On the Number of Prime Solutions to a System of Quadratic Equations

by

Robert Fraser

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate Studies

(Mathematics)

THE UNIVERSITY OF BRITISH COLUMBIA

(Vancouver)

April 2013

© Robert Fraser 2013
Abstract

Consider the system of quadratic diophantine equations

\[ bX^2 - aY^2 = 0 \]
\[ bX \cdot Y - eY^2 = 0 \]

constrained to the prime numbers contained in the box \([0, N]^{2n}\). The Hardy-Littlewood circle method is applied to show that, under some local conditions on \(a, b,\) and \(e\), the number of prime solutions contained in the box is asymptotic to a constant times \(N^{2n-4} \frac{1}{(\log N)^2n}\), where the constant depends on \(a, b,\) and \(e\).
Preface

The strategy of applying the Hardy-Littlewood Circle Method to determine the number of prime solutions to a system of quadratic equations is well-known and not an invention of the author.

The strategy for the estimates appearing in Chapter 4 was devised by Akos Magyar. The proofs for Lemmas 4.3.1 and 4.3.2 were written by A. Magyar. Vaughan’s Identity is a well-known result in additive number theory due to R. C. Vaughan appearing in [7], and the exposition given in this paper is based on the exposition given by T. Gowers in [4].

The strategy for the mean value estimate in Chapter 5 was devised by A. Magyar. The singular series appearing in Chapter 5 is similar to the one given in J. Blair’s thesis [1].

The decomposition of the minor arcs given in Chapter 6 is standard, and is similar to the decomposition of the minor arcs given in chapter 8 of M. Nathanson’s book [6].

The techniques used to evaluate the singular series in Chapter 7 were suggested by A. Magyar. The convergence of the singular series is based on the convergence of the singular series in J. Blair’s thesis [1]. The proof that the singular series does not vanish is the original, unpublished work of the author.

The estimation of the singular integral in Chapter 8 appears in J. Blair’s thesis [1], and is included in this thesis for expository purposes only.

The strategies for the results in Appendix A and Appendix B were devised by Akos Magyar.
All other parts of the thesis are the original, unpublished work of the author.
# Table of Contents

Abstract ......................................................... ii
Preface ......................................................... iii
Table of Contents .............................................. v
Acknowledgements ............................................. vii

1 Introduction and Background Information .................. 1

2 Main Results .................................................. 3

3 Outline of the Proof .......................................... 5
  3.1 Preliminary Definitions ................................. 5
  3.2 Heuristics ................................................ 6

4 Uniform Bound for the Minor Arcs ......................... 8
  4.1 Bounds for Linear Exponential Sums .................... 8
  4.2 Vaughan’s Identity ...................................... 9
  4.3 Lemmas for Estimating the Bivariate Exponential Sums 12
  4.4 Bound for the Quadratic Exponential Sums ............ 15
  4.5 Dealing With More General Quadratic Polynomials .... 16
  4.6 Case Where $\beta$ is not Close to a Rational With Small Denominator ............................................ 17
  4.7 Case Where $\alpha$ is not Close to a Rational with Small Denominator ............................................ 18

5 Mean Value Estimate for the Minor Arcs ................... 20
  5.1 Decomposing the Integrand .............................. 20
  5.2 The Singular Series .................................... 22
  5.3 The Singular Integral .................................. 29

6 Decomposition of the Major Arcs .......................... 30
Acknowledgements

I would like to thank Akos Magyar and Mahta Khosravi for supervising my thesis. I thank Malabika Pramanik for agreeing to read my thesis. Thanks to Malcolm Rupert for help with formatting, and Pam Sargent, Dimitrios Karslidis, and Matthew Coles for helping me organize my thoughts. Thanks to my family for all of their moral support.
Chapter 1

Introduction and Background Information

In this paper, we obtain an asymptotic estimate for the number of prime solutions to the following system of Diophantine equations:

\[ bX^2 - aY^2 = 0 \]
\[ bX \cdot Y - eY^2 = 0 \]

where \( X \) and \( Y \) are \( n \)-dimensional vectors with components \( (x_1, \ldots, x_n) \) and \( (y_1, \ldots, y_n) \), respectively; the notation \( X^2 \) refers to the square of the Euclidean 2-norm of \( X \); that is, \( x_1^2 + \ldots + x_n^2 \); \( X \cdot Y \) is the Euclidean dot product of the vectors \( X \) and \( Y \), and \( a, b, \) and \( e \) are integers satisfying \( ab > e^2 \).

This problem has a geometric interpretation. A triangle is uniquely determined up to congruence by two of its side lengths and the angle between the sides. However, given the two side lengths, we can uniquely determine the angle between them if we are given the dot product of the vectors corresponding to the two sides we are given the length of. In other words, we can uniquely determine a triangle up to congruence by knowing the lengths of the vectors \( X \) and \( Y \) corresponding to two of the sides of the triangle, and the dot product \( X \cdot Y \) of these two vectors.

Fix a triangle \( T \) with a vertex at the origin, and let \( X_0 \) and \( Y_0 \) be vectors corresponding to the sides of the triangle that intersect at the origin. Let \( a = X_0^2, b = Y_0^2, \) and \( e = X_0 \cdot Y_0 \). Now, consider another triangle \( S \) with a vertex at the origin that is similar to the triangle \( T \), with the similarity set up so that \( \frac{||X_1||}{||X_0||} = \frac{||Y_1||}{||Y_0||} = k \) where \( X_1 \) and \( Y_1 \) are vectors that correspond to the sides of \( S \) that intersect at the origin. If the triangles \( S \) and \( T \) are similar, then we would need the angle between \( X_1 \) and \( Y_1 \) to be the same as the angle between \( X_0 \) and \( Y_0 \). But the cosine of the angle between \( X_1 \) and \( Y_1 \) is given by \( \frac{X_1 \cdot Y_1}{||X_1|| ||Y_1||} = \frac{k^2 X_0 \cdot Y_0}{||X_0|| ||Y_0||} \). It follows that for the angle to be the same, we need \( X_1 \cdot Y_1 = k^2 X_0 \cdot Y_0 \). Let \( a = ||X_0||^2, b = ||Y_0||^2, \) and
\( e = X \cdot Y \). Then \( ab > e^2 \) by the Cauchy-Schwarz inequality. Furthermore, we just showed that \( k^2 = \frac{X_1^2}{a} = \frac{Y_1^2}{b} = \frac{X_1 \cdot Y_1}{e} \) if \( S \) and \( T \) are similar. So an embedding of \( T \) corresponds to a solution to the system of equations

\[
\begin{align*}
    bX^2 - aY^2 &= 0 \\
    bX \cdot Y - eY^2 &= 0.
\end{align*}
\]

Conversely, if the ratio of the side length \( ||X_1|| \) to the length \( ||X_0|| \) is the same as the ratio of \( ||Y_1|| \) to \( ||Y_0|| \) and the angle between \( X_1 \) and \( Y_1 \) is the same as the angle between \( X_0 \) and \( Y_0 \), it follows from the law of cosines that the triangle determined by the vectors \( X_0 \) and \( Y_0 \) is similar to the triangle determined by the vectors \( X_1 \) and \( Y_1 \). Therefore, each solution to the system (1.1) corresponds to an embedding of \( T \).

Therefore, if we restrict ourselves to \( X \) and \( Y \) such that each coordinate of \( X \) and \( Y \) is a prime number, then a solution to the system (1.1) will correspond to an embedding of a triangle similar to \( T \) with prime coordinates.

A lot of work has been done on similar problems. For example, in [5], Hua discusses which numbers can be written as sums of squares of primes. This problem also has a geometric interpretation of embedding vectors of certain lengths into the grid formed by the prime numbers. Hua demonstrated that, for almost all \( n \) congruent to 3 mod 24 but not congruent to 0 mod 5, \( n \) can be written as the sum of three prime numbers.

More recently, James Blair has obtained an asymptotic for the number of solutions to the system of equations

\[
\begin{align*}
    bX^2 - aY^2 &= 0 \\
    bX \cdot Y - eY^2 &= 0
\end{align*}
\]

among the integers for dimensions \( n \geq 5 \). This result, along with its proof, will be referred to frequently throughout this paper. In particular, the calculation of the singular integral for this problem is exactly the same as in [1], and the minor arc mean value estimates in this paper follow from the asymptotic for the number of solutions to this problem among the integers.
Chapter 2

Main Results

Instead of counting the number of solutions to the system
\[ bX^2 - aY^2 = 0 \quad (2.1) \]
\[ bX \cdot Y - eY^2 = 0 \]
directly, we will first obtain an asymptotic for the number of integer solutions of (2.2) weighted by the Von Mangoldt function \( \Lambda \). More precisely, we will define
\[
R_N((a, b, e), \Lambda) := \sum_{bX^2 - aY^2 = 0} \sum_{bX \cdot Y - eY^2 = 0} \Lambda(X)\Lambda(Y)\chi_N(X)\chi_N(Y)
\]
where for \( X = (x_1, \ldots, x_n), Y = (y_1, \ldots, y_n) \):
\[
\Lambda(X) = \prod_{i=1}^{n} \Lambda(x_i)
\]
and
\[
\chi_N(X) = \prod_{i=1}^{n} \chi_N(x_i)
\]
where \( \chi_N \) is the indicator function of the interval \([1, N]\) and \( \Lambda \) is the Von Mangoldt function defined by
\[
\Lambda(x) = \begin{cases} 
\log p, & \text{if } x = p^r \\
0, & \text{otherwise}
\end{cases}
\]
In order for (2.2) to have solutions among the primes, we need to have solutions to (2.2) (mod \( p^r \)) for each prime \( p \) where each \( x \) and \( y \) coordinate is relatively prime to \( p \):
\[
bX^2 - aY^2 \equiv 0 \pmod{p^r}
\]
\[
bX \cdot Y - eY^2 \equiv 0 \pmod{p^r}.
\]
For small values of \( p \), this will impose restrictions on the values \( a, b, \) and \( e \). We will use the notation \( p \parallel a \) to denote the largest positive integer of the form \( p^r \) such that \( p^r \) divides \( a \).
Theorem 2.0.1. Let $a, b, e$ be nonnegative integers such that $ab > e^2$. Let $n \geq 7$ and $N > 1$ be fixed. Then we have that

$$R_N((a, b, e), \Lambda) = CN^{2n-4} + O(N^{2n-4}(\log N)^{-1})$$

for some constant $C > 0$, whenever the following conditions hold.

\begin{align*}
na &\equiv nb \pmod{24(2 \parallel (a, b))(3 \parallel (a, b))} \\
3 \parallel a &= 3 \parallel b \\
3 \parallel b &\leq 3 \parallel e \\
2 \parallel a &= 2 \parallel b = 2 \parallel e
\end{align*}

The constant $C$ in this theorem is the product of the singular series and singular integral, which are explained in chapters 8 through 10. The local conditions 2.3, 2.4, 2.5, and 2.6 are needed in order to show that the constant $C$ in Theorem 2.0.1 is positive.

We will use Theorem 2.0.1 in order to obtain an asymptotic for the number of prime solutions

$$R_n((a, b, e), P) := \#\{(X, Y) \in \mathbb{P}^{2n} : bX^2 - aY^2 = 0, bX \cdot Y - eY^2 = 0\}$$

Theorem 2.0.2. Let $a, b, e$ be nonnegative integers such that $ab > e^2$. Let $n \geq 7$ and $N > 1$ be fixed positive integers. Then we have

$$R_N(T, P) = \sigma N^{2n-4}(\log N)^{-2n} + O(N^{2n-4}(\log N)^{-2n-1})$$

with a constant $\sigma > 0$ as long as $a$, $b$, and $e$ satisfy the local conditions 2.3-2.6.
Chapter 3

Outline of the Proof

3.1 Preliminary Definitions

We start by writing the weighted number of solutions as an integral of an exponential sum:

\[
R_N((a, b, e), \Lambda) = \int_0^1 \int_0^1 \sum_{|X| \leq N} \sum_{|Y| \leq N} \Lambda(X) \Lambda(Y) \cdot e \left( \alpha(bX^2 - aY^2) + \beta(bX \cdot Y - eY^2) \right)
\]

(3.1)

and we notice that the integrand in (3.1) is the \(n\)th power of the exponential sum

\[
T_N(\alpha, \beta) := \sum_{x \leq N} \sum_{y \leq N} e(\alpha(bx^2 - ay^2) + \beta(bxy - ey^2))\Lambda(x)\Lambda(y)
\]

(3.2)

In order to estimate this integral, we split up the square \([0, 1] \times [0, 1]\) in the following way: The major arcs are the points in the square such that \(\alpha\) is within \(\frac{\log(N)^A}{Nq}\) of a rational number \(\frac{k}{q}\) and \(\beta\) is within \(\frac{\log(N)^A}{Nq}\) of a rational number \(\frac{\ell}{q}\) where \((k, \ell, q) = 1\), and \(q < (\log N)^A\). More precisely, Let \(A > 1\) and for a given triple \((k, \ell, q)\) of integers satisfying \(1 = (k, \ell, q) := \gcd(k, \ell, q)\), let

\[
M_{(k, \ell, q)} = \left\{ (\alpha, \beta) : \left| \frac{\alpha - k}{q} \right| \leq \frac{(\log N)^A}{qN^2}, \left| \frac{\beta - \ell}{q} \right| \leq \frac{(\log N)^A}{qN^2} \right\}
\]

and define the major arcs to be the union

\[
\mathcal{M}_A = \bigcup_{q \leq (\log N)^A} \bigcup_{(k, \ell, q) = 1} M_{(k, \ell, q)}
\]

(3.3)

We will define the minor arcs to be the complement of the major arcs:

\[
m_A = [0, 1]^2 \setminus \mathcal{M}_A
\]

(3.4)
3.2 Heuristics

Then most of the contribution to the integral will come from the major arcs. This is because there is very little cancellation on the major arcs. Heuristically, this is because if $\alpha = \frac{k}{q}$ and $\beta = \frac{\ell}{q}$, the sum $T(\alpha, \beta)$ is (ignoring the Von Mangoldt factors) periodic with period $q$, so the sum is comparable to $N^2$. We can get better estimates on the minor arcs. In particular, we will prove the following key estimates on the minor arcs:

**Proposition 3.2.1.** On the minor arcs $m_A$, we have the uniform estimate

$$|T_N(\alpha, \beta)| \leq N^2 (\log N)^{-c(A)}$$

where $c(A)$ is an increasing function of $A$ that can be made arbitrarily large by taking $A$ arbitrarily large.

This estimate can be used alongside a variant of the estimate proved in [1]:

**Proposition 3.2.2.** Let $n \geq 6$, $a \geq 1$ be fixed. Then we have

$$\int_{m_A} |T_N(\alpha, \beta)|^n \, d\alpha \, d\beta \leq N^{2n-4} (\log N)^{12}.$$

In particular, if we define $S_N$ to be the exponential sum

$$S_N(\alpha, \beta) := \sum_{x \leq N} \sum_{y \leq N} e(\alpha (bx^2 - ay^2) + \beta (bxy - ey^2)) \quad (3.5)$$

it is shown in [1] that the integral of the sum $S_N^n$ over all of $[0,1] \times [0,1]$ is asymptotic to a constant times $N^{2n-4}$. We trivially estimate the Von Mangoldt factors by $\log N$, and prove an upper bound of the same form for $|S_N^n|^n$.

We now obtain an asymptotic formula for the integral over the major arcs $M_A$. This asymptotic is obtained via a standard application of the Hardy-Littlewood circle method. We will follow the treatment in [6]. We show that

**Proposition 3.2.3.**

$$\int_{M_A} T(\alpha, \beta)^n = CN^{2n-4} + O(N^{2n-4}(\log N)^{-1}). \quad (3.6)$$
For estimating the major arcs, we decompose the sum (with an error term) into a product of a singular series, that decomposes into a product representation where each factor represents the asymptotic density of solutions to the system mod $p^k$ for every $p$, and a singular integral. The conditions on $a$, $b$, and $c$ in the statement of Theorem 2.0.1 are imposed in order to prevent the local factors from being equal to zero. The singular integral is shown to be positive and to contribute the correct power of $N$ to the asymptotic formula.
Chapter 4

Uniform Bound for the Minor Arcs

The goal for this section is to obtain a uniform bound for $|T(\alpha, \beta)|$, where $T(\alpha, \beta)$ is the sum

$$T(\alpha, \beta) = \sum_{x,y \leq N} e(\alpha(bx^2 - ay^2) + \beta(bxy - ey^2))\Lambda(x)\Lambda(y),$$

and $\Lambda$ is the Von Mangoldt function. The uniform bound will give us a gain of a power of $\log N$ on the minor arcs. In order to do this, we will (in the case where $\alpha$ is not close to a rational number) use a version of Vaughan’s identity to rewrite the sums in a more tractable form. In the case where $\beta$ is not close to a rational number, we will apply standard bounds on exponential sums with linear exponents.

4.1 Bounds for Linear Exponential Sums

First, we obtain standard bounds for exponential sums in which the exponent is linear. In order to obtain these bounds, we need the following lemma on the distribution of the fractional part $\{k\alpha\}$ of rational numbers $\alpha$ close to some rational number $\frac{a}{q}$:

**Lemma 4.1.1.** If $|\alpha - \frac{a}{q}| \leq \frac{b}{q^2}$, where $(a, q) = 1$, then for $k, k'$ such that $0 < k - k' < \frac{q}{2b}$, we have that $|\{k\alpha\} - \{k'\alpha\}| \geq \frac{1}{2q}$.

**Proof.** Write $\alpha = \frac{a}{q} + \beta$, where $|\beta| \leq \frac{b}{q}$. Then

$$|\{k\alpha\} - \{k'\alpha\}| = |(k - k')\alpha - \ell|$$

for some integer $\ell$. But this is at least

$$\left|\frac{(k - k')a}{q} - \ell\right| - |(k - k')\beta|.$$
\((k - k')\beta\) is at most \(\frac{1}{2q}\), and \(|(k - k')a - \ell|\) is a nonzero multiple of \(\frac{1}{q}\). We know it is nonzero, since \(\ell\) is an integer and \(|k - k'| < \frac{q}{2} < q\), so \((k - k')\) is not divisible by \(q\). \(\square\)

In particular, we use Lemma 4.1.1 to prove the following bound on linear exponential sums:

**Lemma 4.1.2.** Suppose that \(\beta\) is within \(\frac{b}{q^2}\) of some rational number \(\frac{\ell}{q}\) where \((\ell, q) = 1\). Then:

\[
\sum_{|z| \leq N} \left| \sum_{|x| \leq N} e(\beta xz) \right| \lesssim \left( N + \frac{N^2}{q} + q \right) \log q.
\]

**Proof.** We start with the sum:

\[
\sum_{|z| \leq N} \left| \sum_{|x| \leq N} e(\beta xz) \right| \leq \sum_{z \leq N} \min \left( N, \frac{1}{\|\beta z\|} \right)
\]

Where \(\|\beta z\|\) is the distance from \(\beta z\) to the nearest integer. Since the fractional parts of any \(\frac{b}{q}\) values \(\beta z\) are \(\frac{1}{2q}\)-separated by 4.1.1, we can split the sum in \(z\) up into at most \(\lesssim \max \left( 1, \frac{N}{q} \right)\) component sums, each of which has one term equal to \(N\), and the other terms at most equal to \(\frac{2q}{j}\), for \(j\) between 1 and \(\frac{2q}{b}\). So, in other words, there are \(\lesssim 1 + \frac{N}{q}\) sums, each of which is \(\lesssim N + q \log q\). Multiplying these together gives that that the whole sum is \(\lesssim (N + \frac{N^2}{q} + q) \log q\), as desired. \(\square\)

This linear exponential sum bound is significantly better than the trivial bound of \(N^2\) when \(q\) is “medium-sized”; that is, the bound is best when \(q\) is between \((\log N)^A\) and \(\frac{N}{(\log N)^A}\) for some \(A\).

### 4.2 Vaughan’s Identity

Vaughan’s identity is a useful tool for estimating sums containing Von Mangoldt factors. Vaughan’s identity was proven by Vaughan in [7]. In particular, Vaughan’s identity lets us rewrite a sum of terms containing Von
Mangoldt factors as a double sum of exponentials (with a small error term), which in practice is usually easier to estimate than the original sum containing the Von Mangoldt factors. We begin by considering the sum

$$\sum_{x \leq N} \Lambda(x)f(x).$$

For this section, $f$ should be a bounded function. In the sections following this one, we will $f(x) = e(x^2)$, and after this, we will apply this for a general quadratic polynomial $f(x) = e(ax^2 + bx + c)$ using the same principles as for the estimate for $x^2$.

