University of New Mexico

UNM Digital Repository

Mathematics & Statistics ETDs

Electronic Theses and Dissertations

Spring 5-12-2024

On the Limitations and Restrictions of the Hardy-Littlewood Circle Method

Daniel W. Havens

University of New Mexico - Main Campus

Follow this and additional works at: https://digitalrepository.unm.edu/math_etds

Part of the Mathematics Commons

Recommended Citation

Havens, Daniel W.. "On the Limitations and Restrictions of the Hardy-Littlewood Circle Method." (2024). https://digitalrepository.unm.edu/math_etds/205

This Thesis is brought to you for free and open access by the Electronic Theses and Dissertations at UNM Digital Repository. It has been accepted for inclusion in Mathematics & Statistics ETDs by an authorized administrator of UNM Digital Repository. For more information, please contact disc@unm.edu.

Daniel W. Havens

Candidate

Mathematics & Statistics

Department

This thesis is approved, and it is acceptable in quality and form for publication:

Approved by the Thesis Committee:

Prof. Maria Cristina Pereyra , Chairperson

Prof. Matthew Blair

Prof. Maxim Zinchenko

On the Limitations and Restrictions of the Hardy-Littlewood Circle Method

by

Daniel W. Havens

B.S. Mathematics, Utah Valley University, 2021

THESIS

Submitted in Partial Fulfillment of the Requirements for
the Degree of

Master of Science in Mathematics

The University of New Mexico

Albuquerque, New Mexico

May, 2024

Dedication

To my grandparents, Bobbie Lu and John, for their support in raising me, and for the love of education which they instilled in me from a young age.

Acknowledgments

I would like to thank my advisor, Professor Maria Cristina Pereyra, for her support in pursuing my own interests over those which she can support. I would also like to thank Dr. Maxim Zinchenko and Dr. Matthew Blair, for the support they have shown me as members of my committee. Finally, my fellow graduate students José Garcia, Austin Bell, and Sarah Poiani all have my thanks, as their support has helped me beyond what words could describe.

On the Limitations and Restrictions of the Hardy-Littlewood Circle Method

by

Daniel W. Havens

B.S. Mathematics, Utah Valley University, 2021

M.S., Mathematics, University of New Mexico, 2024

Abstract

We discuss herein the history, layout, and philosophy of the Hardy-Littlewood Circle method, as well as the more modern renditions thereof. The limitations and scope of each method presented is discussed in detail, providing examples of cases where the failure of the circle method is of relevance. We include a summary of famous problems which have been resolved using each methodology, as well as what limitations each methodology showcases.

Contents

Glossary

$e(x)$ — The multiplicative unit-period exponential function, $e^{2\pi i x}$.

$\ll, \gg$ — The Vinogradov symbols, where $f \ll g$ denotes the existince of a constant c such that $f(x) \leq cg(x)$ for all x, and $\gg$ is defined similarly.

$\mu(n)$ — The Möbius μ function, given to be 0 if n is not square-free, 1 if n is square-free and has an even number of prime factors, and 1 otherwise.

$\Lambda(n)$ — The Von Mangoldt function, given to be $\log(p)$ if $n = p^k$ for some positive integer k, and 0 otherwise.

$\vartheta(n)$ — The Chebyshev (theta) function, given by the sum of the logs of all primes less than or equal to n.

$\lambda(n)$ — The Louiville function, given by 1 if the sums of the prime powers is even, and -1 otherwise.

Chapter 1

Introduction

1.1 Overview

In this chapter, we outline the historical motivation and background for the theory. The goal is to give the reader enough background that they can understand what sorts of problems the circle method has been historically useful for, and to be able to understand when it may be a profitable approach to handle a problem. This includes an outline of the circle method itself, which leads us into our discussion of its limitations.

Chapter 2 covers the historical developments of Vinogrodov in [27], and what the circle method has looked like historically before that. This provides more of a viewpoint as to the developments that have taken place historically rather than the current developments that are taking place. This includes a survey of the removal of the Generalized Riemann Hypothesis as an assumption for standard results obtained via the circle method.

Chapter 3 focuses on what limitations the circle method faces regarding problems involving prime numbers. A short discussion on why the Strong Goldbach problem remains out of reach, while the Weak Goldbach problem was solved in 2013 are included. We then summarize the known analysis of the Von Mangoldt function, including a discussion of its use in the modern theory. We conclude the chapter by discussing the twin prime conjecture in detail.

Chapter 4 focuses primarily on the adaptation to higher order Fourier analysis, as well as current open problems in the field. The limitations here are primarily induced by the lack of an appropriate analogue to Parseval's identity, leading ultimately to needing to pass to the group setting and apply the Gower's norms in order to appropriately bypass these limitations. But in doing so, we lose the sharp bounds one expects to gain with the circle method. This development was almost explicitly to side-step known issues, such as the issues with two-term Diophantine equations discussed in previous chapters.

Chapter 5 coveres briefly some issues and related developments that were are generally beyond the scope of the rest of the thesis. This includes the recent work with efficient congruencing, a brief overview of general improvements of the circle method, and a discussion on the restrictions related to two-term Diophantine equations.

1.2 Historical Motivations

The Circle Method, often called the Hardy-Littlewood or sometimes the Hardy-Littlewood-Vinogradov method, is a centerpiece for additive number theory, and serves as a basis for most of the theory. It traces its origins to a series of papers by G.H. Hardy and J. Littlewood titled *Some problems of 'Partitio numerorum'*, stretching from 1920 to 1928 [2] [3] [5] [4] [6] [7] [8], with article VII being an unpublished manuscript (see [17], paragraph three for details). However, most experts agree that the method itself began earlier, and was used in the motivation of one of

Hardy's earlier papers with Ramanujan in 1916 [9]. The early applications focused primarily on partitioning problems and on Waring's problems.

Broadly speaking, the method operates by exploiting a method reminiscent of an inverse Fourier transform to extrapolate information about counting problems. It was driven broadly by the fascination with complex analysis held by mathematicians of the time, and therefore the involved integration was, at the time, performed along the complex unit circle. Nowadays, the circle method has been stripped of much of the underlying nuances, and much more refined. For instance, see the next chapter for an account of the reliance of early results on the Generalized Riemann Hypothesis.

Notable refinements following from the original circle method include those performed by Vinogradov, where he truncated the series [27], and provided other refinements. This ultimately concluded with the removal of the requirement for the Generalized Riemann Hypothesis to extract the desired results.

1.3 Problems of Interest and the Circle Method

The circle method aims, roughly, to determine the number of solutions to a Diophantine equation within some error bound. This is done by leveraging the structure of the unit-period Fourier transform, along with the analytic properties of exponential functions.

Namely, one would like to define the number of solutions to an equation

$$n = a_1 m_1 + a_2 m_2 + \ldots + a_k m_k. \tag{1.1}$$

The traditional way to do this is to construct a function $f(\theta)$ of the form

$$f(\theta) = \sum_{m_i \in \mathbb{Z}} e(a_1 m_1 \theta) e(a_2 m_2 \theta) \ldots e(a_k m_k \theta)$$

where $e(\theta) = e^{2\pi i\theta}$ denotes the unit-period exponential function, and then to analyze the Fourier transform

$$J(n) = \int_0^1 f(\theta)e(-n\theta)\ d\theta.$$

This leverages the multiplicative-to-additive properties of the exponential function, to count the number of solutions to the equation 1.1. To see this, note that for every collection of m_i values for which do not yield a solution to 1.1 for n, the integral contributes nothing and evaluates to zero. However, when the m_i values do yield a solution, the exponent becomes zero, and the integral contributes a factor of one.

So, in the framework of problems surrounding the circle method, proving the desired theorem usually boils down to showing that for sufficiently large n, $J(n) > \epsilon$ for some positive ϵ. Since $J(n)$ is always integer valued in this context, showing an epsilon-bound shows a non-negative integer-valued bound, giving us the desired result. The second part of any such problem, once proven, is to obtain the tightest bound on the n values as possible. That is, to put in clear context with the best bound possible what "sufficiently large n" means for that given problem.

A standard variant of problems solved by the circle method is, "How many numbers a_k which are in a set S are required to represent every number in a set T". For these problems, it is more standard to write a single exponential function

$$f(\theta) = \sum_{m\in S} e(m\theta) \tag{1.2}$$

and then determine a bound for the integral

$$J(n) = \int_0^1 (f(\theta))^k e(-n\theta)\ d\theta \tag{1.3}$$

in terms of k, given that n lies in the set T.

