angew. Math.*, 638:1–67, 2010. ISSN 0075-4102,1435-5345. doi: 10.1515/CRELLE.2010.001. URL https://doi.org/10.1515/CRELLE.2010.001.

[34] V. Ramaswami. On the number of positive integers less than x and free of prime divisors greater than x^c. *Bull. Amer. Math. Soc.*, 55:1122–1127, 1949. ISSN 0002-9904. doi: 10.1090/S0002-9904-1949-09337-0. URL https://doi.org/10.1090/S0002-9904-1949-09337-0.

[35] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962. ISSN 0019-2082. URL http://projecteuclid.org/euclid.ijm/1255631807.

[36] A. Sárközy. On products and shifted products of residues modulo p. *Integers*, 8(2):A9, 8, 2008. ISSN 1553-1732.

[37] W. M. Schmidt. Small zeros of additives forms in many variables. ii. *Acta Math.*, 143: 219–232, 1979.

[38] W. M. Schmidt. Small solutions of congruences with prime modulus. In *Diophantine analysis (Kensington, 1985)*, volume 109 of *London Math. Soc. Lecture Note Ser.*, pages 37–66. Cambridge Univ. Press, Cambridge, 1986. ISBN 0-521-33923-5.

[39] C. V. Spencer. Diophantine inequalities in function fields. *Bull. Lond. Math. Soc.*, 41(2):341–353, 2009. ISSN 0024-6093,1469-2120. doi: 10.1112/blms/bdp008. URL https://doi.org/10.1112/blms/bdp008.

[40] R. C. Vaughan. A new iterative method in Waring's problem. *Acta Math.*, 162(1-2):1–71, 1989. ISSN 0001-5962,1871-2509. doi: 10.1007/BF02392834. URL https://doi.org/10.1007/BF02392834.

[41] I. M. Vinogradov. On an upper bound for $G(n)$. *Izv. Akad. Nauk SSSR Ser. Mat.*, 23: 637–642, 1959. ISSN 0373-2436.

[42] A. Weil. Numbers of solutions of equations in finite fields. *Bull. Amer. Math. Soc.*, 55: 497–508, 1949. ISSN 0002-9904. doi: 10.1090/S0002-9904-1949-09219-4. URL https://doi.org/10.1090/S0002-9904-1949-09219-4.

[43] K. Wilson. A note on Diophantine inequalities in function fields. *Notes Number Theory Discrete Math.*, 30(4):776–786, 2024. ISSN 1310-5132,2367-8275. doi: 10.7546/nntdm.2024.30.4.776-786. URL https://doi.org/10.7546/nntdm.2024.30.4.776-786.

[44] T. D. Wooley. New estimates for smooth Weyl sums. *J. London Math. Soc. (2)*, 51 (1):1–13, 1995. ISSN 0024-6107,1469-7750. doi: 10.1112/jlms/51.1.1. URL https://doi.org/10.1112/jlms/51.1.1.

[45] T. D. Wooley. On Diophantine inequalities: Freeman's asymptotic formulae. In *Proceedings of the Session in Analytic Number Theory and Diophantine Equations*, volume 360 of *Bonner Math. Schriften*, page 32. Univ. Bonn, Bonn, 2003.