We now follow the idea of the proof given in [4]: Because of the summatory property of the Möbius function, we have the following: If $\tau_u$ is the sum of the Möbius function among the divisors of $u$ that are at most $X$, we have

$$\sum_{u \leq N} \tau_u \sum_{X < x \leq N/u} \Lambda(x)f(xu) = \sum_{X < u \leq N/d} \mu(d) \sum_{X < x \leq N/u} \Lambda(x)f(x) + \sum_{X < x \leq N} \Lambda(x)f(x)$$

because the terms for $1 < u < X$ are equal to zero. Note further that

$$\sum_{1 \leq x \leq X} \Lambda(x)f(x) \lesssim X \sup_x |f(x)| \lesssim X,$$

by the prime number theorem. But we also have that

$$\sum_{u \leq N} \tau_u \sum_{X < x \leq N/u} \Lambda(x)f(xu)$$

$$= \sum_{d \leq X} \mu(d) \sum_{z \leq N/d} \Lambda(x)f(xdz)$$

So,

$$\sum_{x \leq N} \Lambda(x)f(x) = S_1 - S_2 - S_3 + O(X),$$
where

\[ S_1 = \sum_{d \leq X} \mu(d) \sum_{z \leq N/d} \sum_{x \leq N/dz} \Lambda(x) f(xdz) \]
\[ = \sum_{d \leq X} \mu(d) \sum_{z \leq N/d} \sum_{y \leq z} \Lambda(y) f(dz) \]
\[ = \sum_{d \leq X} \mu(d) \sum_{z \leq N/d} \log(z) f(dz) \]

\[ S_2 = \sum_{d \leq X} \mu(d) \sum_{z \leq N/d} \sum_{x \leq X} \Lambda(x) f(xdz) \]
\[ = \sum_{x \leq X} \Lambda(x) \sum_{d \leq N/x} \mu(d) \sum_{z \leq N/dx} f(xdz) \]
\[ = \sum_{y \leq X^2} \sum_{x \mid y, x \leq X} \Lambda(x) \mu\left(\frac{y}{x}\right) \sum_{z \leq N/y} f(yz) \]

But \( \sum_{x \mid y, x \leq X} \Lambda(x) \lesssim \log(y) \), so we get

\[ \sum_{y \leq X^2} \phi_1(y) \sum_{z \leq N/y} f(yz) \]

where \( \phi_1(y) \lesssim \log(y) \). and

\[ S_3 = \sum_{X \leq u \leq N} \sum_{d \mid u, d \leq X} \mu(d) \sum_{X < x \leq N/u} \Lambda(x) f(xu) \]

But

\[ \left| \sum_{d \mid u, d \leq X} \mu(d) \right| \leq \tau(u), \]

so this comes out to

\[ |S_3| \leq \sum_{X \leq u \leq N} \phi_2(u) \sum_{X < x \leq N/u} \Lambda(x) f(xu) \]

Where \( \phi_2(u) \lesssim \tau(u) \). But the sum is empty if \( N/u \leq X \), so we must have \( u < \frac{N}{X} \):

\[ \sum_{X \leq u \leq N/X} \phi_2(u) \sum_{X < x \leq N/u} \Lambda(x) f(xu) \]
4.3 Lemmas for Estimating the Bivariate Exponential Sums

The following lemma allows us to estimate a term that will arise when we evaluate the double sums given to us by Vaughan’s identity.

**Lemma 4.3.1.** Let $A$ be the set $\{h, |k| \leq N/Y, |\ell| \leq Y : ||hk\ell\alpha|| \leq 1/Y\}$. Then:

$$N^2 \sum_{|h| \leq N/m} \sum_{|k| \leq N/m} \min \left(Y, \frac{1}{||hk\ell\alpha||}\right) \lesssim N^2 Y (\log Y)|A|.$$ 

**Proof.** Fix $h$ and $k$, and use the linearity of the function mapping $\ell$ to $hk\ell\alpha$. Partition the interval $[-1/2, 1/2]$ into a disjoint union of intervals as $\bigcup_{-Y/2 \leq j \leq Y/2} \left[j \frac{j}{Y}, j \frac{j+1}{Y}\right)$. Let $B_j = \{|h|, |k| \leq N/Y, |\ell| \leq Y : ||hk\ell\alpha|| \in \left[j \frac{j}{Y}, j \frac{j+1}{Y}\right)\}$. Suppose that $\ell_1$ and $\ell_2$ are in the same $B_j$, and that $\ell_1$ and $\ell_2$ have the same sign. Then $|\ell_1 - \ell_2| \leq Y$ and $\ell_1 - \ell_2$ maps to the subinterval $(-1/Y, 1/Y)$. So for each point in $A_{h,k} = \{|\ell| \leq Y : ||hk\ell\alpha|| \leq 1/Y\}$ there are at most two $\ell$ in any given $B_j$. So

$$N^2 \sum_{|h| \leq N/m} \sum_{|k| \leq N/m} \min \left(Y, \frac{1}{||hk\ell\alpha||}\right) \leq N^2 \left(Y + \sum_{|h| \leq N/m} \sum_{|k| \leq N/m} \sum_{|j| \leq Y, j \neq 0} |B_j| \frac{Y}{j}\right)$$

$$\leq 2Y \log(Y) N^2 \left(\sum_{|h| \leq N/m} \sum_{|k| \leq N/m} |A_{h,k}|\right)$$

$$= 2Y \log(Y) N^2 |A|.$$ 

\[\square\]

Now, we will want to estimate the quantity $|A|$ appearing in lemma 4.3.1. The following lemma provides an estimate for the size of the set $A$.

**Lemma 4.3.2.** Let $N^{2/5} \leq M \leq N^{3/5}$, let $L = \frac{N}{M(\log N)^r}$, and let $K = \ldots$
Then
\[
\left\{ |h|, |k| \leq \frac{N}{ML}, |\ell| \leq \frac{M}{K} : ||hk\ell\alpha|| \leq \frac{1}{ML^2K} \right\} \gtrsim \frac{1}{L^2K} \left\{ |h|, |k| \leq \frac{N}{M}, |\ell| \leq M : ||hk\ell\alpha|| \leq \frac{1}{M} \right\}
\]

In order to prove this lemma, we will need the following result appearing in Davenport’s paper [3].

**Lemma 4.3.3.** Let $P$ be an origin-symmetric parallelogram with area at most 1. Then the parallelogram $P_A$ with side lengths equal to $\frac{1}{A}$ times the side lengths of $P$ will contain $\gtrsim \frac{1}{A}|P|$ lattice points, where $|P|$ is the number of lattice points in $P$.

We will use Lemma 4.3.3 to prove Lemma 4.3.2.

**Proof.** We use the Lemma 4.3.3 on each of the three variables $h, k, \text{ and } \ell$. We start by using the lemma on $h$. In particular, for a fixed $\ell$ and $k$, the number of $|h| \leq \frac{N}{ML}$ such that
\[
||hk\ell\alpha|| \leq \frac{1}{ML^2K}
\]
is $\gtrsim \frac{1}{L}$ times the number of $|h| \leq \frac{N}{M}$ such that
\[
||hk\ell\alpha|| \leq \frac{1}{MLK}.
\]
Note that this holds because $\frac{N}{ML^2K} \leq 1$ by the choices of $M, L, \text{ and } K$. Therefore,
\[
\left\{ |h|, |k| \leq \frac{N}{ML}, |\ell| \leq \frac{M}{K} : ||hk\ell\alpha|| \leq \frac{1}{ML^2K} \right\} \gtrsim \frac{1}{L} \left\{ |h| \leq \frac{N}{M}, |k| \leq \frac{N}{ML}, |\ell| \leq \frac{M}{K} : ||hk\ell\alpha|| \leq \frac{1}{MLK} \right\}.
\]

We then apply the same argument in the $k$ variable, noting that everything works this time because $\frac{N}{ML^2K} \leq 1$ by the choices of $M$ and $K$. Finally, we apply the same argument in the $\ell$ variable, which works because $\frac{1}{M}$ times $M$ is equal to 1. Therefore, we obtain the desired result. \qed
Finally, we need this bound on the sum of the square of the divisor function appearing in [4]

**Lemma 4.3.4.**

$$\sum_{x \leq n} d(x)^2 \leq 2n (\log n)^3.$$  

**Proof.**

$$\sum_{x \leq n} d(x)^2 = \sum_{x \leq n} \left( \sum_{b \mid x} 1 \right)^2$$

$$= \sum_{x \leq n} \sum_{b \mid x} \sum_{c \mid x} 1.$$  

If $b$ and $c$ divide $x$, then we can write $x$ as a multiple of lcm$(b, c)$

$$= \sum_{b \leq n} \sum_{c \leq n} \sum_{y \leq \text{gcd}(b, c) \leq n} 1$$

Now let $a = (b, c)$ be the greatest common divisor of $b$ and $c$. Write $d = \frac{b}{a}$ and $e = \frac{c}{a}$. Then the above sum is equal to

$$\sum_{a \leq n} \sum_{d \leq \frac{n}{a}} \sum_{e \leq \frac{n}{a}} \sum_{y \leq \frac{n}{ade}} 1$$

we can only increase the value of the sum by dropping the condition $(d, e) = 1$ in the sum in $e$. So we do so:

$$\leq \sum_{a \leq n} \sum_{d \leq \frac{n}{a}} \sum_{e \leq \frac{n}{a}} \sum_{y \leq \frac{n}{ade}} 1$$

Now, the innermost sum will be empty if $e > \frac{n}{ad}$, so this sum is equal to:

$$= \sum_{a \leq n} \sum_{d \leq \frac{n}{a}} \sum_{e \leq \frac{n}{ad}} \sum_{y \leq \frac{n}{ade}} 1$$

$$= \sum_{a \leq n} \sum_{d \leq \frac{n}{a}} \sum_{e \leq \frac{n}{ad}} \frac{n}{ade}$$

$$\leq \sum_{a \leq n} \sum_{d \leq \frac{n}{a}} \frac{n}{ade} (\log n + 1)$$

$$\leq \sum_{a \leq n} \frac{n}{a} (\log n + 1)^2$$

$$\leq n (\log n + 1)^3$$

$$\leq 2n (\log n)^3.$$
4.4 Bound for the Quadratic Exponential Sums

With the lemmas 4.3.1 and 4.3.2 in hand, we can now proceed to estimate the double sums that appear in Vaughan’s identity. We start with the third one, $S_3$. Split $S_3$ up dyadically. For some $Y$ between $N^{2/5}$ and $N^{3/5}$, we have:

$$T_j = \sum_{Y \leq m \leq 2Y} \phi_2(m) \sum_{N^{1/5} \leq n \leq Nm^{-1}} \Lambda(n)f(mn)$$

We apply the Cauchy-Schwarz inequality to the summation in $m$:

$$|T_j| \leq \left( \sum_{Y \leq m \leq 2Y} |\phi_2(m)|^2 \right)^{1/2} \left( \sum_{Y \leq m \leq 2Y} \sum_{N^{1/5} \leq n \leq Nm^{-1}} |\Lambda(n)f(mn)|^2 \right)^{1/2}$$

Squaring both sides, and using the bound given in 4.3.4 for the sum of the divisor function squared:

$$|T_j|^2 \lesssim (\log N)^3 Y \sum_{Y \leq m \leq 2Y} \sum_{N^{1/5} \leq n_1 \leq Nm^{-1}} \sum_{N^{1/5} \leq n_2 \leq Nm^{-1}} |\Lambda(n_1)/\Lambda(n_2)|e(\alpha m(n_1^2 - n_2^2))$$

$$\lesssim (\log N)^3 \sum_{Y \leq m \leq 2Y} \sum_{N^{1/5} \leq n_1 \leq Nm^{-1}} \sum_{|h| \leq Nm^{-1} - N^{1/5}} \Lambda(n_1)/\Lambda(n_1 + h)|e(\alpha m^2(-2hn_1 - h^2))|.$$ 

Now we interchange the order of summation, take an absolute value inside the outer two sums, relax the summation condition on the outer sums, and use the trivial bound $\Lambda(n) \leq \log(N)$:

$$\lesssim Y(\log N)^5 \sum_{n_1 \leq N/Y} \sum_{|h| \leq N/Y} \left| \sum_{Y \leq m \leq 2Y} e(\alpha m^2(-2hn_1 - h^2)) \right|$$

We then use Cauchy-Schwarz again:

$$|T_j|^4 \lesssim Y^2(\log N)^{10} \frac{N^2}{Y^2} \sum_{n_1 \leq N/Y} \sum_{h \leq N/Y} \sum_{\ell \leq Y} \min(Y, \frac{1}{|\alpha 2h(2n_1 + h)\ell|})$$
$S_1$ and $S_2$ are even simpler to handle. We then apply lemmas 1 and 2 to bound each $T_j$ by

$$|T_j|^4 \lesssim (\log N)N^2 Y \frac{N^2}{Y^2} Y (\log N)^{-3B}. $$

$$\cdot \left\{ |h|, |k|, |\ell| \leq (\log N)^B : ||hk\ell\alpha|| \leq \frac{(\log N)^{3B}}{N^2} \right\}$$

$$ \lesssim N^4 (\log N)^{-3B+1} \left\{ |h|, |k|, |\ell| \lesssim (\log N)^B : ||hk\ell\alpha|| \leq \frac{(\log N)^{3B}}{N^2} \right\}. $$

Then, if the only triples in the set are those for which $h$, $k$, or $\ell$ is equal to zero, then the quantity is

$$ \lesssim N^4 (\log N)^{-B+1} $$

If there is another solution, then taking $q = |hk\ell|$ gives a $q \leq (\log N)^{3B}$ with $||q\alpha|| \lesssim \frac{(\log N)^{3B}}{N^2}$. In other words, if $N$ is sufficiently large, then $\alpha$ must be in the major arc $M_{3B+\epsilon}$. Therefore, if $\alpha \not\in M_{A+\epsilon}$, then $|T_j| \lesssim N(\log N)^{-A+\frac{1}{12}+\frac{1}{4}}$.

We apply the same argument to each corresponding sum for $S_1$ and $S_2$, and use the fact that there are only $O(\log(N))$ sums present. So we gain a power of $\log(N)$ in each of the three sums given above, which shows that we gain a power of $\log(N)$ for the sum $\sum_{n=1}^{N} \Lambda(n)e(\alpha n^2)$.

### 4.5 Dealing With More General Quadratic Polynomials

Let’s suppose that we want to evaluate

$$\sum_{m \sim Y} \sum_{k \sim N/m} \xi_m \eta_k e(\alpha m^2 k^2 + \beta mk + \gamma),$$

where the sum in $m$ consists only of terms that are larger than $Y$, and the $\xi_m$ and $\eta_k$ are constants with absolute value 1. We use the Cauchy-Schwarz inequality like in the previous section (and modify the summation condition on the second sum since the quantity being summed is nonnegative):

$$|S|^2 \lesssim Y \sum_{|h| \leq N/Y} \sum_{k \leq N/Y} \left| \sum_{m \sim Y} e(bah(2k+h)m^2 + \beta m(h)) \right|$$

16
Then we have upon using Cauchy-Schwarz again:

\[ |S|^4 \lesssim \frac{Y^2 N^2}{Y^2} \sum_{|h| \leq N/Y} \sum_{k \leq N/Y} \sum_{|\ell| \leq Y} \sum_{s \leq Y} e(\alpha 2h(2k + h)2\ell(2s + \ell) + \beta \ell h) \]

We then change variables, letting \(2k + h\) be the new \(k\) and \(2s + \ell\) be the new \(s\):

\[ \sum_{|h| \leq N/Y} \sum_{k \leq N/Y} \sum_{|\ell| \leq Y} \sum_{s \leq Y} e(\alpha 4hks + \beta (\ell h)) \]

We now switch the order of summation around a bit and pull the absolute value signs inside the sum:

\[ \sum_{|h| \leq N/Y} \sum_{|\ell| \leq Y} \sum_{k \leq N/Y} \sum_{s \leq Y} e(\alpha 4hks + \beta (\ell h)) \leq \sum_{|h| \leq N/Y} \sum_{|\ell| \leq Y} \sum_{k \leq N/Y} \sum_{s \leq Y} e(\alpha 4hkl) \min \left( Y, \frac{1}{||\alpha 4hkl||} \right) \]

The rest of the argument proceeds almost exactly the same way as before, except for the fact that the extra constant necessitates enlarging the major arcs by a little bit. In particular, the bound from the previous section must be modified a little to state that if \( \alpha \notin \mathcal{M}_{A+\epsilon} \), then for sufficiently large \( N \) depending on \( \epsilon \), \( |T_j| \lesssim N \log N \frac{N^4}{N^4} + \frac{1}{4} \).

### 4.6 Case Where \( \beta \) is not Close to a Rational With Small Denominator

Define:

\[ T(\alpha, \beta) = \sum_{|x| \leq N} \sum_{|y| \leq N} e(\alpha (bx^2 - ay^2) + \beta (bxy - ey^2)) \Lambda(x) \Lambda(y) \]

and

\[ S(x, \alpha, \beta) = \sum_{|y| \leq N} e(\alpha (bx^2 - ay^2) + \beta (bxy - ey^2)) \Lambda(y) \]

Then

\[ T(\alpha, \beta) = \sum_{|x| \leq N} S(x, \alpha, \beta) \Lambda(x). \]
We now apply the Cauchy-Schwarz inequality:

\[ |T(\alpha, \beta)|^2 \leq \sum_{|x| \leq N} |\Lambda(x)|^2 \sum_{|x| \leq p} |S(x, \alpha, \beta)|^2 \]

Then, applying PNT to one instance of the Von Mangoldt function and the uniform bound to the other one:

\[ \lesssim N \log(N) \sum_{|x| \leq N} \sum_{|y| \leq N} \Lambda(y)\Lambda(y')e(b\beta x(y - y') + (-\alpha a - \beta e)(y^2 - y'^2)) \]

\[ \lesssim N(\log N)^3 \sum_{|y| \leq N} \left| \sum_{|x| \leq N} e(b\beta x(y - y')) \right| \]

Now, let \( z = y - y' \), and notice that a given \( z \) occurs at most \( 2N \) times in the sum:

\[ \lesssim N^2(\log N)^3 \sum_{|z| \leq N} \left| \sum_{|x| \leq N} e(b\beta xz) \right| \]

The Dirichlet principle implies that for any \( \beta \) irrational, there exists a \( q < \frac{N^2}{(\log N)^4} \) such that \( |q\alpha| < \frac{\log N^4}{N^2} \). Now, because \( \beta \) is in a minor arc, we know that this \( q \) must also be larger than \( (\log N)^4 \). So that means that \( b\beta \) is within \( \frac{b(\log N)^4}{qN^2} \leq \frac{1}{q} \) of a rational number of the form \( \frac{r}{b} \), where \( r \) is some number between \( \frac{q}{b} \) and \( q \), where \( (\log N)^4 < r \leq \frac{N^2}{(\log N)^4} \). This, together with Lemma 4.1.1, implies that the above sum is bounded above by

\[ \lesssim N^2(\log N)^3(N + N^2/|q| + |q|)(\log q) \]

\[ \lesssim N^4(\log N)^3(\log \log N). \]

4.7 Case Where \( \alpha \) is not Close to a Rational with Small Denominator

\[ |T(\alpha, \beta)| = \left| \sum_{x \leq N} \sum_{y \leq N} e(\alpha(bx^2 - ay^2) + \beta(bxy - ey^2))\Lambda(x)\Lambda(y) \right| \]
We then interchange the order of summation:

\[
\begin{align*}
&\leq \sum_{y \leq N} \left| e(-\alpha ay^2 - \beta ey^2)\Lambda(y) \sum_{x \leq N} e(\alpha bx^2 + \beta bxy)\Lambda(x) \right| \\
&\leq \log N \sum_{y \leq N} \left| \sum_{x \leq N} e(\alpha bx^2 + \beta bxy)\Lambda(x) \right|
\end{align*}
\]

We then apply the version of Vaughan’s identity given here along with the exponential sum estimates:

\[
\lesssim \log N \sum_{y \leq N} N(\log N)^{-C(A)}
\]

where \( C(A) \) is some unbounded, increasing function of \( A \). So the sum comes out to

\[
\lesssim N^2(\log N)^{-C(A)+1}
\]

So, we conclude that for any \((\alpha, \beta)\) in the minor arcs, we have that

**Proposition 4.7.1.** *On the minor arcs \( m_A \), we have the uniform estimate*

\[
|T_N(\alpha, \beta)| \leq N^2(\log N)^{-c(A)}
\]

*where \( c(A) \) is an increasing function of \( A \) that can be made arbitrarily large by taking \( A \) arbitrarily large.*
Chapter 5

Mean Value Estimate for the Minor Arcs

5.1 Decomposing the Integrand

We want to estimate the integral:

$$\left\| \int_{m_A} T(\alpha, \beta)^7 \right\|$$

where

$$T(\alpha, \beta) = \sum_{|x|,|y|\leq N} e(\alpha(bx^2 - ay^2) + \beta(bxy - ey^2))\Lambda(x)\Lambda(y).$$

and \(\Lambda(X)\) is the Von Mangoldt function. We split the integral up in the typical way:

$$\leq \log(N)^{12} \sup_{m_A} |T(\alpha, \beta)| \int_{[0,1]^2} |S(\alpha, \beta)|^6,$$

where

$$S(\alpha, \beta) = \sum_{|x|,|y|\leq N} e(\alpha(bx^2 - ay^2) + \beta(bxy - ey^2)).$$

We estimate the supremum using the uniform bound. In order to estimate the integral, we split up \([0,1]^2\) into major arcs of the same size as in \([1]\), and the corresponding minor arcs. The minor arc estimate works exactly the same way as in \([1]\), and we gain a small power of \(N\) in the process. The major arc estimate is slightly different because of the presence of the absolute value signs.