With this refined phrasing in mind, one can re-frame the original, more clunky infinite sums of the general case (where $S = \mathbb{Z}$) to truncated finite sums, where for m_i values outside of this truncated set S, depending on n, there is no hope of m_i providing a solution to our equation for our given n. A generalized argument for the truncation of these trigonometric series can be found in Vinogradov's paper [27]. For an overview of what the circle method looked like before this, see chapter 2. However, to summarize the results contained therein, many results obtained via the circle method were known only if the generalized Riemann hypothesis was true. Vinogradov's contributions helped us remove this assumption.

The circle method refers to the particular decomposition of the integral into the so-called "major" and "minor" arcs. The major arcs are denoted $\mathfrak{M}$ and the minor arcs are denoted $\mathfrak{m}$, and a dependence on n is generally assumed (so perhaps the notation $\mathfrak{M}_n$ and $\mathfrak{m}_n$ would be more appropriate).

The details of this decomposition are generally as follows:

- The minor arcs are the collection of intervals where one expects either averaging or extremely unpredictable behavior of the function $|f(\theta)|^k$
- The major arcs are the collection of intervals where one has good L^1 and L^2 estimates on the function $(f(\theta))^k$.
- Both the major and minor arcs consist of finitely many intervals (with the number and length of those intervals often depending on n), centered at rational points with relatively small denominator.

The reasons guiding why one would decompose the interval in such a way are outlined in the next section, but from here, one may decompose the integral to get that

$$J(n) = \int_{\mathfrak{M}} (f(\theta))^k e(-n\theta)\ d\theta + \int_{\mathfrak{m}} (f(\theta))^k e(-n\theta)\ d\theta,$$

where the integral across the major arcs collects the most contributions, and the integral across the minor arcs is treated as an error term.

From here, the bounding on $J(n)$ comes in terms of how strong your estimates on the major and minor arcs are. In general, tight upper bounds on the minor arcs tend to be more important than tight lower bounds on the major arcs due to the choice of decomposition.

1.4 The Philosophy of the Circle Method

While each problem utilizing the circle method is unique (it is a method, and not a theorem, after all), there is a general ansatz for how one tends to handle problems in the circle method. The ansatz is specialized towards problems utilizing equations 1.2 and 1.3. That is, taking a helping function, raising it to a power, and bounding. The approach also generally works for fixed values of k, but it was developed first for Waring's problem (where k varies).

First, one notes that the terms in the exponential function $(f(\theta))^k e(-n\theta)$, each of the components (the parts in the sum defining f, and the $n\theta$ term) are periodic with each having a relatively small rational period, where the exact smallest period being determined by where one truncates the sum defining S. So, one expects the minima and maxima of $(f(\theta))^k e^{-n\theta}$ to be at points which are multiples of the product of these periods. To phrase it differently, one expects the minima and maxima of the function to be attained at rational points with relatively small denominator.

Knowing this, one may then decompose the unit interval into the arcs, with each interval making up the arcs being either based around these rational points, or being the complement of intervals based at these points, called the arcs. One categorizes an arc as major if there are strong L^1 and L^2 bounds on the function $f(\theta)$ in that arc, and minor otherwise. This bounding creates the dichotomy of the integral across the major arcs being considered the control term, while the integral across the minor arcs is considered to be the error term.

Indeed, one typically expects the major arcs to behave in a way that reflects the typical behavior of the function, while the minor arcs reflect the more extreme behavior of the function. In this way, one expects that if there is a bound on the minor arcs, say, in terms of a function $h(n)$, then one can determine the behavior of the major arcs in terms of some arithmetic averaging term A (based on the density of the major arcs compared to the minor arcs), as well as a correction term $\mathfrak{G}(n)$, primarily determined by the density of the set S in the definition of $f(x)$ in equation 1.2.

Putting this all together, the belief is that one can show that

$$J(n) = Ah(n)\mathfrak{G}(n) + O(h(n)).$$

So, when tackling a circle method problem, the usual method is to establish a tight enough bound $h(n)$ so that the corresponding function $\mathfrak{G}(n)$ (called the singular series) grows faster than a constant.

Obtaining a lower bound for the point at which $Ah(n)\mathfrak{G}(n)$ is known to exceed the bound $O(h(n))$ yields a number of cases which may be checked by hand, from which the result is given. On the other hand, if one simply desires a bound for how a function grows, this follows directly from the work done up to this point.

For more details on the inner workings of the circle method, the standard reference of Vaughan's book [26] will serve most well. For those wanting a more gentle introduction, the text by Murty and Sinha is also a good reference [16]. Both texts teach primarily through example, and the text by Vaughan highlights some of the more exotic applications of the circle method, such as Birch's theorem.

1.5 Noteworthy Problems Solved by the Circle Method

As with any method in mathematics, in order to gain deeper insights into the method, it is often useful to look at what problems have been solved with it. The primary four are as follows:

- Waring's problem
- Vinogradov's mean value theorem
- Roth's theorem on progressions
- The weak Goldbach problem

Historically, Waring's problem is where the circle method first become profitable outside of partitioning problems. However, the circle method found its more modern place with Vinogradov's mean value theorem, where it became a centerpiece for analyzing Diophantine equations of many variables. The methods and efficiency bounds on Vinogradov's mean value theorem have since become the driving force behind several new applications of the circle method, providing the sharpest bound on many current theorems [15].

Theorem 1 (Waring's Problem)**.** *For every natural number k, there is a number $g(k)$ such that every natural number n can be written in the form*

$$n = a_1^k + a_2^k + \ldots + a_{g(k)}^k$$

for $a_1, \ldots, a_{g(k)}$ non-negative integers.

Theorem 2 (Vinogradov's Mean Value Theorem)**.** *Let $J_{s,k}(n)$ denote the number of solutions to the k simultaneous equations*

$$\begin{aligned}
x_1^1 + x_2^1 + \ldots + x_s^1 &= y_1^1 + y_2^1 + \ldots + y_s^1 \\
x_1^2 + x_2^2 + \ldots + x_s^2 &= y_1^2 + y_2^2 + \ldots + y_s^2 \\
&\vdots \\
x_1^k + x_2^k + \ldots + x_s^k &= y_1^k + y_2^k + \ldots + y_s^k
\end{aligned}$$

with $x_i, y_i \in \mathbb{Z}$, $1 \leq x_i, y_i \leq n$. Then, for any $\epsilon > 0$, we have that

$$J_{k,s}(n) \ll n^{s+\epsilon} + n^{2s-\frac{k(k+1)}{2}+\epsilon}$$

Roth's theorem on progressions provided an example of a setting where the circle method was profitable, despite not directly counting solutions to a Diophantine equation. There, the error bounds obtained on Vinogradov's mean value theorem drive the bounds on the sizes of sets required for the result to follow.

Theorem 3 (Roth's Theorem on Progressions)**.** *Let $r_3(n)$ denote the size of the largest subset of $\{1, 2, \ldots, n\}$ which does not contain three terms in an arithmetic progression. Then there is an absolute constant $c > 0$ such that*

$$r_3(n) \leq \exp\left(-c(\log(n))^{\frac{1}{9}}\right) n.$$

It is worth noting that, as of the time this thesis is written, the above is the current best bound. The original version that was proved was that $r_3(n) \ll \frac{n}{\log(\log(n))}$.

More recently, however, the scene has changed greatly with the proof of the weak Goldbach problem by H. Helfgott. His proof was quite long, with original drafts stretching upwards of 600 and 400 pages for the major and minor arc analysis respectively (see [11] and [12]), and Helfgott has even stated that the shortest version of the final proof would be, at the very least, 240 pages long. It is no exaggeration to say that the weak Goldbach problem stressed the circle method to its limits, and as it stands, the strong Goldbach problem is out of reach.

Theorem 4 (Weak Goldbach Problem)**.** *Every odd number greater than five is the sum of three prime numbers.*

There are also, of course, various other applications of the circle method, including the original problems in partitioning [9] and applications towards the theory of discrete analogues to singular integrals, such as in [19]. However, these are of less interest historically.

Chapter 2

The Original Circle Method and the Generalized Riemann Hypothesis

2.1 The Generalized Riemann Hypothesis

Here, we provide a summary of the work by Hardy and Littlewood on the weak Goldbach problem found in [5] and [6]. Their work therein is the most classic example of a result stemming from the circle method which depends directly on the Generalized Riemann Hypothesis.

To understand the Generalized Riemann Hypothesis, we first provide a brief glossary of terms for those unfamiliar. A Dirichlet character is a function $\chi : \mathbb{Z} \to \mathbb{C}$ which is a multiplicative embedding of $\mathbb{Z}/N\mathbb{Z}$ for some N. In particular, we have the following three defining properties:

- $\chi(ab) = \chi(a)\chi(b)$

- $\chi(a+N) = \chi(a)$ for all a and some fixed N.
- $\chi(a) = 0$ if and only if $\gcd(a, N) \neq 1$, with N as given above.