We start by attempting to factor the integrand into a product of a singular series and a singular integral, as usual. We begin by expanding the product in the absolute value, and writing \(\alpha = \frac{k}{q} + \gamma, \beta = \frac{\ell}{q} + \delta\) with \(\gamma\) and \(\delta\) smaller than \(N\): 

$$|S(\alpha, \beta)|^6 = S(\alpha, \beta)^3 \overline{S(\alpha, \beta)^3}$$

20
\[
\sum_{X,Y,S,T \in \mathbb{Z}} e \left( \frac{k}{q} X + \gamma (qX + S, qY + T) + \left( \frac{\ell}{q} + \delta \right) g(qX + S, qY + T) \right) \\
\cdot \chi \left( \frac{qX + S}{N} \right) \chi \left( \frac{qY + T}{N} \right) 
\]

where

\[
f(X, Y) = b(x_1^2 + x_2^2 + x_3^2 - x_4^2 - x_5^2 - x_6^2) - a(y_1^2 + y_2^2 + y_3^2 - y_4^2 - y_5^2 - y_6^2)
\]

and

\[
g(X, Y) = b(x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6) - e(y_1^2 + y_2^2 + y_3^2 - y_4^2 - y_5^2 - y_6^2).
\]

Note that the changing \(X\) and \(Y\) shifts the parts of the exponent depending on \(k/q\) and \(\ell/q\) by a full period, so we can pull the parts depending on \(\gamma\) and \(\delta\) out of the sum in \(X\) and \(Y\). This gives

\[
\sum_{S,T \pmod{q}} e(h(S, T)) G(S, T)
\]

where

\[
h(S, T) = \frac{kb(s_1^2 + s_2^2 + s_3^2 - s_4^2 - s_5^2 - s_6^2)}{q} \\
+ \frac{\ell b(s_1t_1 + s_2t_2 + s_3t_3 - s_4t_4 - s_5t_5 - s_6t_6)}{q} \\
- \frac{(ka + \ell e)(t_1^2 + t_2^2 + t_3^2 - t_4^2 - t_5^2 - t_6^2)}{q}
\]

and

\[
G(S, T) = \sum_{X,Y} e(\delta f(qX + S, qY + T) + \gamma g(qX + S, qY + T)) \\
\cdot \chi \left( \frac{qX + S}{N} \right) \chi \left( \frac{qY + T}{N} \right)
\]

We then make the change from \(G(S, T)\) into the singular integral as in [1].
5.2 The Singular Series

The singular series is treated in a manner similar to [1]. We want to estimate the quantity

\[ \sum_{\gcd(k,\ell,q)=1} K_6(K,\ell,q) \]

where

\[ K_6(k,\ell,q) = \frac{1}{q^{12r}} \sum_{S,T(\mod q)} e(h(S,T)). \]

Note that \( K_6(k,\ell,q) = |K(k,\ell,q)|^6 \), where

\[ K(k,\ell,q) = \sum_{s,t(\mod q)} e(kbs^2 + \ellbst - (ka + \ell c)t^2) \]

I will start by looking at \( K_6(k,\ell,p^r) \) for prime powers \( p^r \).

\[ K_6(k,\ell,p^r) = \frac{1}{p^{12r}} \sum_{S,T(\mod p^r)} e(h(S,T)). \]

Then

\[ K_6(k,\ell,p^r) = \frac{1}{p^{12r}} \sum_{S,T(\mod p^r)} e \left( \frac{k}{p^r} (bf(S,S) - af(T,T) + 2) \right) \cdot e \left( \frac{\ell}{p^r} (bf(S,T) - ef(T,T)) \right) \]

where \( f(X,Y) = x_1y_1 + x_2y_2 + x_3y_3 - x_4y_4 - x_5y_5 - x_6y_6 \). Define \( S_1 = (s_1, s_2, s_3) \) and \( S_2 = (s_4, s_5, s_6) \) where \( S = (s_1, s_2, s_3, s_4, s_5, s_6) \), and similarly set \( T_1 = (t_1, t_2, t_3) \) and \( T_2 = (t_4, t_5, t_6) \) where \( T = (t_1, t_2, t_3, t_4, t_5, t_6) \). Then:

\[ K_6(k,\ell,p^r) = \frac{1}{p^{12r}} \sum_{S_1,T_1,S_2,T_2(\mod p^r)} e \left( \frac{k}{p^r} (b(S_1^2 - S_2^2) - a(T_1^2 - T_2^2)) \right) \cdot e \left( \frac{\ell}{p^r} (b(S_1 \cdot T_1 - S_2 \cdot T_2) - e(T_1^2 - T_2^2)) \right) \]
Now reindex the sums, taking \( S_1 = S_2 + U, \quad T_1 = T_2 + U \). This has the advantage of linearizing the \( S_2 \) and \( T_2 \) terms appearing in the sum.

\[
\sum_{U,V,S_2,T_2 \mod p^{2r}} e\left( \frac{k}{p^r} (b(U^2 + 2U \cdot S_2) - a(V^2 + 2V \cdot T_2)) \right) \\
\cdot e\left( \frac{\ell}{p^r} (b(U \cdot T_2 + V \cdot S_2 + U \cdot V) - (V^2 + 2V \cdot T_2)) \right)
\]

We now take out the parts of the sum that don’t depend on \( U \) and \( V \) and apply the triangle inequality:

\[
\leq \frac{1}{p^{12r}} \sum_{U,V \mod p^{2r}} \left| \sum_{S_2,T_2 \mod p^{2r}} e\left( \frac{k}{p^r} (2bU \cdot S_2 - 2aV \cdot T_2)) \right) \\
\cdot e\left( \frac{\ell}{p^r} (bU \cdot T_2 + bV \cdot S_2 - 2eV \cdot T_2) \right) \right|
\]

Note that the sum in \( S_2 \) and \( T_2 \) is over a complete residue system mod \( p^{2r} \) in each variable, so the sum is zero when any of the coefficients of \( S_2 \) or \( T_2 \) is nonzero. That is, the sum in \( S_2 \) and \( T_2 \) will only be nonzero when

\[
2bkU + b\ell V \equiv 0 \pmod{p^{2r}}
\]

and

\[
-2akV + b\ell U - 2e\ell V \equiv 0 \pmod{p^{2r}},
\]

in which case the sum will be \( p^{6r} \) since there are \( 6r \) terms in the inner sum in \( S_2 \) and \( T_2 \), all of which are equal to one.

We will first deal with the case where \( p \) is an odd prime. Let \( p^\gamma = (b,p^r) \), and let \( b = b'/p^\gamma \). Then the first equation becomes:

\[
2kb'U + b'\ell V \equiv 0 \pmod{p^{r-\gamma}},
\]

or, after dividing by \( b' \),

\[
2kU + \ell V \equiv 0 \pmod{p^{r-\gamma}},
\]

Now, one of \( k \) and \( \ell \) must be relatively prime to \( p^\gamma \) because we’re only looking at cases where \( (k,\ell,p^r) = 1 \). assume \( (k,p) = 1 \). Then \( k \) is invertible mod \( p \) and

\[
U \equiv -(2k)^{-1}\ell V. \pmod{p^{r-\gamma}}
\]
So plugging into the second equation gives

\[ (-2ka - 2\ell e)V - (\ell^2 b(2k)^{-1})(V + Cp^{r-\gamma}) \equiv 0 \pmod{p^r} \]
\[ (-2ka - \ell^2 b(2k)^{-1} - 2\ell e)V \equiv 0 \pmod{p^r} \]
\[ (-4k^2 a - \ell^2 b - 4k\ell e)V \equiv 0 \pmod{p^r}. \]

A quick calculation shows that we achieve the same result (with \( U \) instead of \( V \)) we instead assume that \( \ell \) is not divisible by \( p \). This equation has \( p^{3\gamma} \) solutions, where \( p^{\delta} = (p^r, -4k^2 a + \ell^2 b - 4k\ell e) \). Putting this together with the \( p^{3\gamma} \) solutions to the first equation, we have a total of \((-4k^2 ab + \ell^2 b^2 - 4k\ell be, p^r)^3 \) solutions to the system. Multiplying this by the \( p^{6r} \) choices for \( S_2 \) and \( T_2 \), we have that the sum is at most

\[ \frac{1}{p^{6r}}(-4k^2 ab - \ell^2 b^2 - 4k\ell be, p^r)^3. \]

Now we consider numbers of the form \( 2^r \). Again, we’re trying to count the number of solutions to the system

\[ 2bkU + b\ell V \equiv 0 \pmod{2^r} \]
\[ -2akV + b\ell U - 2e\ell V \equiv 0 \pmod{2^r}. \]

Now, we write \( b = 2^\gamma b' \), where \( 2^\gamma = (2^r, b) \).

\[ 2b'kU + b'\ell V \equiv 0 \pmod{2^r-\gamma} \]
\[ 2kU + \ell V \equiv 0 \pmod{2^r-\gamma} \]

if \( r > \gamma \). Then if \( \ell \) is odd, the second equation reduces to

\[ 4ak^2 U + b\ell^2 U + 4e\ell U \equiv 0 \pmod{2^{r-\gamma}}, \]

as in the case where \( p \) is an odd prime. But if \( \ell \) is even, then \( k \) must be odd since \((k, l, 2^r) = 1\), so therefore \( k \) is invertible mod \( 2^r \), so we can divide the equation by 2:

\[ b'kU + b'\frac{\ell}{2} V \equiv 0 \pmod{2^{r-\gamma-1}}. \]

Then, the second equation reduces to the same thing as in the odd case. So the sum is bounded above by

\[ \frac{2}{2^{6r}}(2^r, -4k^2 ab - \ell^2 b^2 - 4k\ell be)^3. \]
We then wish to calculate $|\{(k, \ell) : (k, \ell, p) = 1 \text{ and } (p^r, 4k^2ab + \ell^2b^2 + 4k\ell be) = p^s\}|$ for prime powers $p^r$ and $0 \leq s \leq r$. We start by assuming $p$ is an odd prime. Since $(k, \ell, p) = 1$, either $(k, p)$ or $(\ell, p)$ is equal to 1. Assume first that $(\ell, p) = 1$. Then we complete the square in $k$:

\[
4k^2ab + 4k\ell be + \ell^2b^2 \equiv 0 \pmod{p^s}
\]
\[
4k^2a^2b^2 + 4k\ell ab^2e + \ell^2a^2b^4 \equiv 0 \pmod{p^s}
\]
\[
(2abk + 2b\ell e)^2 - 4e^2b^2\ell^2 + a^3\ell^2b^3 \equiv 0 \pmod{p^s}
\]
\[
(2abk + 2b\ell e)^2 \equiv (4e^2b^2 - ab^3)\ell^2 \pmod{p^s}
\]

Now, the right hand side is divisible by $p^\alpha$ where $p^\alpha$ is the largest power of $p$ that divides $(4e^2b^2 - ab^3)$; furthermore, the right hand side is not divisible by $p^{\alpha+1}$ because we assumed that $\ell$ is not divisible by $p$. So there are at most $2p^\alpha$ values of $\ell$ that can square to give the right hand side (as we can see by dividing the right hand side by $p^\alpha$). Note further that for a given $\ell$, the expression $2abk + 2b\ell e$ hits each residue class $(\mod p^s)$ at most $(ab, p^s) \leq ab$ times as $k$ is chosen $(\mod p^s)$. So therefore there are at most $2abp^\alpha \lesssim 1$ solutions for any given $\ell$. The same argument works up to a constant factor if $p = 2$, and a similar argument works if $(k, p) = 1$ instead.

So, there are at most $2abp^\alpha \lesssim 1$ solutions for any given $\ell$. The same argument works up to a constant factor if $p = 2$, and a similar argument works if $(k, p) = 1$ instead.

Putting these facts together, we get

\[
K_6(p^r) \leq 2 \sum_{k, \ell \mod{p^r}} p^{6r} \sum_{s} p^{3s}|\{(k, \ell) : p^s = (p^r, 4k^2ab + \ell^2b^2 + 4k\ell be)\}|
\]
\[
\lesssim p^{-6r} \sum_{0 \leq s \leq r} p^{3s} p^{2r} p^{-s}p^{-s}
\]
\[
= p^{-4r} \sum_{0 \leq s \leq r} p^{2s} p^{-s}
\]
\[
\lesssim p^{-4r} p^{2r} p^{-2r} = p^{-2r}.
\]

Therefore, if we can prove that $K_6$ is multiplicative, then we will have shown that for any $q$ we have

\[
K_6(q) \leq C^{\omega q}q^{-2}.
\]
In order to show that $K_6$ is multiplicative, I first will show the following multiplicative property:

$$K_6(k_1, \ell_1, q_1)K_6(k_2, \ell_2, q_2) = K_6(k_1q_2 + k_2q_1, \ell_1q_2 + \ell_2q_1, q_1q_2)$$

whenever $(q_1, q_2) = 1$.

**Proof.** Note that it suffices to prove that $K$ has the multiplicative property.

$$K(k_1q_2 + k_2q_1, \ell_1q_2 + \ell_2q_1, q)$$

$$= \sum_{x \pmod{q}} \sum_{y \pmod{q}} e\left(\frac{k_1q_2 + k_2q_1}{q}(bx^2 - ay^2) + \frac{\ell_1q_2 + \ell_2q_1}{q}(bxy - ey^2)\right)$$

We apply the Chinese remainder theorem:

$$= \sum_{x_1 \pmod{q_1}} \sum_{x_2 \pmod{q_2}} \sum_{y_1 \pmod{q_1}} \sum_{y_2 \pmod{q_2}} e\left(\frac{k_1q_2 + k_2q_1}{q}(bx_1q_2 + x_2q_1)^2 - a(y_1q_2 + y_2q_1)^2\right)$$

$$\cdot e\left(\frac{\ell_1q_2 + \ell_2q_1}{q}(bx_1q_2 + x_2q_1)(y_1q_2 + y_2q_1) - e(y_1q_2 + y_2q_1)^2\right)$$

Then, noting that the cross terms all cancel out in the expansion:

$$= \sum_{x_1 \pmod{q_1}} \sum_{x_2 \pmod{q_2}} \sum_{y_1 \pmod{q_1}} \sum_{y_2 \pmod{q_2}} e\left(\frac{k_1q_2 + k_2q_1}{q}(bx_1^2q_2^2 + x_2^2q_1^2) - a(y_1^2q_2^2 + y_2^2q_1^2)\right)$$

$$\cdot e\left(\frac{\ell_1q_2 + \ell_2q_1}{q}(bx_1y_1q_2^2 + x_2y_2q_1^2) - e(y_1^2q_2^2 + y_2^2q_1^2)\right)$$

$$= \sum_{x_1 \pmod{q_1}} \sum_{x_2 \pmod{q_2}} \sum_{y_1 \pmod{q_1}} \sum_{y_2 \pmod{q_2}} e\left(\frac{k_1}{q_1}(bx_1^2q_2^2 - a y_1^2q_2^2) + \ell_1(bx_1y_1q_2^2 - ey_1^2q_2)\right)$$

$$\cdot e\left(\frac{k_2}{q_2}(bx_2^2q_1^2 - a y_2^2q_1^2) + \ell_2(bx_2y_2q_1^2 - ey_2^2q_1)\right)$$

Now, since $q_1$ and $q_2$ are relatively prime, it follows that multiplication by $q_2$ is a bijection on the residue classes mod $q_1$, and vice versa. So it follows that
we can ignore the \( q_1 \) and \( q_2 \) factors multiplying \( x_1, x_2, y_1, \) and \( y_2 \). Therefore, the above sum reduces to

\[
K(k_1, \ell_1, q_1)K(k_2, \ell_2, q_2).
\]

□

From this we conclude that \( K \) is multiplicative:

\[
K(q_1)K(q_2) = \left( \sum_{(k, \ell, q_1) = 1} S(k, \ell, q_1) \right) \left( \sum_{(k, \ell, q_2) = 1} S(k, \ell, q_2) \right)
= \sum_{(k_1, \ell_1, q_1) = 1} \sum_{(k_2, \ell_2, q_2) = 1} K(k_1, \ell_1, q_1)K(k_2, \ell_2, q_2)
= \sum_{(k_1, \ell_1, q_1) = 1} \sum_{(k_2, \ell_2, q_2) = 1} K(k_1 q_2 + k_2 q_1, \ell_1 q_2 + \ell_2 q_1, q_1 q_2).
\]

It follows from a basic CRT argument that this is equal to \( K(q_1 q_2) \), as desired. So \( K \) is multiplicative, and therefore \( K_6 \) is also multiplicative.

Now we show that

\[
\sum_{0 \leq r \leq R} K_6(p^r)
\]

is equal to the density of solutions to the modified system of equations in \((\mathbb{Z}/p^r \mathbb{Z}))^{12}.

\[
\sum_{0 \leq r \leq R} K_6(p^r)
= \sum_{0 \leq r \leq R} \sum_{(k, \ell, p^r) = 1} |K(k, \ell, p^r)^6|
= \sum_{0 < r \leq R} \frac{1}{(p^r)^{2n}} \sum_{(k, \ell, p^r) = 1} \sum_{X, Y \in ((\mathbb{Z}/p^r \mathbb{Z}))^n} e \left( \frac{k}{p^r} f(X, Y) + \frac{\ell}{p^r} g(X, Y) \right),
\]

where \( f(x, y) \) and \( g(x, y) \) are defined as above. First, consider the inner sums over \( k, \ell, X, \) and \( Y, \) fixing \( r \) for now. We interchange the order of summation:

\[
\frac{1}{(p^r)^{2n}} \sum_{X, Y \in ((\mathbb{Z}/p^r \mathbb{Z}))^n} \sum_{(k, \ell, p^r) = 1} e \left( \frac{k}{p^r} f(x, y) + \frac{\ell}{p^r} g(X, Y) \right)
\]
The sum over \( k \) and \( \ell \) satisfying \((k, \ell, p) = 1\) is equal to the sum over all \( k \) and \( \ell \) minus the sum over \( k \) and \( \ell \) such that \( p|k \) and \( p|\ell \). We will first consider the sum over all \( k \) and \( \ell \) and then subtract off the remaining terms later.

Note that since the summand is linear in \( k \) and \( \ell \), the inner sum comes out to zero unless we have \( f(X,Y) \equiv g(X,Y) \equiv 0 \) mod \( p^r \), in which case each term in the sum is equal to 1 so the sum is equal to \( p^{2r} \). So, after multiplying by the \( \frac{1}{p^{12r}} \) out front, the sum over all \( k \) and \( \ell \) comes out to \( p^{2r} N(p^r) \), where \( N(p^r) \) is the number of \( X \) and \( Y \) in \(((\mathbb{Z}/p^r\mathbb{Z}))^n\) solving \( f(X,Y) \equiv g(X,Y) \equiv 0 \) mod \( p^r \).

Now, we look at the terms being subtracted off, in particular, the \( k \) and \( \ell \) such that \( p \) divides both \( k \) and \( \ell \).

\[
\frac{1}{p^{12r}} \sum_{X,Y \in ((\mathbb{Z}/p^r\mathbb{Z}))^n} \sum_{p|k,\ell} e\left( \frac{k}{p^r} f(X,Y) + \frac{\ell}{p^r} g(X,Y) \right)
\]

\[
= \frac{1}{p^{12r}} \sum_{X,Y \in ((\mathbb{Z}/p^r\mathbb{Z}))^n} \sum_{k,\ell \in \mathbb{Z}/p^r-1\mathbb{Z}} e\left( \frac{k}{p^r-1} f(X,Y) + \frac{\ell}{p^r-1} g(X,Y) \right)
\]

Note that the sum in \( k \) and \( \ell \) is nonzero precisely when \( f(X,Y) \equiv g(X,Y) \equiv 0 \) (mod \( p^r-1 \)), which happens \( N(p^{r-1}) \) times mod \( p^r-1 \). Because \( f \) and \( g \) don’t change (mod \( p^r-1 \)) when \( p^r-1 \) is added to any component \( X \) or \( Y \), it follows that there are \( p^{12r} N(p^{r-1}) \) choices for \( X \) and \( Y \) for which the inner sum is nonzero. But when the inner sum is nonzero, each term in the sum is equal to 0 so the sum evaluates to \( p^{2r-2} \). So the subtracted terms’ sum comes out to

\[
\frac{1}{p^{12r}} p^{2r-2} p^{12r} N(p^{r-1})
\]

\[
= (p^{r-1})^2 N(p^{r-1}) \frac{1}{(p^{r-1})^{12}},
\]

which is the sum over all \( k \) and \( \ell \) for the \( r-1 \) term. Therefore, the sum is telescoping, and the sum of the first \( N \) terms is equal to \( p^{2r} N(p^{r-1}) \), which is the density of solutions (mod \( p^r \)). Therefore, the local factor corresponding to \( p \) is the asymptotic density of solutions mod \( p^r \) as \( r \to \infty \).

So the singular series comes out the same as in \( \prod \), except for the fact that the \( A_n(p) \) will be different because we’re counting solutions to a different system of equations.
5.3 The Singular Integral

Most of the calculation for the singular integral here is identical to the singular integral appearing in [1], which is exactly the same as the singular integral appearing here. Since we only need an upper bound, and all of the techniques used to show the convergence of the singular integral depend only on the absolute value of the quantity $L(\delta, \gamma)$, the upper bounds obtained in the evaluation of the singular integral in Chapter 8 are sufficient to show the integral is convergent, and to show that the major arcs are of order $N^8$. Therefore, we have the mean value estimate for the minor arcs, as desired (losing a 12th power of log, which is acceptable).
Chapter 6

Decomposition of the Major Arcs

In order to decompose the integrand into a product of a singular integral and a singular series, we mimic the strategy in chapter 8 of [6].

We will use the following notation:

\[ u(\alpha, \beta) = \sum_{x=1}^{N} \sum_{y=1}^{N} e^{\left( \frac{\alpha}{\beta} (bx^2 - ay^2) + \beta(bxy - ey^2) \right)} \]

\[ S(k, \ell, q) = \sum_{x=1}^{q} \sum_{y=1}^{q} e^{\left( \frac{k}{q} (bx^2 - ay^2) + \frac{\ell}{q} (bxy - ey^2) \right)} \]

\[ S(q) = \sum_{(k, \ell, q)=1} S(k, \ell, q) \]

We start out wanting to estimate the sum

\[ F_{w, z}(\alpha, \beta) = \sum_{p_1 \leq x} \sum_{p_2 \leq x} (\log p_1)(\log p_2)e^{\left( \alpha(bp_1^2 - ap_2^2) + \beta(bp_1p_2 - ep_2^2) \right)} \]

It is sufficient to consider this sum instead of the corresponding sum with the Von Mangoldt factors, as we show in Appendix A.

Consider the case where \( \alpha = \frac{k}{q} \) and \( \beta = \frac{\ell}{q} \), where \( q \leq Q = (\log N)^A \).

We split each sum up mod \( q \), noting that we’re only leaving out primes that divide \( q \) if we only consider the reduced residue classes mod \( q \). Then:

\[ F_{w, z}\left( \frac{k}{q}, \frac{\ell}{q} \right) \]
We now notice that the value of the exponential depends only on the residue class of \( p_1 \) and \( p_2 \) and not on \( p_1 \) and \( p_2 \) themselves. So we pull out the parts of the sum that don’t depend on \( p_1 \) and \( p_2 \).

We now proceed to apply Siegel-Walfisz to both of the inner sums, leaving

\[
= \sum_{r=1}^{q} \sum_{p_1 \leq w, p_1 \equiv r \pmod{q}} \sum_{s=1}^{q} \sum_{p_2 \leq z, p_2 \equiv s \pmod{q}} \\
\left( \log p_1 \right) \left( \log p_2 \right) e^{\left( \frac{k}{q} (bp_1^2 - ap_2^2) + \frac{\ell}{q} (bp_1p_2 - ep_2^2) \right)} + O(q \log^2 q)
\]

We now prove the equivalent of lemma 8.3 in [6] for this problem. The proof is almost exactly the same as the proof appearing in [6].

**Lemma 6.0.1.** For a given \( \alpha = \frac{k}{q} + \delta \) and \( \beta = \frac{\ell}{q} + \gamma \), we have that

\[
F(\alpha, \beta) = \frac{S(k, \ell, q)}{\phi(q)^2} u(\delta, \gamma) + O\left( \frac{Q^4 N^2}{(\log N)^C} \right)
\]

and therefore

\[
F(\alpha, \beta)^n = \frac{S(k, \ell, q)^n}{\phi(q)^{2n}} u(\delta, \gamma)^n + O\left( \frac{Q^{4n} N^{2n}}{(\log N)^C} \right)
\]
Proof. Write \( \alpha = \frac{k}{q} + \delta, \beta = \frac{\ell}{q} + \gamma \), and let \( \lambda \) be the indicator function for the primes weighted by the logarithm. For any \( 1 \leq x, y \leq N \), we have

\[
F(\alpha, \beta) - \frac{S(k, \ell, q)}{\phi(q)^2} u(\delta, \gamma)
\]

\[
= \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} \lambda(m_1)\lambda(m_2)e(\alpha(bm_1^2 - am_2^2) + \beta(bm_1m_2 - em_2^2)) - \frac{S(k, \ell, q)}{\phi(q)^2} \sum_{m_1=1}^{N} \sum_{m_2=1}^{\min(n, m_2)} e(\delta(bm_1^2 - am_2^2) + \gamma(bm_1m_2 - em_2^2))
\]

\[
= \sum_{m_1=1}^{N} \sum_{m_2=1}^{N} \left( \lambda(m_1)\lambda(m_2)e\left(\frac{k}{q}(bm_1^2 - am_2^2) + \frac{\ell}{q}(bm_1m_2 - em_2^2)\right) - \frac{S(k, \ell, q)}{\phi(q)^2} \right) \cdot e(\delta(bm_1^2 - am_2^2) + \gamma(bm_1m_2 - em_2^2)).
\]

Define

\[
B_1(w, z) = \sum_{1 \leq m_1 \leq w} \lambda(m_1)\lambda(m_2)e\left(\frac{k}{q}(bm_1^2 - am_2^2) + \frac{\ell}{q}(bm_1m_2 - em_2^2)\right) - \frac{S(k, \ell, q)}{\phi(q)^2}
\]

\[
B(w, z) = \sum_{1 \leq m_1 \leq w} \sum_{1 \leq m_2 \leq z} \lambda(m_1)\lambda(m_2)e\left(\frac{k}{q}(bm_1^2 - am_2^2) + \frac{\ell}{q}(bm_1m_2 - em_2^2)\right) - \frac{S(k, \ell, q)}{\phi(q)^2}.
\]

Then

\[
B(w, z) = F_{w,z} \left( \frac{k}{q}, \frac{\ell}{q} \right) - \frac{S(k, \ell, q)}{\phi(q)^2} wz + O(1)
\]

\[
= O \left( \frac{Q^2N^2}{(\log N)^C} \right)
\]

Let \( \psi(x, y) = \delta(bx^2 - ay^2) + \gamma(bxy - ey^2) \). We then use partial summation
in the $m_1$ variable to conclude:

$$F(\alpha, \beta) - \frac{S(k, \ell, q)}{\phi(q)^2} u(\delta, \gamma)$$

$$= \sum_{1 \leq m_2 \leq N} B_1(N, m_2)e(\psi(N, m_2))$$

$$- \int_1^N \frac{\partial \psi}{\partial w}(w, m_2)B_1(w, m_2)e(\psi(w, m_2)) \, dw$$

$$= \sum_{1 \leq m_2 \leq N} (B_1(N, m_2)e(\psi(N, m_2)))$$

$$- \int_1^N \sum_{1 \leq m_2 \leq N} 2\pi i \frac{\partial \psi}{\partial w}(w, m_2)B_1(w, m_2)e(\psi(w, m_2)) \, dw$$

We then perform partial summation in the $m_2$ variable:

$$= B(N, N)e(\psi(N, N))$$

$$- \int_1^N 2\pi i \frac{\partial \psi}{\partial z}(N, z)B(N, z)e(\psi(N, z)) \, dz$$

$$- \int_1^N 2\pi i \frac{\partial \psi}{\partial w}(w, N)B(w, N)e(\psi(w, N))$$

$$- \int_1^N 4\pi^2 B(w, z)\left(\frac{\partial \psi}{\partial z}\partial w(w, z) + \frac{\partial \psi}{\partial w}(w, z)\frac{\partial \psi}{\partial z}(w, z)\right) e(\psi(w, z)) \, dz \, dw$$

Now, note that the first partials of $\psi$ are $O\left(\frac{Q}{N}\right)$ since they are linear expressions in $w$ and $z$, which are $O(N)$, and each coefficient contains a $\delta$ or $\gamma$, which is $O\left(\frac{Q}{N}\right)$. Similarly, the second partials of $\psi$ are $O\left(\frac{Q}{N^2}\right)$. Therefore, since the $B$ terms are $O\left(\frac{Q^2 N^2}{(\log N)^{2n}}\right)$, it follows that the whole expression is $O\left(\frac{Q^4 N^2}{(\log N)^{2n}}\right)$. The statement about higher powers of this expression follows trivially from this one. \qed

The $\frac{S(k, \ell, q)^n}{\phi(q)^{2n}}$ terms become the singular series. We then transform $u^n$ into the singular integral as in [1]:

$$F(\alpha, \beta)^n = O\left(\frac{Q^4 N^{2n}}{\log(N)^C} + \frac{S(k, \ell, q)^n}{\phi(q)^{2n}} u(\delta, \gamma)^n\right)$$
where
\[
u(\delta, \gamma)^n = \sum_{X, Y} e(\delta(b(X)^2 - a(Y)^2) + \gamma(b(X) \cdot (Y) - e(Y)^2)) \\
\cdot \chi\left(\frac{X}{N}\right) \chi\left(\frac{Y}{N}\right).
\]

We then show that the summand in \( u^n \) is close to the integral
\[
\int_{X'=0}^1 \int_{Y'=0}^1 e(\delta(b(X + X')^2 - a(Y + Y')^2)) \\
\cdot e(\gamma(b((X + X') \cdot (Y + Y') - e(Y + Y')^2)) \\
\cdot \chi\left(\frac{(X + X')}{N}\right) \chi\left(\frac{(Y + Y')}{N}\right)
\]

We do this by noting that the changing \( X + X' \) to \( X \) in the above integral has only a small effect on its value. In particular, changing \( X + X' \) to \( X \) in the characteristic function only changes the boundary term in the sum, of which there are only \( O((N)^{2n-1}) \), and integrating this error term over the major arcs yields an error of \( \lesssim N^{2n-5}(\log N)^{C(A)} \).

We also change the exponent in the above integral. Noting that \(|\int e(x) - e(t)| \lesssim \int |x - t|\), we realize through direct calculation that the error in changing the exponential is \( O((|\gamma| + |\delta|)N) \), but since we’re in a major arc \( \gamma \) and \( \delta \) are at most \( \frac{(\log N)^{C(A)}}{qN^{2}} \), and \( 1 \leq q < (\log N)^{C(A)} \) so the error becomes \( O\left(\frac{1}{N}(\log N)^{C(A)}\right) \). We now integrate the difference over all of the major arcs, giving an error of \( O\left(N^{2n-5}(\log N)^{2C(A)}\right) \). So we can change \( u^n \) to the integral
\[
\int_X \int_Y e(\delta(b(X)^2 - a(Y)^2) + \gamma(b(X) \cdot (Y) - e(Y)^2)) \\
\cdot \chi\left(\frac{X}{N}\right) \chi\left(\frac{Y}{N}\right) dXdY
\]

This yields the product
\[
F(\alpha, \beta) = \sum_{\text{Major Arcs}} K_n(k, \ell, q) \cdot L(\delta, \gamma, k, \ell, q) + o(N^{2n-4})
\]
where
\[
K_n(k, \ell, q) = \frac{S(k, \ell, q)^n}{\phi(q)^{2n}}
\]
and

\[ L(\delta, \gamma, k, \ell, q) = \int_{X,Y} e^{(\delta(b(X)^2 - a(Y)^2) + \gamma(bX \cdot Y - eY^2))} \cdot \chi \left( \frac{X}{N} \right) \chi \left( \frac{Y}{N} \right) dXdY. \]
Chapter 7

The Singular Series

7.1 Multiplicativity of S

Suppose $q = q_1 q_2$ with $(q_1, q_2) = 1$.

$$S(k_1 q_2 + k_2 q_1, \ell_1 q_2 + \ell_2 q_1, q)$$

$$= \sum_{(x, q) = 1} \sum_{(y, q) = 1} e\left(\frac{k_1 q_2 + k_2 q_1 (b x^2 - a y^2) + \ell_1 q_2 + \ell_2 q_1 (b x y - e y^2)}{q}\right)$$

We apply the Chinese remainder theorem:

$$= \sum_{(x, q_1) = 1} \sum_{(x_2, q_2) = 1} \sum_{(y_2, q_2) = 1} \sum_{(y_1, q_1) = 1} e\left(\frac{(k_1 q_2 + k_2 q_1) (b (x_1 q_2 + x_2 q_2)^2 - a (y_1 q_2 + y_2 q_2)^2)}{q}\right)$$

$$\cdot e\left(\frac{(\ell_1 q_2 + \ell_2 q_1) (b (x_1 q_2 + x_2 q_2) (y_2 q_2 + y_1 q_1) - e (y_1 q_2 + y_2 q_2)^2)}{q}\right)$$

Then, noting that the cross terms all cancel out in the expansion:

$$= \sum_{(x_1, q_1) = 1} \sum_{(x_2, q_2) = 1} \sum_{(y_2, q_2) = 1} \sum_{(y_1, q_1) = 1} e\left(\frac{k_1 (b x_1^2 q_2^2 - a y_1^2 q_2^2) + \ell_1 (b x_1 y_1 q_2^2 - e y_1^2 q_2^2)}{q_1}\right)$$

$$\cdot e\left(\frac{k_2 (b x_2^2 q_1^2 - a y_2^2 q_1^2) + \ell_2 (b x_2 y_2 q_1^2 - e y_2^2 q_1^2)}{q_2}\right)$$
Now, since $q_1$ and $q_2$ are relatively prime, it follows that multiplication by $q_2$ is a bijection on the reduced residue classes mod $q_1$, and vice versa. So it follows that we can ignore the $q_1$ and $q_2$ factors multiplying $x_1, x_2, y_1$, and $y_2$. Therefore, the above sum reduces to

$$S(k_1, \ell_1, q_1)S(k_2, \ell_2, q_2).$$

We then use this fact as follows:

$$S(q_1)S(q_2) = \left( \sum_{(k, \ell, q_1) = 1} S(k, \ell, q_1) \right) \left( \sum_{(k, \ell, q_2) = 1} S(k, \ell, q_2) \right)$$

$$= \sum_{(k_1, \ell_1, q_1) = 1} \sum_{k_2, \ell_2, q_1 = 1} S(k_1, \ell_1, q_1)S(k_2, \ell_2, q_2)$$

$$= \sum_{(k_1, \ell_1, q_1) = 1} \sum_{k_2, \ell_2, q_2 = 1} S(k_1 q_2 + k_2 q_1, \ell_1 q_2 + \ell_2 q_1, q_1 q_2).$$

It follows from a basic CRT argument that this is equal to $S(q_1 q_2)$, as desired.

### 7.2 Convergence of the Product Representation of the Series

Given the multiplicativity shown in the previous section, along with the multiplicativity of the totient function, we hope that the singular series

$$\sum_{q=1}^{\infty} \frac{1}{\phi(q)2^n} S(q)^n$$

will have the Euler product representation

$$\prod_{p \text{ prime}} \left( 1 + \sum_{r=1}^{\infty} \frac{S(p^r)^n}{\phi(p^r)^{2n}} \right).$$

In order to do this, we find an estimate on $S(k, \ell, q)$ for prime powers $q$.  

\[ S(k, \ell, q)^n = \sum_{(X,q)=1} \sum_{(Y,q)=1} e\left( \frac{k}{q}(bX^2 - aY^2) + \frac{\ell}{q}(bX \cdot Y - eY^2) \right). \]

Where the condition \((X, q) = 1\) means that each component of \(X\) is relatively prime to \(q\). In order to estimate this sum for odd prime powers \(p^r\), we break \(X\) up as \(X_1 + p^{[r/2]}X_2\)

\[ S(k, \ell, p^r) = \sum_{(x,p)=1} \sum_{0 \leq X_2 < p^{[r/2]}} \sum_{(Y,p)=1} \sum_{0 \leq Y_2 < p^{[r/2]}} e\left( \frac{k}{p^r}(b(X_1 + p^{[r/2]}X_2)^2 - a(Y_1 + p^{[r/2]}Y_2)^2) \right) \]

\[ \cdot e\left( \frac{\ell}{p^r}(b(X_1 + p^{[r/2]}X_2)(Y_1 + p^{[r/2]}Y_2) - e(Y_1 + p^{[r/2]}Y_2)^2) \right) \]

(Here, the condition in the sum means that each component of \(X_1, X_2, Y_1, \) and \(Y_2\) satisfies each inequality.)

\[ = \sum_{(x,p)=1} \sum_{0 \leq X_2 < p^{[r/2]}} \sum_{(Y,p)=1} \sum_{0 \leq Y_2 < p^{[r/2]}} e\left( \frac{k}{p^r}(b(X_1^2 + 2p^{[r/2]}X_1 \cdot X_2 + (p^{[r/2]}X_2)^2)) \right) \]

\[ \cdot e\left( \frac{k}{p^r}(-a(Y_1^2 + 2p^{[r/2]}Y_1 \cdot Y_2 + (p^{[r/2]}Y_2)^2)) \right) \]

\[ \cdot e\left( \frac{\ell}{p^r}(b(X_1 \cdot Y_1 + p^{[r/2]}X_1 \cdot Y_2 + p^{[r/2]}X_2 \cdot Y_1 + X_2 \cdot Y_2(p^{[r/2]}))^2) \right) \]

\[ \cdot e\left( \frac{\ell}{p^r}(-e(Y_1^2 + 2p^{[r/2]}Y_1 \cdot Y_2 + (p^{[r/2]}Y_2)^2)) \right) \]

Now we eliminate all of the integers from the exponent and pull out everything that doesn’t depend on \(X_2\) and \(Y_2\):

\[ S(k, \ell, q) = \sum_{(X_1,p)=1} \sum_{X_1 \leq p^{[r/2]}} e\left( \frac{k}{p^r}(bX_1^2 - aY_1^2) + \frac{\ell}{p^r}(bX_1 \cdot Y_1 - eY_1^2) \right) \]

\[ \sum_{X_2 \leq p^{[r/2]}} \sum_{Y_2 \leq p^{[r/2]}} e\left( \frac{k}{p^{[r/2]}}(2bX_1 \cdot X_2 - 2aY_1 \cdot Y_2) \right) \]

\[ \cdot e\left( \frac{\ell}{p^{[r/2]}}(bX_1 \cdot Y_2 + bX_2 \cdot Y_1 - 2eY_1 \cdot Y_2) \right) \]
Now, we take the absolute value of both sides and apply the triangle inequality:

\[
\leq \sum_{(X_1,p) = 1 \atop X_1 \leq p^{\lceil r/2 \rceil}} \sum_{Y_1 \leq p^{\lfloor r/2 \rfloor}} e \left( \frac{k}{p^{\lfloor r/2 \rfloor}} (2bX_1 \cdot X_2 - 2aY_1 \cdot Y_2) \right) \cdot e \left( \frac{l}{p^{\lceil r/2 \rceil}} (bX_1 \cdot Y_2 + bX_2 \cdot Y_1 - 2eY_1 \cdot Y_2) \right)
\]

Now, we concern ourselves with the sums inside of the absolute value signs. This sum is

\[
\sum_{X_2 \leq p^{\lceil r/2 \rceil}} \sum_{Y_2 \leq p^{\lfloor r/2 \rfloor}} e \left( X_2 \cdot \frac{1}{p^{\lfloor r/2 \rfloor}} (2kbX_1 + \ell bY_1) \right) \cdot e \left( Y_2 \cdot \frac{1}{p^{\lceil r/2 \rceil}} (-2kaY_1 + \ell bX_1 - 2eY_1) \right)
\]

The exponent in the summand is linear in each of \(X_2\) and \(Y_2\), so the sum is equal to zero unless both the vector multiplying \(X_2\) and the vector multiplying \(Y_2\) are componentwise congruent to zero mod \(p^{\lceil r/2 \rceil}\). So we count the number of solutions to the system of equations

\[
\begin{align*}
2kbX_1 + \ell bY_1 &\equiv 0 \pmod{p^{\lceil r/2 \rceil}} \\
\ell bX_1 - 2kaY_1 - 2eY_1 &\equiv 0 \pmod{p^{\lfloor r/2 \rfloor}}.
\end{align*}
\]

Suppose first that \(b\) is invertible mod \(p^{\lceil r/2 \rceil}\). Consider an arbitrary component \(x_1\) of \(X_1\). Then we can (assuming without loss of generality that \((k,p) = 1\); the same result is obtained if \((l,p) = 1\)) simplify the first equation to

\[
x_1 \equiv -\frac{\ell}{2k} y_1
\]

and then

\[
\frac{-\ell^2b}{2k} - 2ka - 2e(y_1) \equiv 0
\]

Note that since \((y_1,p^{\lfloor r/2 \rfloor}) = 1\) by assumption, this system only has solutions in the case where \(\frac{\ell^2 b}{2k} - 2ka - 2e \equiv 0\), in which case there are \((\phi(p^{\lceil r/2 \rceil}))^n\) solutions corresponding to each different choice of \(Y_1\).
Now suppose instead that $b$ is divisible by $p$. Let $p^{\gamma} = (b, p^{\lfloor r/2 \rfloor})$. Then there are $p^{\gamma}$ different values of $x_1$ that could solve the first equation for a given $y_1$. These values all differ by a multiple of $p^{\lfloor r/2 \rfloor} - \gamma$. Since one solution to the first equation is given by $x_1 = -\frac{\ell}{2k}y_1$, it follows that the other solutions are of the form

$$x_1 = -\frac{\ell}{2k}y_1 + cp^{\lfloor r/2 \rfloor} - \gamma$$

for each component $x_1$ of the vector of the vector $X_1$ and each corresponding component $y_1$ of $Y_1$.