These give rise to the L-functions, which are the natural analogues of the zeta function for questions dealing with the distribution of primes in arithmetic progressions:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}.$$

L-functions give rise to many important results in analytic number theory, such as Dirichlet's theorem on arithmetic progressions. The statement of the Generalized Riemann Hypothesis is similar to that of the traditional Riemann hypothesis, and just as the Riemann Hypothesis gives us information about the distribution of primes, the generalized version gives us information about the distribution of primes in arithmetic progressions.

Conjecture 1 (Generalized Riemann Hypothesis)**.** *For any fixed Dirichlet character χ and every complex number s, if $L(\chi, s) = 0$, then either $s \in (-\infty, 0)$, or $Re(s) = \frac{1}{2}$.*

This directly gives us the standard Riemann Hypothesis by taking the trivial (principle) character, $\chi(n) = 1$. Just as one prefers to think of the standard Riemann hypothesis in terms of the bound it gives on the prime number theorem, one may think of the Generalized Riemann Hypothesis as giving the following version of the prime number theorem in sequences:

Theorem 5 (Prime Number Theorem for Arithmetic Progressions)**.** *if $\pi(n, p, q)$ denotes the number of primes in the progression $\{pk + q | k \in \mathbb{N}\}$, $n \geq q$ we assume the Generalized Riemann Hypothesis, then*

$$\pi(n, p, q) = \frac{1}{\phi(q)} \int_2^n \frac{1}{\ln(x)}\, dx + O(n^{\frac{1}{2}} \ln(n)).$$

2.2 Generalized Riemann and Goldbach

The work of Hardy and Littlewood in their papers [5] and [6] ultimately achieved the weak Goldbach conjecture assuming the Generalized Riemann Hypothesis, roughly ninety years before Helfgott achieved the same result without it in [12] and [11]. This is part of a long-standing tradition in number theory to assume the Riemann or even the Generalized Riemann Hypothesis if it assists in proving the desired result. This is due to the general consensus in analytic number theory that while unproven, these results are either true, or close enough to being true that their counterexamples would be gotten rid of with a few minor additions to the theorem statement. Doing so can give us an idea of if a theorem is even reasonably provable or not.

Here, we provide a sketch of the proof of the weak Goldbach problem assuming the Generalized Riemann Hypothesis

Theorem 6 (Weak Goldbach assuming GRH)**.** *Assuming the Generalized Riemann Hypothesis, every odd number n greater than five is the sum of three primes.*

The primary difference from the current circle method is in that the analogue of equation 1.2, the sum is not truncated. Instead, we have the weighted sum

$$f(x) = \sum_{p \text{ prime}} \log(p) e(px) \tag{2.1}$$

Before we begin sketching the proof, as a final historical note, it is good to know that not all of the results of Hardy and Littlewood required the full generalized Riemann hypothesis. Instead, they required the weaker version (called Hypothesis R in their papers), which is that every non-trivial zero of an L function has real part less than $\frac{3}{4}$. With this out of the way, we begin our summary of the work in these papers.

Denoting $\Lambda(n)$ for the Von Mangoldt function:

$$\Lambda(n) = \begin{cases} \log(p) & n = p^k,\ p\text{prime} \\ 0 & \text{otherwise} \end{cases}$$

The first order of business in the proof of Hardy and Littlewood is to establish that one may split f appropriately into two functions which we may bound individually:

$$f(x) = f_1(x) + f_2(x) = \left(\sum_{\gcd(q,n)\geq 1} \Lambda(n)x^n \right) + \left(\sum_{p \text{ prime}} \log(p)(x^{p^2} + x^{p^3} + \dots) \right)$$

where q is the denominator of the center of the nearest major arc. This estimate only holds for suitable arcs, and this is part of the theorem statement proper (see Lemma 1 of [5]).

The bound on f_1 is established without too much technical work involved, and is given by showing that there exists a universal constant A such that

$$|f_1(x)| < A(\log(q+1))^A(\eta)^{-1/2}$$

where $0 < \eta < 1$ is a constant fixed by the arc. Bounding f_2 non-trivially, however, requires significantly more work. This is because one may realize f_2 to be equal to the (contour) integral

$$f_2(x) = \frac{1}{2\pi i} \int_{2-i\infty}^{2+i\infty} Y^{-s}\Gamma(s) \sum_{k=1}^{h} C_k \frac{L'(\chi_h, s)}{L(\chi_h, s)}\, ds$$

where Y is a constant dependent on the arc, h is a constant determined by the choice of major arcs, χ_h denoting a non-trivial Dirichlet character modulo h, and the C_ks are a well-behaved family of constants determined uniquely by the center of the nearest arc and the choice of characters.

From here, Hardy and Littlewood utilize known facts about L-functions and establish new facts about the Generalized Riemann Hypothesis to draw out the desired bound on $|f_2|$. This is relatively lengthy in the theory of the time, as the Generalized Riemann Hypothesis was still new (indeed, their papers never call it the generalized Riemann Hypothesis, and instead call it Hypothesis R^*). Modern methods would yield the same results with similar efficiency, and the details are thus ommited here.

Their work gives them the weak Goldbach problem, assuming the Generalized Riemann Hypothesis. However, the strong problem does not feel too far out of reach. As Hardy notes in [5], "Our method fails when $r = 2$. It does not fail in principle, for it leads to a definite result which appears to be correct; but we cannot overcome the difficulties of the proof". He follows this directly by the sentiment, "The best upper bound we can determine for the error is still too large by (roughly) a power $n^{\frac{1}{4}}$". They do obtain, however, a heuristic for what the asymptotic growth of the number of representations of an even number as the sum of two primes is:

Conjecture 2 (Hardy and Littlewood's Strong Goldbach Asymptotic)**.** *The number of ways to represent an even number n as the sum of two primes, $N_2(n)$, is of the form*

$$N_2(n) \sim 2C_2 \frac{n}{(\log(n))^2} \prod_{\substack{p|n \\ p \text{ prime}}} \left(\frac{p-1}{p-2}\right)$$

and

$$C_2 = \prod_{\omega=3}^{\infty} \left(1 - \frac{1}{((\omega-1)^2)}\right)$$

is a universal constant.

Indeed, after establishing this conjecture, the aproach changes in [6], in which Hardy and Littlewood leave the idea of utilizing the circle method to prove such a result for all numbers, and prove it for "almost all" numbers. The precise meaning of this is rather difficult, as no probability with desirable number theoretic meaning exists on $\mathbb{N}$ (this being that $\mathbb{P}(x \in N\mathbb{Z}) = \frac{1}{N}$) [25]. So instead, this is taken to be an asymptotic on the number of counterexamples. Specifically, they show that, if the number of counterexamples up to n is of the order $O(n^{\frac{1}{2}+\epsilon})$, where the constant is determined by ϵ, then one may extract stronger results, the proofs of which generalize to give us asymptotics on multiple known results, such as on specific cases of Waring's problem, or the number of ways n may be represented as the sum of two squares and a cube or two squares and a prime.

The key ideas for these proofs is nothing special, just to loosen the requirement for the growth of the major arcs by a factor of $n^{\frac{1}{4}+\epsilon}$, allowing the factor of $n^{\frac{1}{4}}$ in the growth of the minor arcs to no longer be an issue. This result holds for every $\epsilon > 0$, but larger values give smaller constants on the growth order, which can make checking remaining cases by hand easier.

2.3 Vinogradov's Improvements

The work of Vinogradov is primarily concerned with the error induced by truncating the sum in equation 2.1 into the sum in equation 1.2. Truncating this sum invariably induces an extra error into the problem, and historically this was avoided as it caused extra stress on the method, since bounding the minor arcs was already sufficiently difficult.

To this effect, the bulk of the work is done by freeing up extra room in the treatment of the minor arcs on the weak Goldbach problem, which helped prove the Goldbach problem in all but finitely many cases (these finitely many cases were still far too many to be checked even by computer, giving the need for a better proof which Helfgott provided some years later). Vinogradov considered the weighted sum

$$f(x) = \sum_{\substack{p \text{ prime} \\ p \leq n}} \log(p) e(px),$$

with $J(n)$ given as per usual (with f being raised to the third power) and proved the following bound:

Theorem 7 (Vinogradov's Bound)**.** *If (a, b). There exists sufficiently large B such that, for n sufficiently large, if the major arc at any given rational $\frac{p}{q}$ is given by*

$$\mathfrak{M}(p, q) = \left\{ x \,\middle|\, |x - p/q| \leq \frac{(\log(n))^B}{n} \right\}$$

then, for each $x \in \mathfrak{M}(p, q)$, we have that

$$f(x) \ll (\log(n))^4 (nq^{-1/2} + n^{4/5} + n^{1/2} q^{1/2}).$$

This allows the extraction of the following bound on the minor arcs:

Theorem 8. *Let A be a positive constant such that $B \leq 2A + 10$, with B as given in Theorem 7 and the major arcs given similarly. Then*

$$\int_{\mathfrak{m}} |f(x)|^3 \; dx \ll n^2 (\log(n))^{-A}.$$

Combined with non-trivial estimates on the major arcs, see [26] for exposition on the details, this is enough to extract the weak Goldbach problem for sufficiently large values of n. The details of this argument may be generalized to other problems. We focus on those items here, beginning with the fact that sometimes it is more suitable to estimate on Weyl sums, rather than just on the linear terms which one would get from the traditional circle method.

From here, the key becomes a string of computations, which relates Weyl sums to the solution of the systems:

$$\begin{aligned} x_1^1 + x_2^1 + \ldots + x_s^1 &= y_1^1 + y_2^1 + \ldots + y_s^1 \\ x_1^2 + x_2^2 + \ldots + x_s^2 &= y_1^2 + y_2^2 + \ldots + y_s^2 \\ &\vdots \\ x_1^k + x_2^k + \ldots + x_s^k &= y_1^k + y_2^k + \ldots + y_s^k. \end{aligned}$$

The computation in question gives the bound on

$$S = \sum_{k=1}^{N} e(f(k)) \tag{2.2}$$

where f is a polynomial with $\deg(f) = n+1$. Equations of the same form as Equation 2.2 are called Weyl sums, and are important in much of the surrounding theory.

In particular, if we denote $Y = \lfloor N^{1-n^2/4} \rfloor$ we have that for any integer $j \geq 1$,

$$SY - 2r_0Y^2 \leq \left(2^j Y^{2j-0.1} \int_0^1 \ldots \int_0^1 \left| \sum_{k=1}^{N} e(x_1k + x_2k^2 + \ldots x_{n+1}k^{n+1}) \right| \, dx_1 \ldots dx_{n+1} \right)^{\frac{1}{2j}}$$

where $|r_0| \leq 1$ is a fixed constant. This integral is bounded above by the number of solutions to the Vinogradov system from Vinogradov's Mean Value Theorem, Theorem 2. From here, directly applying that theorem to extract the desired result generally gives good asymptotics on the desired problem.

Chapter 3

Limitations with Primes

3.1 Prime Problems for the Circle Method

The first task at hand is to reframe problems dealing with primes in terms of the circle method. The most elementary way to do this is to begin by redefining the function found in equation 1.2 to sum across only prime terms. That is, one would like to consider the case where

$$f(\theta) = \sum_{\substack{p \text{ prime} \\ p \leq n}} e(p\theta).$$

However, when it comes to the actual analysis, this tends to cause issues as we do not know the general distribution of prime numbers beyond what the prime number theorem guarantees us. We could, perhaps, assume the Riemann Hypothesis for a greater degree of control.

Instead, one could solve weaker versions of the problems if we add a weight to each term. Traditionally, one may think of weighing this by the Chebyshev function

$$\vartheta(n) = \sum_{\substack{p \text{ prime} \\ p \leq n}} \log(p).$$

or even the Von Mangoldt function $\Lambda(n)$.

Other applications even weigh with the harmonic function, $\frac{1}{n}$. Each weight has its own benefits and downsides.

As the bounds on the Chebyshev function are approximately equivalent to bounds found in regards to the Riemann Hypothesis (see the proof of the Prime Number Theorem in [18], for instance), one generally prefers the Von Mangoldt function as a weight function. This does, however, have its own downsides.

The Von Mangoldt function yields results towards prime powers, and not directly towards primes. This means that one must usually trim the result afterwards to remove the prime powers. This can cause some odd results, as one has no guarantee that there are infinitely many primes satisfying a condition, and there could be infinitely many prime powers satisfying the desired condition instead.

As it stands, some further analysis on the possible weights we can assign is needed, to shed light on their costs and their benefits.

3.2 Error Terms from Arithmetic Weights

To understand better when one should and should not introduce the Von Mangoldt or Chebyshev functions as weights, it is best to get an idea of what kinds of error terms they induce. The traditional bound on the Chebyshev function is

$$|\vartheta(n) - n| = O(n^{1-\epsilon}),$$

for some $\epsilon > 0$. And this is equivalent to the Prime Number Theorem. Moreover, the strongest bound one can possibly expect is that for all $\epsilon > 0$,

$$|\vartheta(n) - n| = O\left(n^{\frac{1}{2}+\epsilon}\right).$$

which is a portion of an equivalent formulation of the Riemann Hypothesis, where the other requisite step for the Riemann Hypothesis is obtaining same bound on the Chebyshev ψ function, $\psi(n) = \sum_{k=2}^{n} \Lambda(k)$. These equivalences once again follow from the proof of the Prime Number Theorem found in [18].

Due to this, when one introduces a weight of $\vartheta(n)$ to the sum in equation 1.2, we induce an error term on both the major and minor arcs of degree $O(n^{1-\epsilon})$. So, if the bound between the major and minor arcs is loose enough that the addition of this error term does not interfere, it may be helpful to weigh the terms by the Chebyshev function.

On the other hand, if we would like to weigh by something like the Von Mangoldt function, we get the same error bounds as those traditionally used for logarithmic functions. So the results we obtain are not much better than weighing by $\log(n)$ without further, more detailed, arguments in the circle method itself. Indeed, this can be an occasional contributor to the abundance of error bounds containing the repeated composition of logarithms that is all too common in analytic number theory.

Another possibility is to weigh by the square-free indicator function given by $|\mu(n)|$, where $\mu(n)$ denotes the Möbius function

$$\mu(n) = \begin{cases} 0 & n \text{ is not square-free} \\ 1 & n \text{ is square-free with an even number of prime factors} \\ -1 & n \text{ is square-free with an odd number of prime factors} \end{cases}$$

Here, one strictly expects an error term of $O(1)$ from the function, as this is just an indicator function. However, the classical weight on the sum due to Laudau [13]

$$\sum_{k=1}^{n} \mu(k) = o(n)$$

may also be occasionally useful for heuristic arguments. This is infrequently used, as to leverage it appropriately often requires in-depth arguments, or a sum which is already of the form of a convolution (as this allows you to utilize the inversion formula). So, in general, its inclusion does not contribute much to simplifying the problem.

Indeed, to quote the classic text by Hardy and Wright in reference to sums involving these three functions, "Such functions as ... (these) are hard to handle."

The final, more classic, weight is the harmonic weight, $\frac{1}{n}$. This actually tends to be a well-behaved weight, and is often used to extend the integral in equation 1.3 to be across a larger period. There are two reasons one would do this. The first is because one may have better control of the Fourier coefficients at larger integer values, but there is a need to appeal to averaging arguments to get the desired result. The second is that, in this frame, one may send the period to infinity, in integer steps, and then use complex-analytic methods to resolve them with a reasonable error term.

3.3 Naive Twin Prime Conjecture

While not due to the circle method itself, a good place to start when attempting to understand the twin prime conjecture from an analytic standpoint is Brun's Theorem, which gives bounds on how twin primes may behave:

Theorem 9 (Brun's Theorem)**.** *The sum*

$$\sum_{\substack{p \text{ a twin} \\ \text{prime}}} \frac{1}{p}$$

converges.

The result is relatively recent as far as number theory goes, being from 1919 [1], and estimates for the constant that this converges to is constantly being improved. Indeed, as one knows that the sum of the reciprocals of the primes diverges, this gives a good good sense of how scarce twin primes are. It also ensures to us that any proof of the twin prime conjecture must be non-trivially different from that of the standard infinitude of primes.

Using this as a starting point, we note that of the ways we could set up our counting function $J(n)$, perhaps the most beneficial is to directly count the number of twin primes up to (and including) n. As such, we investigate the formulation of the twin prime conjecture with our counting function given by

$$f(x) = f_n(x) = \sum_{\substack{p \text{ prime} \\ p \leq n}} e(px), \tag{3.1}$$

and

$$J(n) = \int_0^1 f_n(x)\overline{f_n(\theta)}e(-2x)\ dx. \tag{3.2}$$

You will note that this formulation of the integral is different from what one traditionally expects, as the exponential term does not have an n term inside of it. However, this is because this counts the number of twin primes up to n, and not the number of ways n can be represented as the sum of twin primes. The analysis, in terms of the circle method, remains much the same as the control there depends solely on the dependence of the sum in f being controlled by n. Indeed, from some point of view this becomes even easier, as the above can be rewritten as

$$J(n) = \int_0^1 |f_n(x)|^2 e(-2x)\ dx,$$

and the control by the norm of f becomes clear.