Note that in this case, $bc p^{\lfloor r/2 \rfloor} - \gamma$ is divisible by $p^{\lfloor r/2 \rfloor}$ so this term disappears in the second equation upon substituting for $X_1^{(k)}$, and the second equation again becomes

$$\left( -\frac{\ell^2b}{2k} - 2ka - 2\ell e \right)(y_1) \equiv 0.$$

So we now pick up $p^{n\gamma} \phi(p^{\lfloor r/2 \rfloor})^n$ solutions if $-4k^2a - \ell^2b - 4k\ell e \equiv 0$ and $p^{\gamma} < p^{\lfloor r/2 \rfloor}$, $\phi(p^{\lfloor r/2 \rfloor})^n \phi(p^{\lfloor r/2 \rfloor})^n$ solutions if $-4k^2a - \ell^2b - 4k\ell e \equiv 0$ and $p^{\gamma} = p^{\lfloor r/2 \rfloor}$, and 0 solutions otherwise. Since there are $(p^{\lfloor r/2 \rfloor})^2n$ terms in the inner two sums, we have that $S(k, \ell, p^r)$ is bounded above by $p^{\gamma n} p^{2(n+1)n} \phi(p^{\lfloor r/2 \rfloor})^n \phi(p^{\lfloor r/2 \rfloor})^n \chi(4k^2a - \ell^2b - 4k\ell e \equiv 0, p^{\gamma} | b)$. Note that $p^{\gamma n}$ is further bounded above by $b^n$.

Now we count the number of $k, \ell$ such that

$$-4k^2a - \ell^2b - 4k\ell e \equiv 0 \pmod{p^{\lfloor r/2 \rfloor}}$$

We can assume without loss of generality that at least one of $a, b,$ and $e$ is not divisible by $p$. If $a$ is not divisible by $p$, then fixing $\ell$ and completing the square in $k$ shows that there are at most 2 solutions (mod $p^{\lfloor r/2 \rfloor}$) where $k$ is not divisible by $p$. Write $k = k'p^\delta$ where $(k', p) = 1$. Suppose that $p^\delta$ divides exactly 2 terms for some $\delta$. Then the third term is not divisible by $p^\delta$ and therefore the system has no solutions. This will happen if, say, $p^\delta > b$, since that would imply that the other two terms, each of which contains a factor of $k$, are divisible by $p^\delta$, but not the $b\ell^2$ term. So there are at most $1 + \frac{\log b}{\log p} \lesssim 1$ possible values of $s$ here.
If \( p^{2s} \) divides all 3 terms, we’re left with the equation

\[
-4ak'^2 - 4e'k'\ell - \ell^2b' \equiv 0 \pmod{p^{\left\lfloor \frac{r}{2} \right\rfloor - 2s}}
\]

for some \( b'|b \) and some \( e'|e \) (it is possible that \( b' \) or \( e' \) may be divisible by \( p \)). So \( k \) can take the values \( cp^{\left\lfloor \frac{r}{2} \right\rfloor + s}k' \). Note that for a given \( \ell \) there are at most two values of \( k' \) that solve this congruence and therefore there are \( \lesssim p^{\left\lceil \frac{r}{2} \right\rceil} \) solutions to the equation for which \( k = p^s k' \), where \( (p, k') = 1 \).

If \( b \) is maximally divisible by \( p^\delta \), but the terms containing \( e \) and \( a \) are also both divisible by \( p^\delta \), then we divide the congruence by \( p^\delta \) to arrive at

\[
-4ap^{2s-\delta}k'^2 - 4ek'^p^s-\delta \ell - \ell^2b' \equiv 0 \pmod{p^{\left\lfloor \frac{r}{2} \right\rfloor - \delta}},
\]

where \( b' \) is not divisible by \( p \). Now, noting that since \( p \) divides \( k \) and \( (p, k, \ell) = 1 \), it follows that \( p \) doesn’t divide \( \ell \). So we can complete the square in \( \ell \) and determine that for \( k \) such that \( p^\delta | k \) (of which there are at most \( p^r \)), there are at most two values of \( \ell \pmod{p^{\left\lfloor \frac{r}{2} \right\rfloor - \delta}} \) that solve the congruence. Therefore, there are at most \( 2p^r p^{\left\lceil \frac{r}{2} \right\rceil} \) solutions to the congruence \( (\pmod{p^r}) \). But since \( p^\delta < b \) in this case, we have that there are \( \lesssim p^r p^{\left\lceil \frac{r}{2} \right\rceil} \) solutions to the congruence \( (\pmod{p^r}) \), as desired. So no matter what \( a, b, \) and \( e \) are, there are \( \lesssim p^r p^{\left\lceil \frac{r}{2} \right\rceil} \) solutions, where the implicit constant depends on the values of \( a, b, \) and \( e \).
So the term added to 1 in the product corresponding to \( p \) is bounded above in absolute value by a constant times the expression:

\[
\sum_{r=1}^{\infty} \frac{b^n p^{2\left[\frac{r}{2}\right]} n \phi(p^{[r/2]}) n p^{[r/2]} p^r}{\phi(p^r)^{2n}} \lesssim \sum_{r=1}^{\infty} \frac{p^{[r/2]} p^r}{(p^{[r/2]})^n (1 - \frac{1}{p})^n} \lesssim \sum_{r=1}^{\infty} \frac{p^{r-(n-1)(r/2)}}{(1 - \frac{1}{p})^n} \leq (1 - \frac{1}{p})^{-n} \sum_{r=1}^{\infty} (p^{-\frac{3-n}{2}})^r
\]

which converges so long as \( n \geq 4 \). This converges to

\[
(1 - \frac{1}{p})^{-n} \left( \frac{p^{-\frac{3-n}{2}}}{1 - p^{-\frac{3-n}{2}}} \right) \lesssim n^2 p^{-\frac{3-n}{2}}.
\]

So the product over all odd primes converges for \( n \geq 6 \).

Now we show that the local factor \( \sigma_2 \) corresponding to \( p = 2 \) also converges. It follows just as before that we need to count the number of solutions to the equations

\[
2kbX_1 + \ell bY_1 \equiv 0 \pmod{2^{[r/2]}}
\]

\[
\ell bX_1 - 2kaY_1 - 2\ell eY_1 \equiv 0 \pmod{2^{[r/2]}}.
\]

Now, note that this system of equations only has solutions if either \( b \) is divisible by \( 2^{[r/2]} \) or if \( \ell \) is divisible by 2 but not by 4 (since if \( \ell \) is divisible by 2, \( k \) can’t be divisible by 2). Note that for sufficiently large \( r \) we must have \( \ell \) divisible by 2 but not by 4 since \( b \) is a constant. So we let \( b = 2^\gamma b' \) and let \( \ell = 2\ell' \):

\[
2^{\gamma+1} k b' X_1 + 2^{\gamma+1} \ell' b' Y_1 \equiv 0 \pmod{2^{[r/2]}}
\]

\[
kb' X_1 + \ell' b' Y_1 \equiv 0 \pmod{2^{[r/2] - \gamma - 1}}
\]

\[
X_1 \equiv -\frac{\ell'}{k} Y_1 \pmod{2^{[r/2] - \gamma - 1}}
\]

We then substitute into the other equation, noting that if \( X_1 = -\frac{\ell' Y_1}{k} + 2^{[r/2] - \gamma - 1} c \), the multiple of \( 2^{[r/2] - \gamma - 1} \) cancels out since it is multiplied by
2b. So we get
\[
2^{\gamma+1} \frac{\ell'^2 b'}{k^2} Y_1 - 2kaY_1 - 4\ell'ey_1 \equiv 0 \pmod{2^{|r/2|}}.
\]
Factoring out the \(Y_1\),
\[
\left(2^{\gamma+1} \frac{\ell'^2 b'}{k} - 2ka - 4\ell' e\right) Y_1 \equiv 0 \pmod{2^{|r/2|}}.
\]
We then multiply through by \(k\) and eliminate a factor of 2 from the equation, and note that \(Y_1\) is componentwise relatively prime to \(p^r\):
\[
2^{\gamma+1} \ell'^2 b' - k^2 a - 2k\ell' e \equiv 0 \pmod{2^{|r/2|}-1}
\]
So we again count the number of \(k\) and \(\ell\) solving this equation. It is then clear that for \(r \geq 4\) there are no solutions if \(a\) and \(b\) don’t have the same parity. If \(a\) and \(b\) are both odd, this equation has at most four solutions, as can be seen by completing the square (this is always possible in at most two ways as the mixed term is always divisible by 2).

As with other primes, we can assume that if \(a\) and \(b\) are even, then \(e\) must be odd. We then remove another factor of two from the equation, setting \(a = 2^\delta a'\)
\[
2^{\gamma+1-\delta} \ell'^2 b' - 2^{\delta-1} k^2 a' - k\ell' e = 0 \pmod{2^{|r/2|}-2}
\]
which only has solutions for \(\gamma = 1, \delta = 1,\) or \(r \leq 5\). So for \(r > 6\), there are at most \(8\phi(2^r)\) solutions in \(k\) and \(\ell\) (mod \(2^{|r/2|}-1\)).

So in either case, the number of solutions in \(k\) and \(\ell\) for a given \(X_1\) and \(Y_1\) is \(\lesssim \phi(2^r)2^{|r/2|}\). Furthermore, for a given \(Y_1\) there are \(\lesssim 2^{(\gamma+1)n} \leq b^n \lesssim 1\) choices for \(X_1\). So the sum over all \(k, \ell\) of \(S(k, \ell, 2^r)\) is bounded by
\[
\lesssim (2^{|r/2|})^{2n} \phi(2^{|r/2|})^n 2^{|r/2|} \phi(2^r),
\]
so as in the case for the odd primes, the local factor \(\sigma_2\) is finite. Therefore the product representation of the singular series converges.

Note that the bound \(\frac{1}{\phi(p^r)} S(p^r) \lesssim p^{\frac{3-n}{2}}\) shown in this section, along with the multiplicativity shown in the previous section, is enough to show that the sum representation of the singular series converges absolutely, since it follows from this statement and the multiplicativity that
\[
\frac{1}{\phi(q)} S(q) \lesssim C^{\omega(q)} q^{\frac{3-n}{2}} \lesssim q^{\frac{3-n}{2}+\epsilon},
\]
so the sum over all \(q\) of this quantity converges for \(n \geq 6\).
In the following few sections, we show that none of the local factors are equal to zero.

### 7.3 Local Factors and the Asymptotic Density of Solutions mod $p^r$

In this section, it is shown that the sum

$$\sum_{0 \leq r \leq R} \frac{1}{\phi(p^r)^2} S_n(p^r)$$

is equal to the density of solutions to the system of equations in $((\mathbb{Z}/p^r\mathbb{Z})^*)^{2n}$.

$$\sum_{0 \leq r \leq R} \frac{1}{\phi(p^r)^2} S_n(p^r) = \sum_{0 \leq r \leq R} \sum_{(k,\ell,p^r)=1} S(k,\ell,p^r)^n$$

First, consider the inner sums over $k,\ell,X\text{, and }Y$, fixing $r$ for now. We interchange the order of summation:

$$\frac{1}{\phi(p^r)^2} \sum_{X,Y \in ((\mathbb{Z}/p^r\mathbb{Z})^*)^n} \sum_{(k,\ell,p^r)=1} e\left(\frac{k}{p^r} f(X,Y) + \frac{\ell}{p^r} g(X,Y)\right)$$

The sum over $k$ and $\ell$ satisfying $(k,\ell,p^r) = 1$ is equal to the sum over all $k$ and $\ell$ minus the sum over $k$ and $\ell$ such that $p|k$ and $p|\ell$. We will first consider the sum over all $k$ and $\ell$ and then subtract off the remaining terms later.

Note that since the summand is linear in $k$ and $\ell$, the inner sum comes out to zero unless we have $f(X,Y) \equiv g(X,Y) \equiv 0 \mod p^r$, in which case each term in the sum is equal to $1$ so the sum is equal to $p^{2r}$. So, after multiplying by the $\frac{1}{\phi(p^r)^2}$ out front, the sum over all $k$ and $\ell$ comes out to $\frac{p^{2r} N(p^r)}{\phi(p^r)^2}$, where $N(p^r)$ is the number of $X$ and $Y$ in $((\mathbb{Z}/p^r\mathbb{Z})^*)^n$ solving $f(X,Y) \equiv g(X,Y) \equiv 0 \mod p^r$. 

44
Now, we look at the terms being subtracted off, in particular, the $k$ and $\ell$ such that $p$ divides both $k$ and $\ell$.

\[
\frac{1}{\phi(p^r)^{2n}} \sum_{X,Y \in ((\mathbb{Z}/p^r)^*)^n} e\left(\frac{k}{p^r} f(X,Y) + \frac{\ell}{p^r} g(X,Y)\right)
\]

\[
= \frac{1}{\phi(p^r)^{2n}} \sum_{X,Y \in ((\mathbb{Z}/p^r)^*)^n} \sum_{k,\ell \in \mathbb{Z}/p^r-1} e\left(\frac{k}{p^r-1} f(X,Y) + \frac{\ell}{p^r-1} g(X,Y)\right)
\]

Note that the sum in $k$ and $\ell$ is nonzero precisely when $f(X,Y) \equiv g(X,Y) \equiv 0 \pmod{p^r-1}$, which happens $N(p^r-1)$ times mod $p^r-1$. Because $f$ and $g$ don’t change (mod $p^r-1$) when $p^r-1$ is added to any component $X$ or $Y$, it follows that there are $p^{2n}N(p^r-1)$ choices for $X$ and $Y$ for which the inner sum is nonzero. But when the inner sum is nonzero, each term in the sum is equal to 1 so the sum evaluates to $p^{2r-2}$. So the subtracted terms’ sum comes out to

\[
\frac{1}{\phi(p^r)^{2n}} p^{2r-2} p^{2n} N(p^r-1)
\]

\[
= (p^r-1)^2 N(p^r-1) \frac{1}{\phi(p^r)^{2n}},
\]

which is the sum over all $k$ and $\ell$ for the $r-1$ term. Therefore, the sum is telescoping, and the sum of the first $N$ terms is equal to $\frac{p^2}{\phi(p^r)^n} N(p^r-1)$, which is the density of solutions (mod $p^r$). Therefore, the local factor corresponding to $p$ is the asymptotic density of solutions mod $p^r$ as $r \to \infty$.

### 7.4 Finding a Large Space of Solutions with Prime Modulus

We can find a set of $\gg p^{12}$ solutions to the system

\[
bX^2 - aY^2 \equiv 0 \pmod{p}
\]

\[
bX \cdot Y - eY^2 \equiv 0 \pmod{p}
\]

for any prime that is at least 23. Select any choices for $x_1, \ldots, x_n,\ y_5, y_6, \ldots, y_n$ that satisfy $x_1^2 + x_2^2 \neq 0, x_3^2 + x_4^2 \neq 0, \text{ and } x_1^2 + x_2^2 + x_3^2 + x_4^2 \neq 0 \pmod{p}$. We will show that some "2-dimensional" set in the remaining 4 variables solves the two equations (mod $p$) (assuming for now that none of $a, b, \text{ and } e$ is divisible by $p$). In particular, we can select $y_1, y_2, y_3, \text{ and } y_4$ such that $bX^2 - aY^2 = 0$ and so that $bX \cdot Y - eY^2 = 0$. 

45
To do this, we seek solutions to the system

\[ w_1 z_1 + w_2 z_2 = A \]
\[ w_3 z_3 + w_4 z_4 = B \]
\[ z_1^2 + z_2^2 + z_3^2 + z_4^2 = C. \]

Then, we get

\[ z_2 = \frac{1}{w_2} (A - w_1 z_1) \]
\[ z_4 = \frac{1}{w_4} (B - w_3 z_3) \]

(we can do this because \( w_j \) is invertible mod \( p \) for every \( j \)). Then, we must solve

\[ z_1^2 + \frac{1}{w_2^2} (w_1^2 z_1^2 - 2A w_1 z_1 + A^2) + z_3^2 + \frac{1}{w_4^2} (w_3^2 z_3^2 - 2B w_3 z_3 + B^2) = C \]

We then divide by \( w_1^2 + w_2^2 \) and \( w_3^2 + w_4^2 \), and complete the square in \( z_1 \) and \( z_3 \), leaving

\[
\frac{1}{(w_1^2 + w_2^2)(w_3^2 + w_4^2)}(z_1 - \frac{A w_1}{w_1^2 + w_2^2})^2 + \frac{1}{(w_1^2 + w_2^2)w_4^2}(z_3 - \frac{B w_3}{w_3^2 + w_4^2})^2
\]

\[ = \frac{C}{(w_1^2 + w_2^2)(w_3^2 + w_4^2)} \]

\[ \frac{A^2}{w_2^2(w_1^2 + w_2^2)(w_3^2 + w_4^2)} - \frac{B^2}{w_4^2(w_1^2 + w_2^2)(w_3^2 + w_4^2)} + \frac{A^2 w_1^2}{w_2^2(w_1^2 + w_2^2)^2(w_3^2 + w_4^2)} + \frac{B^2 w_3^2}{w_4^2(w_1^2 + w_2^2)^2(w_3^2 + w_4^2)} \]

The right hand side simplifies to

\[ \frac{C}{(w_1^2 + w_2^2)(w_3^2 + w_4^2)} - \frac{A^2 w_1^2}{w_2^2(w_1^2 + w_2^2)^2(w_3^2 + w_4^2)} - \frac{B^2 w_3^2}{w_4^2(w_1^2 + w_2^2)(w_3^2 + w_4^2)^2} \]

which is a nontrivial first degree polynomial expression in \( A^2 \) and \( B^2 \). We will show that only at most two choices of \( A \) make this expression zero.

In particular, note that since we’re fixing \( A + B \), the system \( A + B = D_1, GA^2 + HB^2 = D_2 \) has at most 2 solutions as long as \( G \neq -H \), which in this case would mean that \( w_1^2 + w_2^2 + w_3^2 + w_4^2 \neq 0 \) (mod \( p \)) (this is a necessary
assumption anyway). Then, there are 4 “bad” ways to decompose the right side as a sum of residues/nonresidues (that correspond to $z_j$ being zero for some $j$), so as long as $p$ is at least 23, it follows from [2] are at least 5 (and in particular $\sim \frac{p}{4}$) ways to write the rhs as desired, showing our result. Since $A$ was allowed to range over $p−1$ different choices, and $B$ depends on $A$, and the number of decompositions of the right side of the equation at the end is a multiple of $\frac{p}{4}$, there are at least a nonzero constant times $\phi(p^{10}) \ast p^2$ solutions mod $p$.

Suppose instead that $e$ is equal to zero, and that $b$ is nonzero. Then we can select $X, y_5, y_6, \ldots, y_n$ however we want, and then select the remaining $y$ variables to make the dot product zero and to make the first equation work out, as in the case where $e$ is nonzero. If $b$ is divisible by $p$, then the equations reduce to $aY^2 = 0$ and $eY^2 = 0$, which clearly has at least a 12-dimensional solution space. If $a$ is divisible by $p$, then the equations reduce to $bx^2 = 0$ and $bX \cdot Y − eY^2 = 0$. Here, we use a different solution strategy, selecting all the $y$ variables first and choosing the last four $x$ variables as in the above argument, to make both equations work out.

### 7.5 Some Results for Smaller Moduli

For $p = 5, 11, 13, 17$, or 19, we use a different strategy. A brute-force computation using the program in Appendix D shows that we can achieve any values we want for $x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$ and $y_2^2 + y_3^2 + y_4^2$ simultaneously, for any choice of $x_1, x_2, x_3, \text{ and } x_4$, guaranteeing a solution.

Furthermore, another brute force computation using the program in Appendix D shows that we can accomplish the same feat mod 7 for any $x_1, x_2, x_3, x_4$ such that at most 3 of the variables are either 1 or 6, at most 3 of the variables are either 2 or 5, and at most 3 of the variables are either 3 or 4. This, together with the lifting argument, is sufficient to show that the local factor mod 7 is positive.

Mod 9, a brute force computation using the program in Appendix E shows that we can get any value for $x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4$ that we want provided that none of $x_1, x_2, x_3, \text{ and } x_4$ are divisible by 3 (which is certainly true if they are prime), and simultaneously get $y_1^2 + y_2^2 + y_3^2 + y_4^2$ to be any value mod 9 as long as it’s congruent to 1 mod 3, providing us with a solution to the system (mod 9).
7.6 Finding a Nonsingular Solution mod $p$ for Odd Primes $p$

In the previous section, we have found, for each odd prime $p$ except for 3, a solution to the system

$$bX^2 - aY^2 \equiv 0 \pmod{p}$$
$$bX \cdot Y - eY^2 \equiv 0 \pmod{p}.$$ 

(We have also found a solution for 9). Call a solution to the system “nonsingular” if any of the following conditions hold:

1. $b$ is not divisible by $p$, and the matrix

$$\begin{pmatrix} 2bx_5 & -2ay_5 \\ by_5 & bx_5 - 2ey_5 \end{pmatrix}$$

has nonzero determinant.