From here, we note that the rational points on which we can estimate our arcs are exactly the points for which we have denominator less than $2 \cdot 3 \cdot \ldots \cdot p_k$, where p_k is the largest prime less than (or equal to) n. Note that $k = \pi(n)$, so we have asymptotic formulae, but we opt not to denote it this way for the time being for notational simplicity.

Now we can build our major arcs in the standard way, invoking Dirichlet's Approximation Theorem to note that for all $\alpha \in (0,1)$, there are $a, q \in \mathbb{N}$ such that, for a global constant P,

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

with $1 \leq q \leq P$ and $\gcd(a,q) = 1$. So, we take $P \geq 2p_1p_2 \ldots p_k$, as is normal, and allow our major arcs to be those centered at the points with square-free denominators.

To put it formulaically, we let our major arcs be:

$$\mathfrak{M} = \bigcup_{1 \leq q \leq p_1 \ldots p_k} \left(\frac{q}{p_1 \ldots p_k} - \frac{1}{P}, \frac{q}{p_1 \ldots p_k} + \frac{1}{P}\right)$$

with P as defined above. We take $\mathfrak{m} = (0,1) \backslash \mathfrak{M}$, as per usual. We omit the endpoints as they have no contribution to the integral, and we may thus freely choose to add them as a zero term in our decomposition.

As we know that this is not a profitable approach to solve the twin prime conjecture, we will start in the opposite order as normal. We show a reasonable error bound on the minor arcs, and follow it with a tighter bound on the major arcs. As this is the opposite of what one usually wants, we will be unable to get better, and thus unable to resolve the theorem via this method.

For the minor arcs, we apply the standard (yet inelegant) trick of "hit it with Parseval's until you get something nice". Here, this works especially well. Some initial bounding gives us that

$$\left|\int_{\mathfrak{m}} |f_n(x)|^2 e(-2x)\ dx\right| \leq \int_{\mathfrak{m}} |f_n(x)|^2 |e(-2x)|\ dx = \int_{\mathfrak{m}} |f_n(x)|^2\ dx$$

and we note that, as $\mathfrak{m}$ is contained in $[0,1]$ and the function $|f_n(x)|^2$ is non-negative,

$$\int_{\mathfrak{m}} |f_n(x)|^2\ dx \leq \int_0^1 |f_n(x)|^2\ dx = \sum_{k \in \mathbb{Z}} |\widehat{f_n}(k)|^2.$$

From here, Parseval's identity gives us the bound in terms of the sum of the Fourier coefficients of f. To apply Parseval's identity, we note that

$$\widehat{f_n}(k) = \begin{cases} 0 & k \leq n \text{ or } k \text{ not prime} \\ 1 & \text{otherwise} \end{cases}$$

So we get that

$$\left| \int_{\mathfrak{m}} |f_n(x)|^2 e(-2x)\ dx \right| \leq \sum_{k \in \mathbb{Z}} |\widehat{f_n}(k)|^2 = \pi(n).$$

From here, we apply the prime number theorem, noting that there exists some $\epsilon > 0$ such that

$$\left| \int_{\mathfrak{m}} |f_n(x)|^2 e(-2x)\ dx \right| \leq \pi(n) = \frac{n}{\log(n)} + O(x^{1-\epsilon}).$$

From here, we get our final estimate of

$$\left| \int_{\mathfrak{m}} |f_n(x)|^2 e(-2x)\ dx \right| \ll \frac{n}{\log(n)} \tag{3.3}$$

Heuristic arguments show that the best one should expect from the minor arcs is to be able to treat the induced error as being of the order $O\left(\frac{n}{\log(n)}\right)$ [21]. This is due to the effect of the uncertainty principle on the problem. So, our estimate here is actually as sharp as one can expect from the circle method (up to a constant).

With our minor arcs out of the way, For the major arcs, we can go one of two directions. We can either proceed through the traditional route, finding a lower bound on the integral across the major arcs and then commenting that it does not suffice, or we can proceed for a contradiction – showing that we instead have an upper bound on our major arcs which is not less than our bound on the minor arcs.

We proceed for a contradiction, as this is notably faster. Afterward, one may find a few remarks which assist in finding underestimates on the major arcs.

We begin by noting that, as our argument for the major arcs was entirely free from the choice of arcs, we have that our argument applies to the major arcs as well. That is,

$$\left|\int_{\mathfrak{M}} |f_n(x)|^2 e(-2x)\ dx \leq \pi(n)\right| = \frac{n}{\log(n)} + O(x^{1-\epsilon}) \ll \frac{n}{\log(n)} \tag{3.4}$$

for the exact same choice of ϵ as before.

Comparing equations 3.3 and 3.4, we get our desired contradiction, showing that with this particular analysis we cannot obtain a bound on the major arcs which is sharp enough to obtain the desired result with the given bound on the minor arcs. One may question if the a better choice of major arcs would allow us to extract a better bound on the minor arcs, but the distribution of primes makes this heuristically impossible. This gives us the distinct notion that under the current framework of the circle method, one cannot obtain a result as strong as the twin primes conjecture (at least with this formulation).

For those interested in finding an underestimate on the minor arcs, as is more traditional, begin by noting that as our entire integral is real-valued, we have that

$$J(n) = \int_0^1 |f_n(x)|^2 e(-2x)\ dx = \int_0^1 |f_n(x)|^2 \cos(-4\pi x)\ dx$$

so, leveraging the evenness of cos for simplification, we may perform our estimates on the function $|f_n(x)|^2 \cos(4\pi x)$. We may also redefine $f_n(x)$, omitting the prime 2, as it has no twin:

$$f_n(x) = \sum_{\substack{p \text{ prime} \\ 4 \leq p \leq n}} e(px),$$

We make this adjustment, as with it we have that $|f_n(x)|^2$ contains elements of the form $e((p_1 - p_2)x)$, where each $p_1 - p_2$ is even. As such, we have that $|f_n(x)|^2$ is $\frac{1}{2}$-periodic. So, splitting our major arcs as $\mathfrak{M}_+$ and $\mathfrak{M}_-$, with an interval $(q-P, q+p) \in$

$\mathfrak{M}$ being in $\mathfrak{M}_+$ if $(q - P, q + p)$ is a subset of $[0, \frac{1}{2})$ and categorizing it as being in $\mathfrak{M}_-$. In this setting, we have that

$$\int_{\mathfrak{M}} |f_n(x)|^2 \cos(4\pi x)\ dx = \int_{\mathfrak{M}_+} |f_n(x)|^2 \cos(4\pi x)\ dx + \int_{\mathfrak{M}_-} |f_n(x)|^2 \cos(4\pi x)\ dx.$$

Here, we may begin with polynomial estimates on $\cos(x)$, overestimating and underestimating as needed. Estimates on the distribution of the difference of primes yields the remaining portion of the problem, but this is beyond the scope of this thesis.

Indeed, heuristically the best one should expect from the minor arcs in this setting being of the order $O\left(\frac{n}{(\log(n))^2}\right)$, meaning that the major arcs do not grow sufficiently quickly for the matching heuristic bounds on the minor arcs [21]. These heuristics are often based in the uncertainty principle, and thus are almost certainly unavoidable when utilizing the circle method.

3.4 A Note on Kloosterman's Method

The astute (and those familiar with the circle method) will notice that most, if not all, applications of the circle method contain at least three terms in the Diophantine equation which is being solved. That is, the exponent of $f(\theta)$ in the formulation of $J(n)$ is at least three, and this allows for us to exploit bounds on $f(\theta)$ non-trivially. However, in the twin-primes problem, the formulation has exponent two, and so we cannot exploit bounds in the same way (notably, we have a similar issue in the strong Goldbach problem). As such, one traditionally moves to the method of Kloosterman, using so-called Kloosterman sums.

In general, Kloosterman sums can achieve much more with the circle method than just the traditional method alone. For instance, it can obtain asymptotics of sequences, obtain sharper asymptotics on solutions to Diophantine equations, and even recover historically known results. Indeed, the first result that proved the superiority of Kloosterman's method was utilizing the circle method to recover Legrange's four-squares theorem, which is the solution to Waring's problem in the case $k = 2$:

Theorem 10 (Legrange's Four-Squares Theorem). *For every natural number n, there are four other natural numbers a_1, a_2, a_3, and a_4 (which may possibly be zero) such that*

$$n = a_1^2 + a_2^2 + a_3^2 + a_4^2.$$

Indeed, with the historical circle method, even with the sharpest current bounds, obtaining this result is impossible. But, while utilizing Kloosterman's method, obtaining this result is not too bad.

The rough idea of Kloosterman's method is to investigate problems with two sets of variables:

$$x_1y_1 + x_2y_2 + \ldots + x_my_m = n.$$

This allows one to solve problems of one variable with only two variables by setting $x_1 = x_2 = 1$, and $x_i = 0$ for all other x_i (or similar)

Here, we begin by introducing not just a single sum in equation 1.2, but a double sum. In particular, for a suitable choice of helper function $f_S(x)$, defined as in equation 1.2, but with Diophantine variables taken from a set S, we may adjust the method. In particular, with our x_i variables living in the family S and y_i living in the family T, we can compute the counting function as

$$J(n) = \int_0^1 f_S(x)f_T(x)e^{-nx}\, dx.$$

This different form lends itself to problems in a method more like partitioning problems. As such, another major difference in Kloosterman's method comes from the selection of the major arcs. The philosophy behind the major and minor arc divide remains the same, but we no longer utilize Dirichlet's approximation theorem to select our major arcs. Instead, we utilize the numerical properties of Farey sequences to select Farey arcs centered around the desired points.

In some traditional Hardy-Littlewood problems with the circle method, similar techniques are incorporated, but this is only done in the context of partitioning problems, and not in the theory of Diophantine equations.

Chapter 4

Fixes with Higher Order Fourier Analysis

4.1 Introductory Higher Order Fourier Analysis

We begin with an outline of the Higher Order Fourier analysis needed for our purposes, which can be found primarily in the text by T. Tao [22]. To this end, it is important to note that the tools of higher order Fourier analysis are not truly intended for the circle method, but are instead tools of the theory of additive combinatorics, which may instead be applied to the circle method. They also rest too strongly on the theory of filtrations and ultrafilters for us to go into significant detail here, so instead we provide an overview of the specific theory in the case of counting solutions to Diophantine equations

Because of this, we initially diverge rather quickly from the classical version of the circle method. Our first decision is to opt to work directly over the torus $\mathbb{R}/\mathbb{Z}$ rather than over the interval $[0, 1]$. While similar in the formalities of the computations, this allows us to take a slightly different measure-theoretic view. Instead of directly fixing the Lebesgue measure to work in (which gives us the function space $L^2(T)$), we instead seek to fix a probability measure μ on the torus which is translation invariant.

While more probabilistic in nature, the harmonic analysis is saved by the fact that there is only one such measure on the torus – the Haar measure. This recovers the special case of the traditional circle method, where in one dimension we equate the torus with the half-open interval $[0, 1)$, where the Haar measure is the Lebesgue measure, and the theory is thus developed. Therefore, the formality of referring to our measure as the Haar measure is done primarily for the generalization to groups.

To develop our theory for groups, we consider the group acting on a finite group which will help us approximate the behavior on the torus in the limiting case. For us, this traditionally means taking our group to be $\mathbb{Z}/N\mathbb{Z}$, where we take a limit of our result when we formalize to $\mathbb{Z}$. Rather than constructing a function with Fourier coefficients equal to the number of solutions to our Diophantine equation, such as in equations 1.2 and 1.3, we instead construct a multilinear form which, when evaluated along specific functions, gives us similar information. For the sake of the measure theory, these functions that our multilinear form is usually evaluated on are traditionally indicator functions.

For instance, as presented in [23], one can consider the trilinear form

$$\Lambda_3^S(f, g, h) = \sum_{n \in S} \sum_{r=1}^{\infty} f(n)g(n+r)h(n+2r), \tag{4.1}$$

which, when evaluated across $S = \mathbb{Z}$ and $f = g = h = 1_A$, we get the number of three-term progressions in A.

The challenge becomes translating this into the group setting, so that we may leverage finite symmetries to simplify our work. To do so, we note that if we restrict ourselves to $S = \mathbb{Z}/N\mathbb{Z}$, and take our operation to be over the group, the number of possible r values that yield solutions also becomes restricted to elements in the group. So instead, we may consider the weighted version of our function over the group $\mathbb{Z}/N\mathbb{Z}$:

$$\Lambda_3(f,g,h) = \frac{1}{N}\sum_{n\in\mathbb{Z}/N\mathbb{Z}}\sum_{r\in\mathbb{Z}/N\mathbb{Z}} f(n)g(n+r)h(n+2r). \tag{4.2}$$

But, this is just the group-theoretic expected value:

$$\Lambda_3(f,g,h) = \mathbb{E}_{n,r\in\mathbb{Z}/N\mathbb{Z}} f(n)g(n+r)h(n+2r). \tag{4.3}$$

This translates well into the language of probability theory, and thus into our Haar measure. So, if we have a suitable notion of convergence with which to phrase our results, one should hope that taking the limit as N tends to infinity of a suitable result gives us the desired generalization of our result to $\mathbb{Z}$.

We define our norm on the space of functions, as this will give us a notion of convergence in the multilinear forms similar to weak convergence. So, letting G be a finite abelian group, we construct a norm on the class of functions $\{f | f : G \to \mathbb{C}\}$. The classical norm in our setting is not a single norm, but instead a family of norms called the Gowers norms. These norms have a variety of desirable properties which we will cover later.

We begin by defining the operator J by $Jf(x) = \overline{f(x)}$ to be the complex conjugation operator, and we denote J^n for the n-fold composition of the conjugate, with the zero fold composition just being the identity. From here, we can define the d-Gowers Norm by

$$||f||_{U^d(G)}^{2^d} = \sum_{x,h_1,\ldots,h_d\in G}\prod_{\omega_1,\ldots,\omega_d\in\{0,1\}} J^{\omega_1+\ldots+\omega_d} f(x+h_1\omega_1+\ldots+h_d\omega_d). \tag{4.4}$$

The most notable property of the Gowers norms is that they are countably indexed, which allows us to work with them quite nicely. It is also convenient that they are nested. That is, for a function f where the Gowers norm is defined, we have that

$$||f||_{U^1(G)} \leq ||f||_{U^2(G)} \leq ||f||_{U^3(G)} \leq \cdots.$$

This gives us the intuition that if we wish to control f, we should control it by the smallest Gowers norm possible which gives us the properties we are after. Assuming that such a norm is $||\cdot||_{U^d(g)}$, we call d the complexity of our function f. Of course, the properties which we are after vary widely from problem to problem, so there are many different definitions of complexity.

4.2 Complexity, Structure Theorems, and More

The exact notion of complexity is due to the existence of the so-called inverse theorems. Inverse theorems are theorems that inform us that a certain mode of convergence in the Gowers norm gives us a desired convergence in terms of our functions approximating their estimated values in $\mathbb{Z}/N\mathbb{Z}$ when N tends to infinity.

One common definition of complexity is that of Fourier Complexity. In this case, we consider a function f defined over $\mathbb{Z}/N\mathbb{Z}$. Formally, let $f : \{0, 1, 2, \ldots, N\} \to \mathbb{C}$. Then f has Fourier complexity M if M is the smallest natural number such that there exist numbers $c_1, \ldots, c_M \in \mathbb{C}$ and $a_1, \ldots, a_M \in \mathbb{Z}$ such that

$$f(n) = \sum_{k=1}^{M} c_k e(a_k n).$$

There is also the notion of Cauchy-Schwarz complexity, which describes the behavior of a collection of linear transformations on vector spaces of a group to the group itself. To put it in definite terms, if $L_1, L_2, \ldots, L_t : G^d \to G$ are affine-linear forms, then the system of transformations has Cauchy-Schwarz complexity s if s is the smallest number such that for every $1 \leq i \leq t$, one can partition

$\{1, 2, \dots, i-1, i+1, \dots, t\}$ into $s+1$ classes such that L_i does not lie in the affine-linear span over $\mathbb{Q}$ of the forms of any of these classes. If no such smallest number exists, we say that the system has infinite Cauchy-Schwarz complexity.

There are also other notions of complexity which are more general, but which we omit here due to their limited usages, such as the true complexity of works such as [10], the complexity nilmanifolds, and the complexity of tori [22]. In general, however, the complexity measures which Gowers norm we should bound our function with. If one has complexity d, for instance, one should seek to bound your function in the Gowers $d+1$ norm, $||\cdot||_{U^{d+1}(G)}$.