2. $p$ divides $b$ and $p$ divides $a$ or $e$,

3. $p > 3$, $p$ divides $b$, $p$ doesn’t divide $a$ or $e$, and the system

$$\begin{pmatrix} 2b'x_5 & -2ay_5 \\ b'y_5 & bx_5 - 2ey_5 \end{pmatrix}$$

has nonzero determinant, where $b'$ is the largest divisor of $b$ that is relatively prime to $p$, that is $b' = \frac{b}{\gcd(b, p)}$.

We will show that nonsingular solutions exist for every odd prime $p$, and then use a lifting argument to generate $\gtrsim p^{r(2n-2)}$ nonsingular solutions (mod $p$) for each $p$.

Note that the argument in the previous section only required control over the first four variables $x_1, x_2, x_3, x_4$ and $y_1, y_2, y_3, y_4$. So there are solutions to the system (mod $p$) or (mod 9) for any values of $x_5$ and $y_5$. So in case 1, we need only find $x_5$ and $y_5$ for which the quadratic form $2b(bx_5^2 - 2ex_5y_5 + ay_5^2)$ is nonzero, which is certainly possible if $e$ is not divisible by $p$ (since we can complete the square in $x_5$ to conclude that for a fixed $y_5$ there are at least $\frac{p-1}{2}$ possible values for this expression), but also possible if $e$ is divisible by $p$ since then we’re left with a linear form in $x_5^2$ and $y_5$, so fixing $y_5$ and letting $x_5$ vary will produce at least 2 different values for $2b^2x_5^2$ since $p > 3$; specifically, the quadratic residues (mod $p$) translated by the value $-\frac{e^2}{b}y_5^2$. In case 2, any solution is nonsingular, so there is nothing to do. Case 3 is handled in exactly the same way as case 1. So there is always a nonsingular solution (mod $p$).
7.7 Lifting Argument for Odd Primes when $b$ is not Divisible by $p$

In this section, we produce a “lifting” argument that will generate $p^{2n-2}$ nonsingular solutions $(X,Y)$ to the system

\[
\begin{align*}
    bX^2 - aY^2 &\equiv 0 \pmod{p^{r+1}} \\
    bX \cdot Y - eY^2 &\equiv 0 \pmod{p^{r+1}}.
\end{align*}
\]

given a nonsingular solution $(\tilde{X}, \tilde{Y})$ to the system mod $p^r$. These generated solutions will satisfy $(X, Y) \equiv (\tilde{X}, \tilde{Y}) \pmod{p^r}$. Therefore, if $N((a, b, e), p^r)$ is the number of solutions to the system (mod $p^r$), then we have that $N((a, b, e), p^{r+1}) \geq p^{2n-2} N((a, b, e), p^r)$.

Suppose that $(\tilde{X}, \tilde{Y})$ satisfy

\[
\begin{align*}
    b\tilde{X}^2 - a\tilde{Y}^2 &\equiv 0 \pmod{p^r} \\
    b\tilde{X} \cdot \tilde{Y} - e\tilde{Y}^2 &\equiv 0 \pmod{p^r}.
\end{align*}
\]

Suppose first that $b$ is not divisible by $p$. Suppose that $(\tilde{X}, \tilde{Y})$ is nonsingular in the sense that the matrix

\[
\begin{pmatrix}
2bx_5 & 2ay_5 \\
by_5 & bx_5 - ey_5
\end{pmatrix}
\]

is nonsingular (mod $p$).

Let $\tilde{X}, \tilde{Y} \in \mathbb{Z}/(p^{r+1}\mathbb{Z})$ satisfy $(\tilde{X}, \tilde{Y}) \equiv (\tilde{X}, \tilde{Y}) \pmod{p^r}$. Take $X = \tilde{X} + c_5 f_5 p^r$ and $Y = \tilde{Y} + d_5 f_5 p^r$, where $f_1$ is the vector $(1, 0, \ldots, 0)$. I will show that there is a pair $(c_1, c_2)$ that solves the equation. Since there are $p^{2n-2}$ choices for the remaining $X$ and $Y$ variables, we will eventually obtain $p^{2n-2}$ solutions.

Solving the system of equations is equivalent to solving

\[
\begin{align*}
    b(\tilde{X} + c_5 p^r f_5)^2 - a(\tilde{Y} + d_5 p^r f_5)^2 &\equiv 0 \pmod{p^{r+1}} \\
    b((\tilde{X} + c_5 p^r f_5) \cdot (\tilde{Y} + d_5 p^r f_5) + (\tilde{Y} + d_5 p^r f_5)^2 &\equiv 0 \pmod{p^{r+1}}.
\end{align*}
\]

Expanding and immediately cancelling out the $p^{2r}$ terms gives

\[
\begin{align*}
    b\tilde{X}^2 - a\tilde{Y}^2 + 2bc_5 p^r x_5 f_5 - 2ay_5 d_5 p^r f_5 &\equiv 0 \pmod{p^{r+1}}
\end{align*}
\]
\[ b\hat{X} \cdot \hat{Y} - e\hat{Y}^2 + bc_5p^r y_5 f_5 + bd_5 x_5 p^r f_5 - 2ed_5 y_5 p^r f_5 \equiv 0 \pmod{p^{r+1}}. \]

But \( \hat{X} \) and \( \hat{Y} \) are congruent to \( \tilde{X} \) and \( \tilde{Y} \) \pmod{p^r}, so \( b\hat{X}^2 - a\hat{Y}^2 \) is divisible by \( p^r \). Similarly, \( b\hat{X} \cdot \hat{Y} - e\hat{Y}^2 \) is divisible by \( p^r \). Write \( b\hat{X}^2 - a\hat{Y}^2 = sp^r \) and \( b\hat{X} \cdot \hat{Y} - e\hat{Y}^2 = tp^r \). Then the above system reduces to

\[
\begin{align*}
2bp^r x_5 c_5 - 2ap^r y_5 d_5 &\equiv -sp^r \pmod{p^{r+1}} \\
bp^r y_5 c_5 + bp^r x_5 d_5 - 2ep^r y_5 d_5 &\equiv -tp^r \pmod{p^{r+1}}.
\end{align*}
\]

But a solution to this system is equivalent to solving

\[
\begin{align*}
2bx_5 c_5 - 2ay_5 d_5 &\equiv -s \pmod{p} \\
bx_5 c_5 + bx_5 d_5 - 2ey_5 d_5 &\equiv -t \pmod{p},
\end{align*}
\]

which has at least one solution in \( c_5 \) and \( d_5 \) given the nonsingularity of \((\tilde{X}, \tilde{Y})\). Since the coordinates of \( \hat{X} \) and \( \hat{Y} \) other than the 5th one can take on any values as long as they’re congruent to \( \tilde{X} \) and \( \tilde{Y} \) \pmod{p^r}, there are \( p^{2n-2} \) solutions \pmod{p^{r+1}} corresponding to each solution \pmod{p^r}.

### 7.8 Lifting Argument for Odd Primes when \( b \) is Divisible by \( p \)

At least one of \( a \) and \( e \) is not divisible by \( p \). Assume for now that \( e \) is not divisible by \( p \).

Note that a solution to

\[
\begin{align*}
bX^2 - aY^2 &\equiv 0 \pmod{p^{r+1}} \\
bX \cdot Y - eY^2 &\equiv 0 \pmod{p^{r+1}}
\end{align*}
\]

must solve

\[
\begin{align*}
b'X^2 - a'Y^2 &\equiv 0 \pmod{p^{r+1}} \\
bX \cdot Y - eY^2 &\equiv 0 \pmod{p^{r+1}}
\end{align*}
\]

where \( b' | b, a' | a, \) and \((b', a', p) = 0\). Define \( \hat{X}, \hat{Y}, \tilde{X}, \tilde{Y}, \) and \( X \) and \( Y \) as in the previous section. If \( b' \) is not divisible by \( p \), then applying the linearization argument from the previous section gives that the system is equivalent to

\[
\begin{align*}
2b'x_5 c_5 - 2a'y_5 d_5 &\equiv -s \pmod{p} \\
-2ey_5 d_5 &\equiv -t \pmod{p}.
\end{align*}
\]
Note that any solution to the system \( (\mod p^r) \) must therefore be nonsingular since we required that \( x_5 \) and \( y_5 \neq 0 \), and the system is upper triangular. Similarly, if \( a \) is not divisible by \( p \), and \( (b',p) = 1 \), the system becomes

\[
-a'y_5d_5 \equiv -s \quad (\mod p)
\]

\[
b'x_5d_5 + b'y_5c_5 - 2e'y_5d_5 \equiv -t \quad (\mod p),
\]

Which is always solvable since the first equation depends only on \( d_5 \) and the second equation depends on both of \( c_5 \) and \( d_5 \) (noting again that \( y_5 \) is assumed to be nonzero).

So the only remaining case is when \( p \parallel b > \max(p \parallel a,p \parallel e) \). Note that this case is never going to happen if \( p = 3 \) because the local conditions prevent it. To get this case to work, we will need to modify the lifting argument somewhat.

Suppose \( p \) does not divide \( e \). Let \( p^\delta \) be the largest power of \( p \) dividing \( a \) and \( b \), and let \( b' = \frac{b}{p^\delta} \) and \( a' = \frac{a}{p^\delta} \). By assumption, \( p \) divides \( b' \) but not \( a' \). Let \( p^\gamma \) be the largest power of \( p \) dividing \( b' \), so that \( p^{\gamma + \delta} \) is the largest power of \( p \) dividing \( b \). Then we have that we wish to solve

\[
b'X^2 - a'Y^2 \equiv 0 \quad (\mod p^{r-\delta+1})
\]

\[
bX \cdot Y - eY^2 \equiv 0 \quad (\mod p^{r+1}).
\]

This system has more solutions than

\[
b'X^2 - a'Y^2 \equiv 0 \quad (\mod p^{r+1})
\]

\[
bX \cdot Y - eY^2 \equiv 0 \quad (\mod p^{r+1}).
\]

Now, let \( \hat{X}, \hat{Y}, \hat{X}, \) and \( \hat{Y} \) be as in all the other cases. If \( r < \gamma \), then the system is solved whenever \( Y^2 \) is divisible by \( p^{r+1} \), and the linearized version of this equation (following the strategy in the previous section) is solved for the correct choice of \( d_5 \). So suppose that \( r \geq \gamma \) and choose \( X = \hat{X} + c_5p^{r-\gamma}f_5 \), and \( Y = \hat{Y} + d_5p^rf_5 \). Note that \((X,Y)\) is a solution to the system \( (\mod p^r) \).

We perform the linearization as in the previous section:

\[
b'(\hat{X} + c_5p^{r-\gamma}f_5)^2 - a'(\hat{Y} + d_5p^rf_5)^2 \equiv 0 \quad (\mod p^{r+1})
\]

\[
b((\hat{X} + c_5p^{r-\gamma}f_5) \cdot (\hat{Y} + d_5p^rf_5) + (\hat{Y} + d_5p^rf_5)^2) \equiv 0 \quad (\mod p^{r+1}).
\]
Now, we expand and collect the terms in the same way, noting that $b'p^{r-\gamma}$ is divisible by $p^r$ but not $p^{r+1}$:

\[
\begin{align*}
  b'(\hat{X})^2 - a'(\hat{Y})^2 + 2b'p^{r-\gamma}x_5c_5f_5 + 2a'p^ry_5d_5f_5 &\equiv 0 \pmod{p^{r+1}} \\
  b(\hat{X}) \cdot (\hat{Y}) - e(\hat{Y})^2 + bp^{r-\gamma}y_5c_5f_5 - 2ep^ry_5d_5f_5 &\equiv 0 \pmod{p^{r+1}}.
\end{align*}
\]

Note that if $p$ divides $a$, then $b$ is divisible by $p^{\gamma+1}$ and so the $bp^{r-\gamma}y_5c_5f_5$ term drops out. Since $(\hat{X}, \hat{Y})$ solves the system $(\mod p^r)$, this system is of the form

\[
\begin{align*}
  2b''x_5c_5 - 2a'y_5d_5 &\equiv s \pmod{p} \\
  b'''y_5c_5f_5 - 2ey_5d_5f_5 &\equiv t \pmod{p}
\end{align*}
\]

for some $s$ and $t$, where $b'' := \frac{b'}{p^r}$ and $b''' = b''$ if $b = b'$ (or equivalently, if $p$ does not divide $a$, and $b''' = 0$ otherwise. If $p$ divides $a$, then the system is upper triangular and automatically nonsingular. If $p$ does not divide $a$, then the system is solvable as long as $(\tilde{X}, \tilde{Y})$ is a nonsingular solution to the system with $b$ replaced by $b''$ and $a$ replaced by $a'$.

In the case where $p$ doesn’t divide $a$ but does divide $e$, the argument is exactly the same, except with the roles of $b''$ and $b'''$ reversed.

### 7.9 The Local Factor mod 2

We seek to find odd solutions to the system

\[
\begin{align*}
  bX^2 - aY^2 &\equiv 0 \pmod{2^{r+1}} \\
  bX \cdot Y - eY^2 &\equiv 0 \pmod{2^{r+1}}.
\end{align*}
\]

The local conditions state that $a, b$ and $e$ are all maximally divisible by the same power of 2. We can therefore assume by division that each of $a, b,$ and $e$ is odd. Note that $X$ and $Y$ are of the form

\[
\begin{align*}
  X &= 2X_1 + 1 \\
  Y &= 2Y_1 + 1
\end{align*}
\]

So we want to solve

\[
\begin{align*}
  b(2X_1 + 1)^2 - a(2Y_1 + 1)^2 &\equiv 0 \pmod{2^{r+1}} \\
  b(2X_1 + 1) \cdot (2Y_1 + 1) - e(2Y_1 + 1)^2 &\equiv 0 \pmod{2^{r+1}}
\end{align*}
\]

52
Expanding gives

\[ b(4X_1^2 + 4X_1 \cdot 1 + n) - a(4Y_1^2 + 4Y_1 \cdot 1 + n) \equiv 0 \pmod{2^{r+1}} \]
\[ b(4X_1 \cdot Y_1 + 2X_1 \cdot 1 + 2Y_1 \cdot 1 + n) - e(4Y_1^2 + 4Y_1 \cdot 1 + n) \equiv 0 \pmod{2^{r+1}} \]

and combining terms gives:

\[ 4(bX_1^2 + bX_1 \cdot 1 - aY_1^2 - aY_1 \cdot 1) + n(b - a) \equiv 0 \pmod{2^{r+1}} \]
\[ 2(2bX_1 \cdot Y_1 - 2eY_1^2 + (b - 2e)Y_1 \cdot 1 + bX_1 \cdot 1) + n(b - e) \equiv 0 \pmod{2^{r+1}} \]

By the local conditions, we can assume that \( n(b - a) \) is equal to 8\( k \) for some \( k \) and that \( n(b - e) \) is equal to 2\( \ell \) for some \( \ell \). Dividing the first equation by 4 and the second equation by 2 gives

\[ bX_1^2 + bX_1 \cdot 1 - aY_1^2 - aY_1 \cdot 1 + 2k \equiv 0 \pmod{2^{r-1}} \]
\[ 2bX_1 \cdot Y_1 - 2eY_1^2 + (b - 2e)Y_1 \cdot 1 + bX_1 \cdot 1 + \ell \equiv 0 \pmod{2^r}. \]

We can only decrease the number of solutions by insisting that the first equation hold \( \pmod{2^r} \) as well. Let \( X_1 = (x_1, \ldots, x_n) \) and \( Y_1 = (y_1, \ldots, y_n) \). For now, fix all the \( X \)-coordinates and fix \( (y_6, y_7, \ldots, y_n) \).

Let \( \gamma = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5, g = y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 \), and \( h = y_1 + y_2 + y_3 + y_4 + y_5 \). We then wish to solve

\[ -ag - ah \equiv 2k' \pmod{2^r} \]
\[ (b - 2e)h + 2b\gamma - 2eg \equiv \ell' \pmod{2^r} \]

for \( g, h \), with the same parity, and \( \gamma \) with the opposite parity. Using the fact that \( a \) is odd and therefore a unit, we can solve the first equation for \( g \) to get

\[ g \equiv -h - 2a^{-1}k' \pmod{2^r} \]

which implies that \( g \) and \( h \) will have the same parity, and we solve the second equation to get

\[ (b - 2e)h + 2b\gamma - 2e(-h - 2a^{-1}k') \equiv \ell' \pmod{2^r}, \quad (7.1) \]

which is guaranteed to have a solution in \( h \) because the coefficient \( b - 4e \) on \( h \) is certainly odd. So, for any \( \gamma \), we can solve the system

\[ -ag - ah \equiv 2k' \pmod{2^r} \]
\[ (b - 2e)h + 2b\gamma - 2eg \equiv \ell' \pmod{2^r} \]
in a unique way that guarantees that \( g \) and \( h \) must have the same parity. Note that since the coefficient \( b - 4e \) of \( h \) in the equation (7.1) is always odd, and the constant being added to \( \ell' \) is always even, it follows that \( h \) will have the parity of \( \ell' \). In particular, the parity of \( h \) does not depend on the parity of \( \gamma \).

We will now show via a lifting argument that there are \( \gtrsim 2^{r(n-2)} \) solutions in \( X \) and \( Y \) to

\[
-ag - ah \equiv 2k' \quad (\text{mod } 2^r)
\]

\[
(b - 2e)h + 2b \gamma - 2eg \equiv \ell' \quad (\text{mod } 2^r).
\]

We now show that we can construct simultaneous solutions to

\[
y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 \equiv g \quad (\text{mod } 4)
\]

\[
y_1 + y_2 + y_3 + y_4 + y_5 \equiv h \quad (\text{mod } 2^r)
\]

\[
x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 \equiv \gamma \quad (\text{mod } 2^r)
\]

whenever \( g \) and \( h \) have the same parity, and \( \gamma \) has the opposite parity, such that \( x_1, x_2, x_3 \) are odd, \( x_4, x_5 \) are even (which uniquely determines these (mod 2)), and where \( y_4 \) is odd and \( y_5 \) is even (which uniquely determine \( y_4 \) and \( y_5 \) (mod 2) and \( y_1^2 \) and \( y_2^2 \) (mod 4)). We then take exactly \( g - 1 \) of \( y_1, y_2, \) and \( y_3 \) to be odd. We also take \( y_4 \) and to be odd, making the equation for \( g \) work out. Finally, since \( y_1^2 \) and \( y_2^2 \) have the same parity, it follows that \( y_1 + y_2 + y_3 + y_4 + y_5 \) must be congruent to \( h \) (mod 2), and since \( x_1y_1 + x_2y_2 + x_3y_3 \) has the same parity as \( g - 1 \), it has the opposite parity of \( h \) and therefore \( \gamma \) and \( h \) will have opposite parity.

It suffices to show that given \( g, h, \gamma \) (mod \( 2^{r+1} \)), and \( \hat{X} \) and \( \hat{Y} \) satisfying

\[
y_1^2 + y_2^2 + y_3^2 + y_4^2 + y_5^2 \equiv g \quad (\text{mod } 2^{r+1})
\]

\[
y_1 + y_2 + y_3 + y_4 + y_5 \equiv h \quad (\text{mod } 2^r)
\]

\[
x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 + x_5y_5 \equiv \gamma \quad (\text{mod } 2^r),
\]

and any \( \hat{X} \) and \( \hat{Y} \) (mod \( 2^{r+1} \)) satisfying \( \hat{X} \equiv \hat{X} \) (mod \( 2^r \)) and \( \hat{Y} \equiv \hat{Y} \) (mod \( 2^r \)), where \( y_4 \) is odd, \( y_5 \) is even, \( x_1, x_2, \) and \( x_3 \) are odd, \( x_4 \) and \( x_5 \) are even, we can select \( d_3, d_4 \) and \( d_5 \), \( Y = (y_1, y_2, y_3 + 2^r d_3, y_4 + 2^r d_4, y_5 + 2^r d_5, ) \) so that

\[
y_1^2 + y_2^2 + (y_3 + 2^r d_3)^2 + (y_4 + 2^r d_4)^2 + (y_5 + 2^r d_5)^2 \equiv g \quad (\text{mod } 2^{r+2}),
\]

\[
y_1 + y_2 + (y_3 + 2^r d_3) + (y_4 + 2^r d_4) + (y_5 + 2^r d_5) \equiv h \quad (\text{mod } 2^{r+1}),
\]

54
and

\[ x_1y_1 + x_2y_2 + x_3(y_3 + 2^r d_3) + x_4(y_4 + 2^r d_4) + x_5(y_5 + 2^r d_5) \equiv \gamma \pmod{2^{r+1}}. \]

This is good enough because there are \(2n - 5\) variables for which we can make 2 choices at each step that determine \(k\) and \(\ell\), and 2 additional variables \(y_1\) and \(y_2\) that can be chosen in any way, leading to \(\gtrsim 2^{(2n-3)r}\) solutions for a given triple \((g, h, \gamma)\), and the space of solutions to the system given a fixed \(k'\) and \(\ell'\) is a hyperplane in \(g, h, \gamma\), which has \(\frac{2^r}{2}\) solutions that satisfy the parity condition for \(\gamma\).

We do this in the following way: \(\gamma\) does not depend on \(d_4\) or \(d_5\), so select \(d_3\) to make \(x_1y_1 + x_2y_2 + x_3(y_3 + 2^{n-1} d_3) + x_4y_4 + x_5y_5 \equiv \gamma \pmod{2^{r+1}}\). Now, if \(r > 1\), the expression for \(g\) does not depend on \(d_5\), since \(y_5\) is even so \((y_5 + 2^r d_5)^2 - y_5^2\) will always be divisible by \(2^r+2\). So select \(d_4\) to make \(y_1^2 + y_2^2 + (y_3 + 2^r d_3)^2 + (y_4 + 2^r d_4)^2 + y_5^2 \equiv g \pmod{2^{r+2}}\). Finally, we select \(d_5\) to make \(y_1 + y_2 + y_3 + y_4 + y_5 + 2^r(d_3 + d_4 + d_5)\) congruent to \(h\pmod{2}\).

If instead \(r = 1\), then the roles of \(d_4\) and \(d_5\) are reversed, since if \(y_5\) is odd then \((y_5 + 2^r d_5)^2 - y_5^2\) will always be divisible by 8. So there are \(\gtrsim 2^{(n-2)r}\) values for \(x_1, \ldots, x_n, y_1, \ldots, y_n\) that satisfy

\[
\begin{align*}
  bX^2 - aY^2 &\equiv 0 \pmod{2^r} \\
  bX \cdot Y - eY^2 &\equiv 0 \pmod{2^r}.
\end{align*}
\]
Chapter 8

The Singular Integral

In this section, we wish to show, for \( q \leq (\log N)^{\frac{A}{2}} \), that the integral

\[
\int_{M(k,\ell,q)} L_n(\delta,\gamma; k,\ell, q) \, d\delta d\gamma = \int_{|\delta|,|\gamma| \leq \frac{N^2}{q\log N}} \int_{X,Y} e((\delta(b(X)^2 - a(Y)^2)) \cdot e(\gamma(bX \cdot Y - eY^2)) \cdot \chi \left( \frac{X}{N} \right) \chi \left( \frac{Y}{N} \right)
\]

converges to some nonzero value \( L \) that is independent of \( q \), and that for \( (\log N)^{\frac{A}{2}} < q < (\log N)^{A} \), the difference between

\[
\int \int_{M_{K,\ell,q}} \sum_{(k,\ell,q)=1} K_n(k,\ell,q) L(\delta,\gamma; k,\ell, q)
\]

and \( L \sum_{(k,\ell,q)=1} K_n(k,\ell,q) \) is negligible. We follow the strategy used in [1]. In particular, we first show that, where \( L(\delta,\gamma) \) is the integral for \( x \) and \( y \) each single-dimensional variables in \( \mathbb{R} \),

**Lemma 8.0.1.**

\[
L(\delta,\gamma) \lesssim \frac{N^2 \log(N)}{1 + N^2(|\delta| + |\gamma|)}.
\]

**Proof.** We start by making a change of variables to replace \( \frac{x}{N} \) and \( \frac{y}{N} \) by \( x \) and \( y \). Then

\[
L(\delta,\gamma) = N^2 \int_{x,y} e \left( N^2(\delta(b(x)^2 - a(y)^2) + \gamma(bxy - e(y)^2)) \right) \chi(x)\chi(y) \, dx \, dy
\]

We consider \( |L(\delta,\gamma)|^2 = L(\delta,\gamma) \overline{L(\delta,\gamma)} \). Then

\[
|L(\delta,\gamma)|^2 = N^4 \int_{x,y,x',y'} e \left( N^2\delta b((x')^2 - x^2) - a((y')^2 - y^2) \right) \cdot e \left( N^2\gamma(b((x')(y') - xy) - e((y')^2 - y^2)) \right) \cdot \chi(x)\chi(y) \, dx \, dy \, dx' \, dy'
\]
Now, write \( u = x' - x \), \( v = y' - y \). Then this integral is equal to

\[
N^4 \int_{x,y,u,v} e \left( N^2 (\delta(b(u(u + 2x)))) \right) \\
\cdot e \left( N^2 (\delta(a(v + 2y))) \right) \\
\cdot e \left( N^2 (\gamma(b(v + (x + u)y + (y + v)x - 2xy))) \right) \\
\cdot e \left( N^2 (\gamma(-e(v(v + 2y))) \right) \chi(x) \chi(y) \\ dx dy du dv 
\]

\[
= N^4 \int_{u,v} e \left( (N^2(\delta(bu^2 - av^2) + \gamma(buv - ev^2))) \right) \\
\cdot \int_{x,y} e \left( N^2(\delta(2bux - 2avy)) \right) \\
\cdot e \left( N^2\gamma(buy + bxv - 2evy) \right) \chi(x) \chi(y) \\ dx dy du dv.
\]

As with the singular series, we use the triangle inequality:

\[
\leq N^4 \int_{u,v} \left| \int_{x,y} e \left( N^2(\delta(2bux - 2avy)) \right) \\
\cdot e \left( N^2\gamma(buy + bxv - 2evy) \right) \chi(x) \chi(y) \\ dx dy \right| du dv.
\]

Now let \( u' \) be the coefficient of \( x \) and let \( v' \) be the coefficient of \( y \). Then we can split the inner integral into the product of two integrals of the form \( \int e(tx)\chi(x)dx \). Note that by the triangle inequality each of these two integrals is at most 2, and by directly carrying out the integration, it follows that each integral is bounded above by a constant over \( t \). So, in particular, we have that \( \int e(tx)\chi(x)dx \lesssim \frac{1}{1 + t} \). Therefore, we have that

\[
\int_{x,y} e \left( N^2(\delta(2bux - 2avy) + \gamma(buy + bxv - 2evy)) \right) dx dy \\
\lesssim \frac{1}{1 + N^2|u'|} \frac{1}{1 + N^2|v'|}
\]

Now, we try to count the measure of the set where \( u' \) and \( v' \) are of a given size. Since \( u \) and \( v \) are less than 2, and \( a,b,e \) are all constants, it follows that \( u' \) and \( v' \) are each bounded above by some constant \( c \). Split the box \([-c,c] \times [-c,c]\) into \( \frac{N}{2} \) blocks of side length \( \frac{N^2}{2} \). We want to get an estimate on the measure of the \((u,v)\) that correspond to \((u',v')\) in each block \( B_{i,j} \). Fix \((u_1, v_1)\) such that \((u'_1, v'_1)\) is in \( B_{i,j} \). Then by linearity, if \((u_2, v_2)\) such that \((u'_2, v'_2)\) is in \( B_{i,j} \), then it follows that \((u_1 - u_2, v_1 - v_2)\) satisfies \(|(u_1 - u_2)'| \leq \frac{1}{N^2} \), and \(|(v_1 - v_2)'| \leq \frac{1}{N^2} \). So therefore the measure of
the set of \((u, v)\) such that \((u', v')\) is in \(B_{ij}\) is bounded above by the measure of the set \(B\), where \(B\) is the set of \((u, v)\) for which \(|u'| \leq \frac{1}{N^2}\) and \(|v'| \leq \frac{1}{N^2}\).

So, we have that

\[
L(\delta, \gamma)^2 \lesssim N^4 \sum_{0 \leq s \leq N^2} \sum_{0 \leq t \leq N^2} \frac{1}{1 + s} \frac{1}{1 + t} \text{meas}(B) \lesssim N^4 \log^2(N) \text{meas}(B).
\]

So all we need to do now is estimate \(\text{meas}(B)\). But \(|u'|\) is always at least a constant times \(\max(|\gamma u|, |\delta v|)\), and \(|v'|\) is always at least a constant times \(\max(|\gamma v|, |\delta u|)\), so it follows that \(|(u', v')| \gtrsim |u'| + |v'| \gtrsim (|\delta| + |\gamma|) \max(u, v)\)

So,

\[
\text{meas}(B) \lesssim \text{meas}\left(\{(u, v) : \max(u, v) \leq \frac{1}{N^2} (|\delta| + |\gamma|)\}\right),
\]

because if \(|(u', v')|\) is smaller than \(\frac{1}{N^2}\) then \(\max(|u'|, |v'|) < \frac{1}{N^2}\). But the above expression is

\[
\lesssim \frac{1}{N^4(|\delta| + |\gamma|)^2}.
\]

So,

\[
L(\delta, \gamma) \lesssim \frac{N^2 \log(N)}{N^2(|\delta| + |\gamma|)}.
\]

But we also know trivially that \(|L(\delta, \gamma)|^2 < N^4\), so combining these estimates gives

\[
L(\delta, \gamma) \lesssim \frac{N^2 \log(N)}{1 + N^2(|\delta| + |\gamma|)}.
\]

as desired. \(\square\)

The next step is to extend the integral in \(\delta\) and \(\gamma\) to all of \(\mathbb{R}^2\) with a small error. In other words, we want to calculate

\[
\int \int_{|\gamma| + |\delta| \geq N^{-2} \log N} |L(\delta, \gamma)|^n - \int \int_{|\gamma| + |\delta| < N^{-2} \log N} |L(\delta, \gamma)|^n \, d\gamma d\delta
\]

\[
= \int \int_{|\gamma| + |\delta| \geq N^{-2} \log N} |L(\delta, \gamma)|^n \, d\gamma d\delta
\]

\[
\leq (\log N)^n \int \int_{|\gamma| + |\delta| \geq N^{-2} \log N} \left(\frac{1}{|\gamma| + |\delta|}\right)^n \, d\gamma d\delta
\]

\[
= 4(\log N)^n \int \int_{|\gamma| + |\delta| \geq N^{-2} \log N} \left(\frac{1}{|\gamma| + |\delta|}\right)^n \, d\gamma d\delta
\]

58
\[
= 4(\log N)^n \int_{u=N^{-2q-1}(\log N)^A}^{\infty} \int_{\delta=0}^{u} \left(\frac{1}{u}\right)^n d\delta du \\
= 4(\log N)^n \int_{u=N^{-2q-1}(\log N)^A}^{\infty} u^{-n-1} du \\
= \frac{4}{n-2}(\log N)^n N^{2n-4}q^{n-2}(\log N)^A(-n+2) \\
\lesssim N^{2n-4}(\log N)^{n-\frac{A}{2}(n-2)},
\]
if \( q < (\log N)^{\frac{A}{2}} \). But we have from the singular series bound that
\[
\sum_{(k,\ell,q)=1}^{q>(\log N)^{\frac{A}{2}}} |K_n(k,\ell,q)| \lesssim \sum_{q>(\log N)^{\frac{A}{2}}} q^{-\frac{3}{2}} \lesssim (\log N)^{-\frac{A}{4}},
\]
so the total contribution from extending the integral in \( \delta \) and \( \gamma \) for all the \( (k,\ell,q) \) where \( q \) is at least \( (\log N)^{\frac{A}{2}} \) is bounded above by
\[
\lesssim N^{2n-4}(\log N)^{n-\frac{A}{4}}.
\]
Therefore, we can extend the integral in \( \gamma \) and \( \delta \) to all of \( \mathbb{R}^2 \) with an error term that is smaller than the main term, which will be \( O(N^{2n-4}) \). This leaves us with the following integral:
\[
\int_{\delta,\gamma} \int_{XY} e \left( (\delta(b(X)^2 - a(Y)^2) + \gamma(bX \cdot Y - eY^2)) \right) \\
\cdot \chi \left( \frac{X}{N} \right) \chi \left( \frac{Y}{N} \right) dXdY.
\]
Note that by the estimate in the previous lemma, this integral is absolutely convergent. We are therefore free to rearrange the integrals however we want. Note that the integral is unaffected by removing the hyperplane where \( x_1 = 0 \). We then split the \( \mathbb{R}^{2n} \) without this hyperplane into two half-spaces, \( H \) and \( G \), where \( H \) is the halfspace where \( x_1 > 0 \) and \( G \) is the halfspace where \( x_1 < 0 \), and write the integral as a sum of the integral over \( H \) and the integral over \( G \). Since the function we’re integrating is even (in the sense that plugging in \((-X,-Y)\) always yields the same value as plugging in \((X,Y)\), we know that
\[
\int_{\delta,\gamma} \int_{(X,Y)\in \mathbb{R}^{2n}} e \left( (\delta(b(X)^2 - a(Y)^2) + \gamma(bX \cdot Y - eY^2)) \right)
\]
\[
\cdot \chi \left( \frac{X}{N} \right) \cdot \chi \left( \frac{Y}{N} \right) dX dY
\]

\[
= 2 \int \int \int_{(X,Y) \in H} e \left( (\delta(bX)^2 - a(Y)^2) + \gamma(bX \cdot Y - eY^2) \right) \\
\cdot \chi \left( \frac{X}{N} \right) \cdot \chi \left( \frac{Y}{N} \right) dX dY
\]

We make the following change of variables in this integral: Send the vector \((X,Y)\) to \((U,V)\) where

\[
U = (u_1, u_2, \ldots, u_n) := (bX^2 - aY^2, x_2, x_3, \ldots, x_n)
\]

\[
V = (v_1, v_2, \ldots, v_n) := (bX \cdot Y - eY^2, y_2, y_3, \ldots, y_n).
\]

First, I will verify that this change of variables is injective on each of \(G\) and \(H\), and, for any selection of \(u_2, \ldots, u_n, v_2, \ldots, v_n\) "misses" only a ray in the \((u_1, v_1)\)-plane. Fix \(x_2, \ldots, x_n\), and \(y_2, \ldots, y_n\). Then, we want to solve the equations

\[
bX^2 - aY^2 = u_1
\]

\[
bX \cdot Y - eY^2 = u_2
\]

for \(x_1\) and \(y_1\). Moving all the other components of \(X\) and \(Y\) to the other side, we want to solve a system of the form

\[
\sqrt{bx} = \sqrt{C_1 + ay^2}.
\]

For convenience, we will now replace \(x_1\) by \(x\) and \(y_1\) by \(y\). I will begin by checking the case where \(C_1\) is nonnegative. Then, we have (remembering that we’re looking for solutions in the half-plane where \(x\) is nonnegative, but it doesn’t matter whether we’re in \(G\) or \(H\) since this term will be squared anyway)

\[
\sqrt{bx} = \sqrt{C_1 + ay^2}.
\]

This will be strictly positive unless \(C_1\) and \(y\) are both equal to zero. Upon substituting this into the other equation, we get

\[
\sqrt{by}\sqrt{C_1 + ay^2} - ey^2 = C_2
\]

\[
by^2(C_1 + ay^2) = (ey^2 + C_2)^2
\]

\[
bC_1y^2 + ab(y^2)^2 = e^2(y^2)^2 + 2eC_2y^2 + C_2^2
\]
\[ 0 = (ab - e^2)(y^2)^2 + (bC_1 - 2eC_2)y^2 - C_2^2. \]

We then use the quadratic formula:
\[
y^2 = \frac{2eC_2 - bC_1 \pm \sqrt{(bC_1 - 2eC_2)^2 + 4(ab - e^2)C_2^2}}{2(ab - e^2)}.
\]

But our condition on \(a, b,\) and \(e\) implies that \(ab - e^2\) is always positive. So, as long as \(C_2\) is nonzero, we have that \(\sqrt{(bC_1 - 2eC_2)^2 + 4(ab - e^2)C_2^2} > |2eC_2 - bC_1|,\) so exactly one of the possible values for \(y^2\) is positive. If \(C_2\) is zero, then one of the possible values for \(y^2\) will be zero and the other one will be negative, again allowing for only one plausible value for \(y^2\). Furthermore, since \(x\) was assumed to be nonzero, if \((x, y)\) is a solution of \(bxy - ey^2 = C_2,\) then \(-y\) will not be a solution, so the system of equations has exactly one real solution satisfying \(x > 0\) as long as \(C_1\) is nonnegative and \(C_2\) is nonzero, or if \(C_1\) is positive regardless of the sign of \(C_2.\)

If \(C_1\) is negative, then \(bx^2 - C_1\) is positive, so it makes sense to write that
\[
y = \pm \frac{1}{\sqrt{a}} \sqrt{bx^2 - C_1},
\]

since \(bx^2 - C_1\) is a nonnegative number. So we want to solve
\[
\pm \frac{bx}{\sqrt{a}} \sqrt{bx^2 - C_1} - \frac{e(bx^2 - C_1)}{a} = C_2
\]
\[
\pm \frac{bx}{\sqrt{a}} \sqrt{bx^2 - C_1} = C_2 + \frac{be}{a} x^2 - \frac{eC_1}{a}
\]
\[
\frac{b^2 x^2}{a} (bx^2 - C_1) = \left( C_2 + \frac{be}{a} x^2 - \frac{eC_1}{a} \right)^2
\]
\[
\frac{b^3 (x^2)^2}{a} - \frac{b^2 C_1 x^2}{a} = \frac{e^2 b^2}{a^2} (x^2)^2 + 2(C_2 - \frac{eC_1}{a}) \frac{be x^2}{a} + (C_2 - \frac{eC_1}{a})^2
\]

So, multiplying both sides by \(a^2\) gives
\[
ab^3 (x^2)^2 - ab^2 C_1 x^2 = e^2 b^2 (x^2)^2 + 2(aC_2 - eC_1) be x^2 + (aC_2 - eC_1)^2
\]

Then, we solve for \(x^2\) using the quadratic formula:
\[
x^2 = \frac{ab^2 C_1 + 2(aC_2 - eC_1) be}{2(ab^3 - e^2 b^2)}
\]
\[
\pm \frac{\sqrt{(-ab^2 C_1 - 2(aC_2 - eC_1) be)^2 + 4(ab^3 - e^2 b^2)(aC_2 - eC_1)^2}}{2(ab^3 - e^2 b^2)}.
\]
Here, we notice that \(4ab^3 - e^2b^2\) is nonnegative since \(e^2 < ab\). So the square root term is larger in magnitude than the other term in the numerator as long as we don’t have \(aC_2 = eC_1\), meaning that there is exactly one possible value for \(x^2\). If \(aC_2 = eC_1\), then one of the roots is zero, and the other root is \(ab^2C_1\), which is negative because we were operating under the assumption that \(C_1\) was negative. So the system

\[
\begin{align*}
  bx^2 - ay^2 &= C_1 \
  bxy - ey^2 &= C_2
\end{align*}
\]

will always have exactly one real solution with \(x > 0\) unless \(aC_2 = eC_1\) where \(C_1 < 0\). That is, for a fixed \(u_2, \ldots, u_n, v_2, \ldots, v_n\), we hit each point \((U, V)\) except for a ray depending on \(u_2, \ldots, u_n, v_2, \ldots, v_n\) exactly once when \(x_1 > 0\) and exactly once when \(x_1 < 0\). The Jacobian matrix \(J(X, Y)\) for the has the following form (when the \(X\) and \(Y\) variables are arranged in the order \((x_1, y_1, x_2, y_2, \ldots, x_n, y_n)\):

\[
J(X, Y) = \begin{pmatrix}
  2bx_1 - 2ay_1 & 0 & \cdots & 0 \\
  by_1 & bx_1 - 2ey_1 & 0 & \cdots & 0 \\
  J_0 & & & & \\
  & & & & \\
  & & & & \end{pmatrix},
\]

So the Jacobian determinant \(|J(X, Y)|\) is the value

\[
2b^2x_1^2 - 4be x_1 y_1 + 2aby_1^2
\]

Since we’re looking at the hyperplane where \(x_1\) is positive, we know that if \(y_1\) is nonpositive then this quantity will be (strictly) positive. So we need only consider the case where \(y_1\) is strictly positive.