For any such theorem to be true, we need some notion of the equidistribution of our terms with respect to the measure. This allows us to rationalize that when N becomes sufficiently large, the distribution of the terms in the torus $\mathbb{R}/\mathbb{Z}$ is relatively uniform, and thus gives us the complete picture. A classic example of such a theorem is Weyl's equidistribution theorem:

Theorem 11 (Weyl Equidistribution)**.** *If $a \in \mathbb{R} \setminus \mathbb{Q}$, the representatives of the sequence*

$$\{a, 2a, 3a, \dots\}$$

modulo one are equidistributed in the unit interval $[0, 1]$.

We also need some notion of result which allows us to infer a portion of the asymptotic behavior on $\mathbb{R}$ from the behavior described by our function in $\mathbb{Z}/N\mathbb{Z}$. More specifically, we would like to know that if a function f has a non-negligible Gowers norm on the group, then there had to be some portion of the function on $\mathbb{R}$ which caused this behavior. As the goal is to invert our knowledge from the group setting to the continuous setting, such theorems are traditionally called inverse theorems. A classical example of an inverse theorem is the Gowers Inverse Theorem:

Theorem 12 (Gowers Inverse Theorem)**.** *Given an integer* $s \geq 0$*, and* $0 < \delta \leq 1$*. Then there exists a finite collection* $\mathcal{M}$ *of s-step manifolds (denoted* G/Γ*), each with a smooth Riemannian metric and constants* $C, c > 0$ *such that the following holds for any function* $f : \{1, 2, \ldots, N\} \to \mathbb{C}$ *for which we have that* $\delta \leq ||f||_{U^{s+1}(\mathbb{Z}/N\mathbb{Z})}$ *and* $|f(g)| \leq 1$*:*

There exists a nilmanifold $G/\Gamma \in \mathcal{M}$*, a constant* $g \in G$*, and a function* $F : G/\Gamma \to \mathbb{C}$ *for which* $|f(g)| \leq 1$*, such that* F *has Lipschitz constant at most* C *such that* $|\mathbb{E}_{n \in \mathbb{Z}/N\mathbb{Z}} f(n)\overline{F(g^n x)} > c$*.*

The exact language involved here (particularly that of nilmanifolds) and the related theory is not particularly difficult to define or develop, but doing so would distract from our purposes here. Interested readers are directed towards section 1.6 of the text by Tao on Higher Order Fourier Analysis [22]. However, intuitively, one may think of them as generalizing the behavior one expects of a torus.

The final key ingredient in such a problem is a structure theorem, which tells us how we may initially split our function effectively so that we may retain as much information as possible by passing to the group case. The most insightful statement of one is the informal structure theorem provided in [23]. This states that if one has a f function which is bounded by one, then one may split f as:

$$f = f_{str} + f_{unf}$$

where f_{unf} is Fourier-Uniform, a condition meaning roughly that f has small inner product with every Fourier term, and f_{str} being the structured portion. This structured portion is the linear combination of a bounded number of Fourier terms, and is bounded by one as well.

With these tools put together, we now have everything we need to provide a brief overview of how one generlizes the circle method utilizing higher order Fourier analysis.

4.3 Outline of the Circle Method with Higher Order Fourier Analysis

The notion, as per [23], is to reframe a problem from the classical circle method setting with its Fourier Transform into a problem in the setting of Higher Order Fourier Analysis.

As sketched previously in this chapter, this means phrasing the problem in terms of a multilinear form, such as in equation 4.2, and then deriving a corresponding expectation computation in the group setting, such as in equation 4.3.

First, one wishes to construct a multilinear form, with (roughly) one term in the form for every variable in our Diophantine equation. This form, when evaluated over the characteristic function for a set A, should count the number of solutions to the Diophantine equation with terms in A.

Settings in which one has a global relation between the constants, such as in the case of arithmetic progressions, give us the requisite linear form especially easily, such as in equation 4.1. This multilinear form should, traditionally, be the sum of an indicator function (indicating the success of the equation to hold at a particular value or collection of values) over a set (usually $\mathbb{Z}$ or $\mathbb{N}$).

The structure of the multilinear form being an indicator summed over $\mathbb{Z}$ or $\mathbb{N}$ allows us to sum it over a cyclic group $\mathbb{Z}/N\mathbb{Z}$ instead. From here, we may analyze the expected value in our group setting, normalizing by the size of our group. Later, one may expect to normalize by a potential growth rate function $f(N)$, in addition to the harmonic weight $\frac{1}{N}$ added to yield the expected value.

To put symbolically what we have put into words above, we establish a multilinear form $\Lambda_S(f_1, f_2, \ldots, f_k)$, for which $\Lambda_{\mathbb{Z}}(1_A, 1_A, \ldots, 1_A)$ yields the number of solutions to our Diophantine equation taken over $\mathbb{Z}$ with variables in A. We normalize to the group setting $\Lambda_N = \Lambda_{\mathbb{Z}/N\mathbb{Z}}$, and examine

$$\mathbb{E}\Lambda_N(f_1, f_2, \ldots, f_k).$$

In this group setting, the characteristic functions 1_A have smooth representations, and we can thus analyze their Fourier series. So, we view f_i as the appropriate characteristic functions, and denote them (by abuse of notation) as f, where the specific characteristic is clear from which index i is taken.

From here, we may begin analyzing f. We first seek to find a suitable Gowers norm to bound it non-trivially in, deriving the notion of the complexity of our problem. Once we have determined that a fixed norm, say, the Gowers $s+1$ norm suffices, one can apply a inverse theorem such as the Gowers $s+1$ inverse theorem (Theorem 12) to obtain a notion of what terms should be non-trivial.

From here, one builds a structure theorem, splitting f into a structured and uniform portion, where one may approximate with degree s Fourier phases (terms of the form $e(P(n)x)$, where $\deg(P) = s$), and this s is the same as in the choice of norm.

At this point, we perform some fairly standard analysis on the structured portion of f, utilizing the information provided by the inverse theorem to lift the information to be free of the order of the group. After this, we may obtain asymptotics on the expected value in the standard way, and limit to the infinite group case to extract the desired information.

This process gives the basis of many of the modern arguments found in the literature of higher order Fourier analysis which prove similar arguments to those of the circle method. Some of the most important recent results in analytic number theory stem from this, such as the recent work by Leng, Sah, and Sawhney in their improvement to Szemeredi's theorem from their recent preprint [14]:

Theorem 13 (Szemeredi)**.** *Let $r_k(N)$ denotes the size of the largest subset of $\{1, 2, \ldots, N\}$ such that there is no k-term arithmetic progression. For all $k \geq 5$, there exists $c_k > 0$ such that*

$$r_k(N) \ll Ne^{-(\log(\log(N)))^{c_k}}.$$

Chapter 5

Additional Limitations and Improvements

5.1 A Summary of Current Limitations

The primary limitation of interest is the inability to apply Kloosterman's method beneficially in certain two-variable Diophantine equations. For instance, the twin prime conjecture and the strong Goldbach problems resist attacks with the circle method.

A secondary limitation which, while of interest, stands primarily on conjecture and various open problems, is that of the parity problem, also called parity blindness. This refers, in general, to the inability of certain methods in number theory to see the difference between an entire set S, and the same set with certain elements removed according to certain divisibility rules.

This is a common issue in applications of sieve theory, where the issue is most accurately conjectured, as well as in most areas of multiplicative number theory. As such, the circle method itself also suffers from parity blindness to some degree. A good summary of the issue in sieve theory is the following (informal) conjecture from Terence Tao [20]:

Conjecture 3 (Tao). *Sieve theory alone cannot detect a difference in the size of a set S, and the subset of S whose elements are the product of an odd number of primes. Moreover, conjecturally any upper bounds differ from the sharpest possible bound by at least a factor of two.*

To formalize our notion, we let $\lambda : \mathbb{N} \to \{-1, 1\}$ denote the Louiville function, where

$$\lambda(p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}) = (-1)^{a_1+a_2+\dots+a_n}.$$

with the numbers p_i all being prime.

Parity blindness refers to the phenomenon of a method yielding the same results for a set S, as it does for the subsets

$$S_{\lambda^+} = \{s \in S | \lambda(s) = 1\}$$

and

$$S_{\lambda^-} = \{s \in S | \lambda(s) = -1\},$$

(with the value of each element reweighted accordingly, so there is no initial difference) no matter how stark the difference in the sets may be.

The circle method, as it rests primarily on the methods of multiplicative number theory to obtain the bounds on the major arcs, suffers from the same parity blindness that these methods do (see [24], for instance). To this effect, it is in our interest to survey the tools from multiplicative number theory which tend to crop up in the circle method, and analyze their parity blindness.

5.2 Recent Improvements to Asymptotics

One method which has been recently introduced and has led to improved asymptotics is the so-called method of efficient congruencing, and the related method of nested efficient congruencing, due to T. Wooley [28]. This has led to many of the current best bounds on theorems such as Vinogradov's Mean Value Theorem, which itself has led to improved bounds on many other theorems.

Efficient congruencing effectively utilizes the equivalence of asymptotic bounds to certain counting problems modulo prime numbers. For instance, when establishing a bound on Vinogradov's Mean Value Theorem, given that

$$f(x_1, x_2, \ldots, x_n, k) = \sum_{m=1}^{k} e(x_1 m + x_2 m^2 + \ldots x_n m^n)$$

and (with some sufficiently large $N = N(k)$ as the cutoff for the summation)

$$f_v(x_1, x_2, \ldots, x_n, \xi) = \sum_{\substack{m=1 \\ m \equiv \xi \pmod{p^v}}}^{N} e(x_1 m + x_2 m^2 + \ldots + x_m m^n)$$

to obtain a bound on the number of solutions less than X for some $m + s$ equations, one needs to bound the value of

$$\max_{1 \leq \xi \leq p} \int_0^1 \cdots \int_0^1 |(f(x_1, \ldots, x_n, X))^{2m} |f_1(x_1, \ldots, x_n, \xi))^{2s} dx_1 \ldots dx_k. \tag{5.1}$$

However, for certain well-behaved values, it suffices to compute congruence classes modulo prime powers, utilizing f_2, f_3, and so forth, rather than just f_1. In particular, we may utilize the j-th power if one has the equality

$$\sum_{i=1}^{k} (x_i - \eta)^j \equiv \sum_{i=1}^{k} (y_i - \eta)^j \pmod{p^j}$$

from the Vinogradov system (see Theorem 7), for the value of ξ which maximizes the selection in equation 5.1.

This method generalizes to other problems if one can find similar reductions, and has proven beneficial to finding the current best bounds in several different problems. There are other variants, such as the so-called nested efficient congruencing method, which yield even better results than just the method of efficient congruencing.

5.3 Recent Improvements to the Method

Of course, if one is speaking of recent improvements, the scope by which we mean must be defined. The improvements due to Vinogradov's method of truncating the sum in equation 1.2 cannot be understated [27]. However, we really mean more recent improvements than this.

To this effect, while not always applicable, Kloosterman's method is perhaps the most important item to mention here. However, more efficient methods of selecting the major arcs have also been recently implemented. Historically, such as in the sequence of papers by Hardy and Littlewood, up until the work of Vinogradov, one selected major arcs via Farey sequences and related properties. However, more recently selection of the major arcs via Dirichlet's approximation theorem has given more desirable results, as it can allow for a higher degree of precision when needed. This proves to be a key step in proofs such as that of the weak Goldbach problem, where extracting bounds is a struggle even with these sharper bounds.

Indeed, beyond this there are not many direct improvements to the circle method that have been developed, as most historical improvements have been in methods utilized to improve the asymptotic bounds, since those improvements also work new results into the scope of the method. Instead, it has been more of a trend to develop new tools which obtain the same information as the circle method.

To this end, one may view the entire field of additive combinatorics as an improvement to the circle method, although it is quite different in flavor. If one wishes to view only that in additive combinatorics which is closest to the circle method in philosophy, then the methods of higher order Fourier analysis, covered in Chapter 4, would be closest. However, the theory is still being actively developed, and many of the conjectural results in even the most recent texts have already been proven. As such, it is more of a developing field than an already developed field, so resources to learn it (other than picking up and reading research papers directly) are few and far between. New results flowing from higher order Fourier analysis are still forthcoming, and these results have even improved results from the circle method's asymptotics [14] – something which higher order Fourier analysis was thought to give weaker bounds on compared to the traditional circle method.

References

[1] Viggo Brun, *La serie 1/5 + 1/7 + 1/11 + 1/13 + 1/17 + 1/19 + 1/29 + 1/31 + 1/41 + 1/43 + 1/59 + 1/61 + ..., ou les denominateurs sont nombres premiers jumeaux est convergente ou finie*, Bulletin des Sciences Mathematiques (1919), no. 43, 100—104, 124—128.

[2] G. H. Hardy and J. E. Littlewood, *Some problems of 'partitio numerorum'; i: A new solution of waring's problem.*

[3] ———, *Some problems of "partitio numerorum": Ii. proof that every large number is the sum of at most 21 biquadrates*, Mathematische Zeitschrift **9** (1921), no. 1, 14–27.

[4] ———, *Some problems of 'partitio numerorum': Iv. the singular series in waring's problem and the value of the number g(k)*, Mathematische Zeitschrift **12** (1922), no. 1, 161–188.

[5] ———, *Some problems of 'partitio numerorum'; iii: On the expression of a number as a sum of primes*, Acta Mathematica **44** (1923), 1–70.

[6] ———, *Some problems of 'partitio numerorum'(v): A further contribution to the study of goldbach's problem*, Proceedings of the London Mathematical Society **s2-22** (1924), no. 1, 46–56.

[7] ———, *Some problems of 'partitio numerorum' (vi): Further researches in waring's problem*, Mathematische Zeitschrift **23** (1925), no. 1, 1–37.

[8] ———, *Some Problems of 'Partitio Numerorum' (VIII): The Number* $\Gamma(k)$ *in Waring's Problem*, Proceedings of the London Mathematical Society **s2-28** (1928), no. 1, 518–542.

[9] G.H. Hardy and Srinivasa Ramanujan, *Asymptotic formulae in combinatory analysis*, Journal of The London Mathematical Society-second Series **17**, 75–115.

[10] Hamed Hatami and Shachar Lovett, *Higher-order fourier analysis of and the complexity of systems of linear forms*, Geometric And Functional Analysis **21** (2011), no. 6, 1331–1357.

[11] H. A. Helfgott, *Minor arcs for goldbach's problem*, 2013, preprint on ArXiV.org at ArXiV:1205.5252.

[12] ———, *Major arcs for goldbach's problem*, 2014, preprint on ArXiV.org at ArXiV:1305.2897.

[13] Edmund von Landau, *Neuer beweis der gleichung* $\sum_{k=1}^{\infty} \frac{\mu(k)}{k} = 0$, Ph.D. thesis, Universität zu Berlin, 1899.

[14] James Leng, Ashwin Sah, and Mehtaab Sawhney, *Improved bounds for szemeredi's theorem*, 2024.

[15] Hugh L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, Reg. Conf. Ser. Math., vol. 84, Providence, RI: American Mathematical Society, 1994 (English).

[16] Ram Murty and Kaneenika Sinha, *An introduction to the circle method*, American Mathematical Society, 1981.

[17] R. A. Rankin, *The difference between consecutive prime numbers. ii*, Mathematical Proceedings of the Cambridge Philosophical Society **36** (1940), no. 3, 255–266.

[18] Elias M. Stein and Rami Shakarchi, *Complex analysis*, Princeton lectures in analysis, Princeton University Press, 2010.

[19] Elias M. Stein and Stephen Wainger, *Discrete analogues in harmonic analysis, i: ℓ^2 estimates for singular radon transforms*, American Journal of Mathematics **121** (1999), 1291 – 1336.

[20] Terence Tao, *Open question: The parity problem in sieve theory*, 2007, https://terrytao.wordpress.com/2007/06/05/open-question-the-parity-problem-in-sieve-theory/.

[21] ———, *Heuristic limitations of the circle method*, 2012, https://terrytao.wordpress.com/2012/05/20/heuristic-limitations-of-the-circle-method/.

[22] ———, *Higher order fourier analysis*, Graduate Studies in Mathematics, American Mathematical Society, 2012.

[23] ______, *The circle method from the perspective of higher order fourier analysis*, Plenary Talk, Hausdorff Center for Mathematics, https://terrytao.files.wordpress.com/2021/07/higher-order-fourier-analysis.pdf, Jul 2021.

[24] ______, *Correlations of multiplicative functions*, Colloqium Lecture, 2024 Joint Math Meetings Colloquium Lecture Series, https://terrytao.files.wordpress.com/2024/03/correlations-jan-5.pdf, Jan 2024.

[25] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Graduate Studies in Mathematics, American Mathematical Society, 2015.

[26] Robert C. Vaughan, *The hardy-littlewood method*, Cambridge University Press, 1981.

[27] Ivan M Vinogradov, *The method of trigonometric sums in number theory*, 1985.

[28] Trevor D. Wooley, *Vinogradov's mean value theorem via efficient congruencing*, Ann. of Math. (2) **175** (2012), no. 3, 1575–1627. MR 2912712