We factor out a \(2b\) from the Jacobian determinant:

\[
2b(bx_1^2 - 2ex_1y_1 + ay_1^2)
\]

However, we assumed that \(e < \sqrt{ab}\), so the above expression is strictly larger than

\[
2b(bx_1^2 - 2\sqrt{ab} x_1 y_1 + ay_1^2) = 2b(\sqrt{bx_1} - \sqrt{ay_1})^2,
\]

which is nonnegative. Therefore, as long as we’re not on the hyperplane where \(x_1\) is zero, the Jacobian determinant for this change of variables is
strictly positive. Therefore, since the determinant of this Jacobian is positive everywhere except on the hyperplane $H$ where $x_1$ is equal to zero, $|J^{-1}(U,V)|$ is well-defined and positive. So we make the change of variables in our integral to get

$$2 \int_{\mathbb{R}^2} \int_{(X,Y) \in H} e(\delta u_1 + \gamma v_1) \rho(u_1, U', v_1, V') \, dUdV \, d\delta d\gamma,$$

where $\phi$ is the transformation representing the change of variables, $\rho$ is the nonnegative function $\chi(\phi^{-1}(U,V))|J(U,V)|^{-1}$, and $U'$ and $V'$ are the vectors $(u_2, \ldots, u_n)$ and $(v_2, \ldots, v_n)$. Now, it suffices to show that by excluding the places where $x_1 = 0$, haven’t excluded much of the integral in $u_1$ and $v_1$. In other words, let’s fix $U'$ and $V'$, and see which values for the vector $(u_1, v_1)$ we exclude by forcing $x_1$ to be nonzero. Then

$$u_1 = bx_1^2 - ay_1^2 + C_1$$
$$v_1 = bx_1 y_1 - ey_1^2 + C_2.$$

So, the set of points we get when $x_1 = 0$ is the line

$$(-ay_1^2 + C_1, -ey_1^2 + C_2).$$

Note that this ray is a set of measure zero in the $(u_1, v_1)$ plane. In other words, removing this ray never affects the integral in $(u_1, v_1)$, regardless of the other coordinates of $U$ and $V$. But the integral in $u_1$ and $v_1$ is the Fourier transform of $\rho$ in the $u_1$ and $v_1$ variables. So the above integral comes out to

$$2 \int_{\mathbb{R}^{2n-2}} \int_{\mathbb{R}^2} \tilde{\rho}(\delta, U', \gamma, V') \, d\delta d\gamma \, dU' \, dV'.$$

By the Fourier inversion theorem, this is equal to

$$2 \int_{\mathbb{R}^{2n-2}} \rho(0, U', 0, V') \, dU' \, dV'.$$

But $\rho(0, U', 0, V')$ is strictly positive at any point $U', V'$ for which there exists a positive $x_1$ and a real $y_1$ such that $(x_1, U')$ and $(y_1, V')$ satisfy the equations

$$bX^2 - aY^2 = 0$$
$$bX \cdot Y - eY^2 = 0.$$

Since $\rho$ is continuous and nonnegative, and since we know by the result in [1] that that $a, b$, and $e$ correspond to the squares of the side lengths of a triangle with rational coordinates, it follows that these equations have at least one solution with $x_1 > 0$, and therefore the singular integral is positive since the integrand must be strictly positive on some open set.
Bibliography


Appendix A

Changing the Von Mangoldt Factors to Logarithmic Factors

We want to make the change from evaluating

$$\sum_{|X|,|Y| \leq N} \Lambda(X)\Lambda(Y)\chi(X,Y)$$

where $\chi$ is the indicator function for the $X$ and $Y$ satisfying

$$bX^2 - aY^2 = 0$$
$$bX \cdot Y - eY^2 = 0.$$

We want to change the $\Lambda$ functions into logarithm functions times the indicator of the primes. To do this, we note that the sum of $\log p^k$ over all prime powers $p^k$ less than or equal to $N$ is at most $O(N^{\frac{3}{2}}(\log N)^A)$ for some $A$. So

$$\sum_{|X|,|Y| \leq N} \Lambda(X)\Lambda(Y)\chi(X,Y)$$
$$= \sum_{|X|,|Y| \leq N, x_1 \text{ prime}} \log(x_1)\Lambda(x_2, \ldots, x_n)\Lambda(Y)\chi(X,Y)$$
$$+ O \left( N^{\frac{3}{2}}(\log N)^A \right) \max_{k,\ell} \sum_{|X'|,|Y'| \leq N} \Lambda(X')\Lambda(Y')\chi_{k,\ell}(X',Y')$$

We now trivially estimate the Von Mangoldt factors in the error term by a large power of $\log N$.

$$= \sum_{|X|,|Y| \leq N, x_1 \text{ prime}} \log(x_1)\Lambda(x_2, \ldots, x_n)\Lambda(Y)\chi(X,Y)$$
$$+ O \left( N^{\frac{3}{2}}(\log N)^B \right) \max_{k,\ell} \sum_{|X'|,|Y'| \leq N} \chi_{k,\ell}(X',Y').$$
Now we apply the result in Appendix C to the sum in the error term. So the order of the sum is $N^{2(n-1)-4} = N^{2n-6}$. So the error term is $O(N^{2n-6}(\log N)^B)$, which is smaller than the main term. We apply the same estimate in each of the other variables to change from estimating Von Mangoldt factors to estimating the logarithm function applied to the primes.
Appendix B

Eliminating the Logarithmic Factors from the Sum

We now have an asymptotic estimate for the number of prime solutions to the system

\[ bX^2 - aY^2 = 0 \]
\[ bX \cdot Y - eY^2 = 0 \]

when weighted by the logarithmic factors. We now seek to obtain an asymptotic the logarithmic weights by the following method: We start with the sum

\[ \sum_{|X|,|Y| \leq N} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi(X, Y) = C N^{2n-4}, \]

where \( \chi(X, Y) \) is the indicator that \( X \) and \( Y \) solve the system. We cut the sum off at \( \frac{N}{(\log N)^A} \), where \( A \) is a dimension-dependent power that will be determined later:

\[ \sum_{\substack{X, Y \leq N \\\text{prime} \\\text{or}\\\text{prime}}} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi(X, Y) \]
\[ + \sum_{\frac{N}{(\log N)^A} \leq X, Y \leq N} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi(X, Y) = C N^{2n-4}. \]

Note that if \( X \) and \( Y \) are not pointwise greater than \( \frac{N}{(\log N)^A} \), then there is (at least) one coordinate \( x_j \) or \( y_j \) such that \( x_j < \frac{N}{(\log N)^A} \) or \( y_j < \frac{N}{(\log n)^A} \). Assume this coordinate is \( x_1 \). Then, after losing a factor of \( 2n \) (since there are \( 2n \) possible variables that could be less than \( (\log N)^A \)), the first sum is
bounded above by

\[
\sum_{X, Y \leq N \atop \text{prime}} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi(X, Y)
\]

\[\leq \sum_{X' \leq N \atop \text{prime}} \sum_{Y' \leq N} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi((x, X'), Y).
\]

Now, we apply a trivial estimate to the sum in \(x_1\) and \(y_1\), as well as all of the logarithm factors appearing in the sum:

\[
\leq \frac{N^2}{(\log N)^4} (\log N)^{2n} \max_{c_1, c_2} \left( \sum_{X' \text{prime}} \sum_{Y' \text{prime}} \chi_{c_1, c_2}(X', Y') \right)
\]

where \(\chi_{c_1, c_2}(X', Y')\) is the indicator for solutions to

\[
\begin{align*}
bX^2 - aY^2 &= c_1 \\
bX \cdot Y - eY^2 &= c_2.
\end{align*}
\]

Removing the restrictions in the sum that force \(X'\) and \(Y'\) to be prime can only make the sums bigger:

\[
\leq \frac{N^2}{(\log N)^4} (\log N)^{2n} \max_{c_1, c_2} \left( \sum_{X' \leq N} \sum_{Y' \leq N} \chi_{c_1, c_2}(X', Y') \right).
\]

We then use the result in Appendix C to conclude that the above sum is

\[
\lesssim \frac{N^{2n-4}}{(\log N)^{A-2n}}.
\]

Now, the other sum will become the main term.

\[
\sum_{N \atop \text{prime}} \prod_{i=1}^{n} \prod_{j=1}^{n} \log(x_i) \log(y_j) \chi(X, Y).
\]

68
We estimate each logarithmic factor by $\log N$. The error in this estimate in each factor will be at most a constant times $\log \log N$.

$$=(\log N)^{2n} \sum_{\substack{N \leq X,Y \leq N \\ X,Y \text{ prime}}} \chi(X,Y)$$

$$+O((\log N)^{2n-1} \log \log N) \sum_{\substack{N < X,Y \leq N \\ X,Y \text{ prime}}} \chi(X,Y)$$

$$=(1+o(1))(\log N)^{2n} \sum_{\substack{N < X,Y \leq N \\ X,Y \text{ prime}}} \chi(X,Y).$$

So, if we select $A = 2n + 1$, we get that

$$\sum_{\substack{N \leq X,Y \leq N \\ X,Y \text{ prime}}} \chi(X,Y) \sim \frac{CN^{2n-4}}{(\log N)^2 n}. $$

The sum of the remaining terms without the logarithmic factor will be bounded above by the sum of the remaining terms with the logarithmic factor, which we showed to be smaller than the main term. So

$$\sum_{\substack{X,Y \leq N \\ X,Y \text{ prime}}} \chi(X,Y) \sim \frac{CN^{2n-4}}{(\log N)^2 n}.$$
Appendix C

The Number of Solutions to a Modified System

In this appendix, we show that the number of integer solutions to the system of equations

\[
\begin{align*}
    bX^2 - aY^2 &= c_1 \\
    bX \cdot Y - eY^2 &= c_2
\end{align*}
\]

is bounded above by \( CN^{2n-4} \), where \( C \) is a constant depending on \( a, b, \) and \( e \) but not on \( c_1 \) or \( c_2 \). We can use most of [1] verbatim, but a few tiny modifications need to be made to some of the arguments in this slightly more general setting.

The integral we are trying to estimate is slightly different from the one in [1]:

\[
\int_0^1 \int_0^1 e\left( -c_1 \alpha - c_2 \beta \right) \left( \sum_{|x|,|y| \leq N} e\left( \alpha (bx^2 - ay^2) + \beta (bxy - ey^2) \right) \right)^n \, d\alpha \, d\beta.
\]

However, since the minor arc estimates in [1] involve an immediate invocation of the triangle inequality, the extra \( e(-c_1 \alpha - c_2 \beta) \) term in my integral immediately drops out and the minor arc estimates are exactly the same. So it is only necessary to check that the major arc estimates work in almost the same way as in [1].

The decomposition of the major arcs into the singular series and the singular integral is almost exactly the same: The terms in the singular series are now

\[
K_n(k, \ell, q) = \frac{1}{q^{2n}} e\left( -c_1 \frac{k}{q} - c_2 \frac{\ell}{q} \right) \sum_{S,T} e\left( \frac{kbS^2 + \ell bS \cdot T - (ka + \ell e)T^2}{q} \right),
\]
where the sum over $S$ and $T$ is taken mod $q$, and the singular integral is now
\[ L(\delta, \gamma, k, \ell, q) = e(-c_1 \delta - c_2 \gamma) \int_{X,Y} \exp(2\pi i \phi(X, Y)) \chi \left( \frac{X}{P} \right) \chi \left( \frac{Y}{P} \right) dX dY. \]

Because only an upper bound is necessary, there is no need to show that the singular series or singular integral is nonzero.

The bounds in [1] on $K(k, \ell, q)$ (using the definition of $K(k, \ell, q)$ given in [1]) are exactly the same. Since the bounds on $K_n(q)$ that are used to show the convergence of the sum depend only on the absolute value of $K_n(k, \ell, q)$, which hasn’t changed here since we only multiplied by a unit complex number, it follows that the singular series has the same termwise upper bound as in [1], and therefore the singular series is bounded above by a constant not depending on $c_1$ or $c_2$.

As for the singular integral, the extension of the integral in $\delta$ and $\gamma$ to all of $\mathbb{R}$ works out in the same way as in [1] (for which the singular integral is the same as the singular integral in this paper). We make the same change of variables as in [1]. The only difference is that, in the last step, when we apply the Fourier inversion theorem, we arrive at the expression
\[ \rho \left( \frac{c_1}{N^2}, U', \frac{c_2}{N^2}, V' \right). \]

Since the system will never have any solutions unless $c_1$ and $c_2$ are bounded above by a dimension-dependent constant times $N$, it follows that this is bounded above by the maximum of $\rho$ on a compact set not depending on $c_1$ and $c_2$, and therefore the constant arising from the singular integral does not depend on $c_1$ and $c_2$. Therefore, the number of solutions to the system
\[
\begin{align*}
  bX^2 - aY^2 &= c_1 \\
  bX \cdot Y - cY^2 &= c_2
\end{align*}
\]
is bounded above by $CN^{2n-4}$, where $C$ is a constant that does not depend on $c_1$ or $c_2$. 

71
Appendix D

Program for Testing Prime Moduli Between 5 and 19

The computation performed by the following program is referenced in the section "Some Results for Small moduli."

```java
import java.util.Scanner;
/*This program calculates the possible vector sums
 * (x_1r_1+x_2 r_2+x_3r_3+x_4r_4,r_1^2+r_2^2+r_3^2+r_4^2)
 * and prints out the values for x_j that don't give a
 * complete list. This only works for prime moduli and
 * should be used only for primes that are at most 19.
 * /
public class BruteForceSmallModulus {
public static void main(String[] args){
 //select a modulus
 Scanner scanner = new Scanner(System.in);
 System.out.println("Which modulus would you like to test?");
 int modulus = scanner.nextInt();
 //make a list of (r, r^2) mod p
 int[][] qrs = new int[modulus - 1][2];
 boolean modulusok = true;
 for(int i=0; i< modulus - 1; i++) {
 qrs[i][0] = i + 1;
 qrs[i][1] = ((i+1) * (i+1))%modulus;
 }
 //initialize the list of vectors
 int[][]vectorlist = qrs;
 for(int x1 = 1; x1 < modulus; x1++) {
 for(int x2 = 1; x2 < modulus; x2++) {
 for(int x3 = 1; x3 < modulus; x3++) {
 for(int x4 = 1; x4 < modulus; x4++) {
 //initialize the list of vectors
```
vectorlist = qrs;
// multiply the first term of each vector by x_1
// make vectorlist point to a different array
vectorlist = mult(vectorlist, x1, modulus);
// add (x_2 r_2, r_2^2) for every r_2
vectorlist = vecsums(vectorlist, qrs, modulus, x2);
// add (x_3 r_3, r_3^2) for every r_3
vectorlist = vecsums(vectorlist, qrs, modulus, x3);
// add (x_4 r_4, r_4^2) for every r_4
vectorlist = vecsums(vectorlist, qrs, modulus, x4);
// test to see if the list of vectors is complete
if(vectorlist.length < modulus * modulus) {
    if(true == modulusok) {
        System.out.println("Here are the bad values:");
        modulusok = false;
    }
    System.out.print(x1);
    System.out.print(x2);
    System.out.print(x3);
    System.out.println(x4);
}
// output current progress
System.out.println("Progress:");
System.out.println(x1 + " out of " + (modulus - 1));
}
// produce output if every quadruple works
if(true == modulusok) {
    System.out.println("There are no problems mod " + modulus);
}
/* Create a list of sums of 2 vectors in a list of vectors
   * multiplying the first component of the vectors in the
   * second list by x*/
static int[][] vecsums(int[][] in1, int[][] in2, int p, int x){
    int[][] preout = new int[in1.length * in2.length][2];
    // list (v_1 + x_2 v_2, v_1 + v_2)
    for(int i = 0; i < in1.length; i++) {
for(int j = 0; j < in2.length; j++) {
preout[i * in2.length + j][0] = (in1[i][0] + x*in2[j][0]) % p;
preout[i * in2.length + j][1] = (in1[i][1] + in2[j][1]) % p;
}

//eliminate redundancies in the list
int[][] out = eliminate(preout, p);
return out;

/*eliminate redundancies in a list of vectors*/
public static int[][] eliminate(int[][] input, int modulus) {
    //initialize
    boolean[][] inset = new boolean[modulus][modulus];
    for(int i=0; i< modulus; i++) {
        for(int j = 0; j< modulus; j++) {
            inset[i][j] = false;
        }
    }
    //mark the elements in the set
    for(int i= 0; i< modulus; i++) {
        for(int j = 0;j < modulus; j++) {
            for(int k = 0; k < input.length; k++) {
                if(input[k][0] == i && input[k][1] == j) {
                    inset[i][j] = true;
                }
            }
        }
    }
    //determine the length of the output
    int size = 0;
    for(int i = 0; i< modulus; i++) {
        for(int j = 0; j< modulus; j++) {
            if(inset[i][j] == true) {
                size ++;
            }
        }
    }
    //include one copy of each vector in the list
    int index= 0;
    int[][] out = new int[size][2];
for(int i = 0; i< modulus; i++) {
    for(int j = 0; j< modulus; j++) {
        if(inset[i][j] == true) {
            out[index][0] = i;
            out[index][1] = j;
            index++;
        }
    }
}
return out;

/*Multiplies the first term of a vector by x*/
public static int[][] mult(int[][] input, int x, int modulus) {
    //initialize
    int[][] out = new int[input.length][2];
    for(int i = 0; i< out.length; i++) {
        out[i][0] = input[i][0];
        out[i][1] = input[i][1];
    }
    // multiply the first term by x
    for(int i=0; i<input.length; i++) {
        out[i][0] = input[i][0] * x % modulus;
    }
    return out;
}
Appendix E

Program for Testing the Value 3

The computation performed by the following program is referenced in the section "Some Results for Small moduli."

/*This program shows the existence of solutions mod 9*/
public class BruteForceNine {
    public static void main(String[] args) {
        System.out.println("Here are the bad values mod 9.");
        //set the modulus to 9
        int modulus = 9;
        int[][] qrs = new int[6][2];
        int count = 0;
        for(int i=0; i< 6; i++) {
            //skip over multiples of 3
            if(count % 3 == 2) {
                count++;
            }
            //find (r, r^2) mod 9
            qrs[i][0] = count + 1 % modulus;
            qrs[i][1] = ((count + 1) * (count +1)) % modulus;
            count++;
        }
        //initialize the list of sums
        int[][] vectorlist = qrs;
        for(int x1 = 1; x1 < modulus; x1++) {
            for(int x2 = 1; x2 < modulus; x2++) {
                for(int x3 = 1; x3 < modulus; x3++) {
                    for(int x4 = 1; x4 < modulus; x4++) {
                        //initialize the sums
                        vectorlist = qrs;
// multiply linear term by \( x_1 \)
// make vectorlist point to a different array
vectorlist = multiply(vectorlist, x_1, modulus);
// add \((\mathbf{x}_2 \mathbf{r}_2, \mathbf{r}_2^2)\) for every \(\mathbf{r}_2\)
vectorlist = vecsums(vectorlist, qrs, modulus, x_2);
// add \((\mathbf{x}_3 \mathbf{r}_3, \mathbf{r}_3^2)\) for every \(\mathbf{r}_3\)
vectorlist = vecsums(vectorlist, qrs, modulus, x_3);
// add \((\mathbf{x}_4 \mathbf{r}_4, \mathbf{r}_4^2)\) for every \(\mathbf{r}_4\)
vectorlist = vecsums(vectorlist, qrs, modulus, x_4);
// Print out \((\mathbf{x}_1, \mathbf{x}_2, \mathbf{x}_3, \mathbf{x}_4)\) that
// don’t yield a complete list for
// \((\mathbf{x}_1\mathbf{r}_1 + \ldots + \mathbf{x}_4\mathbf{r}_4, \mathbf{r}_1^2, \mathbf{r}_2^2\mathbf{r}_3^2\mathbf{r}_4^2)\)
if (vectorlist.length < 27) {
    System.out.print(x_1);
    System.out.print(x_2);
    System.out.print(x_3);
    System.out.println(x_4);
}
}
}
}
}
}
}

/* Create a list of sums of 2 vectors in a list of vectors
 * multiplying the first component of the vectors in the
 * second list by \( x \) */

static int[][] vecsums(int[][] in1, int[][] in2, int p, int x) {
    int[][] preout = new int[in1.length * in2.length][2];
    for (int i = 0; i < in1.length; i++) {
        for (int j = 0; j < in2.length; j++) {
            preout[i * in2.length + j][0] = (in1[i][0] + x * in2[j][0]) % p;
            preout[i * in2.length + j][1] = (in1[i][1] + in2[j][1]) % p;
        }
    }
    // eliminate the redundancy in the output
    int[][] out = eliminate(preout, p);
    return out;
}
/*eliminate redundancies in a list of vectors*/
public static int[][] eliminate(int[][] input, int modulus) {
    boolean[][] inset = new boolean[modulus][modulus];
    //initialize
    for(int i=0; i< modulus; i++) {
        for(int j = 0; j< modulus; j++) {
            inset[i][j] = false;
        }
    }
    //mark off the vectors in the list
    for(int i= 0; i< modulus; i++) {
        for(int j = 0;j < modulus; j++) {
            for(int k = 0; k < input.length; k++) {
                if(input[k][0] == i && input[k][1] == j) {
                    inset[i][j] = true;
                }
            }
        }
    }
    //determine the length for the output vector
    int size = 0;
    for(int i = 0; i< modulus; i++) {
        for(int j = 0; j< modulus; j++) {
            if(inset[i][j] == true) {
                size ++;
            }
        }
    }
    int index= 0;
    //output the list without redundancies
    int[][] out = new int[size][2];
    for(int i = 0; i< modulus; i++) {
        for(int j= 0; j< modulus; j++) {
            if(inset[i][j] == true) {
                out[index][0] = i;
                out[index][1] = j;
                index++;
            }
        }
    }
}
return out;
}
/*Multiplies the first coordinate of a vector 
* by x*/
public static int[][] mult(int[][] input, int x, int modulus){
    int[][] out = new int[input.length][2];
    //initialize the output
    for(int i = 0; i< out.length; i++) {
        out[i][0] = input[i][0];
        out[i][1] = input[i][1];
    }
    //multiply the first coordinate by x
    for(int i=0; i<input.length; i++) {
        out[i][0] = input[i][0] * x % modulus;
    }
    return out;
}