Simultaneous Cubic and Quadratic Diagonal Equations Over the Primes

Alan Talmage

September 5, 2019

Abstract

The system of equations
\[ u_1 p_1^2 + \ldots + u_s p_s^2 = 0 \]
\[ v_1 p_1^3 + \ldots + v_s p_s^3 = 0 \]
has prime solutions \((p_1, \ldots, p_s)\) for \(s \geq 13\), assuming that the system has solutions modulo each prime \(p\). This is proved via the Hardy-Littlewood circle method, with the main ingredients in the proof being Wooley’s work on the corresponding system over the integers \([11]\) and results on Vinogradov’s mean value theorem. Additionally, a set of sufficient conditions for the local solvability is given: If both equations are solvable modulo 2, the quadratic equation is solvable modulo 3, and at least 7 of each of \(u_i\), \(v_i\) are not zero modulo \(p\) for each prime \(p\), then the system has solutions modulo each prime \(p\).

1 Introduction

Much work has been done in applying the Hardy-Littlewood circle method to find integral solutions to systems of simultaneous equations (see \([2]\), \([3]\), \([9]\), and \([11]\) for examples). In particular, recent progress on Vinogradov’s mean value theorem (see \([1]\), \([8]\)) has enabled progress on questions of this type. Here we consider the question of solving systems of equations with prime variables, generalizing the Waring-Goldbach problem in the same way existing work on integral solutions of systems of equations generalizes Waring’s problem. Following Wooley \([11]\), we address here the simplest nontrivial case of a
quadratic equation and a cubic equation. We find that under suitable local conditions, 13 variables will suffice for us to establish an eventually positive asymptotic formula guaranteeing solutions to the system of equations.

Consider a pair of equations of the form

\[
\begin{align*}
    u_1 p_1^2 + \ldots + u_s p_s^2 &= 0 \\
    v_1 p_1^3 + \ldots + v_s p_s^3 &= 0
\end{align*}
\] (1)

where \(u_1, \ldots, u_s, v_1, \ldots, v_s\) are nonzero integer constants and \(p_1, \ldots, p_s\) are variables restricted to prime values. We seek to prove the following theorem:

**Theorem 1.1. If**

1. The system (1) has a nontrivial real solution,
2. \(s \geq 13\), and
3. for every prime \(p\), the corresponding local system

\[
\begin{align*}
    u_1 x_1^2 + \ldots + u_s x_s^2 &= 0 \pmod{p} \\
    v_1 x_1^3 + \ldots + v_s x_s^3 &= 0 \pmod{p}
\end{align*}
\] (2)

has a solution \((x_1, \ldots, x_s)\) with all \(x_i \neq 0 \pmod{p}\).

then the system has a solution \(\{p_1, \ldots, p_s\}\) with all \(p_i\) prime. Moreover, if we let \(R(P)\) be the number of solutions \((p_1, \ldots, p_s)\), each weighted by \((\log p_1) \ldots (\log p_s)\), then we have \(R(P) \sim \mathcal{S} P^{s-5}\) where \(\mathcal{S} > 0\) uniformly over all choices of \(u_1, \ldots, u_s, v_1, \ldots, v_s\).

In section 8 we give a sufficient condition for (2) to be satisfied, giving us the explicit theorem

**Theorem 1.2. Consider the system**

\[
\begin{align*}
    u_1 p_1^2 + \ldots + u_s p_s^2 &= U \\
    v_1 p_1^3 + \ldots + v_s p_s^3 &= V
\end{align*}
\] (3)

where \(u_1, \ldots, u_s, v_1, \ldots, v_s, U, V\) are nonzero integer constants. If

1. The system has a nontrivial real solution,
2. \( s \geq 13 \),

3. \( \sum_{i=1}^{s} u_i = U \pmod{2} \) and \( \sum_{i=1}^{s} v_i = V \pmod{2} \)

4. \( \sum_{i=1}^{s} u_i = U \pmod{3} \), and

5. for each prime \( p \neq 2 \), at least 7 of the \( u_i \) and the \( v_i \) are not zero modulo \( p \),

then the system has a solution \( \{p_1, \ldots, p_s\} \) with all \( p_i \) prime. Moreover, if we let \( R(P) \) be the number of solutions \( (p_1, \ldots, p_s) \), each weighted by \( (\log p_1) \cdots (\log p_s) \), then we have \( R(P) \sim \mathcal{G} P^{s-5} \) where \( \mathcal{G} > 0 \) uniformly over all choices of \( u_1, \ldots, u_s, v_1, \ldots, v_s \).

We use the Hardy-Littlewood circle method to prove these results. Section 2 performs the necessary setup for the application of the circle method: defining the relevant functions and the major arc/minor arc dissection. Section 3 proves a Weyl-type bound needed for the minor arcs by means of Vaughan’s identity. Section 4 uses the bound from section 3 and Wooley’s work on the corresponding problem over the integers to obtain the necessary minor arc bounds. Section 5 is the circle method reduction to the singular series and singular integral. Section 6 shows the convergence of the singular series and Section 7 shows that it is eventually positive, contingent on the local solvability of the system 11. Section 8 shows sufficient conditions for the solvability of the local system. This depends on a computer check of local solvability for a finite number of primes. Section 9 discusses several techniques which can be employed to improve the efficiency of this computation. Section 10 finishes the proof of Theorem 11. Appendix A contains the source code used to run the computations laid out in section 9.

2 Circle Method Setup

As is standard in the literature, we use \( e(\alpha) \) to denote \( e^{2\pi i \alpha} \). The letter \( p \) is assumed to refer to a prime wherever it is used, and \( \epsilon \) means a sufficiently small positive real number. \( \Lambda \) and \( \mu \) are the von Mangoldt and Möbius functions, respectively. We write \( f(x) \ll g(x) \) for \( f(x) = O(g(x)) \), and
f(x) \sim g(x) \text{ if both } f(x) \ll g(x) \text{ and } g(x) \ll f(x) \text{ hold. When we refer to a solution of the system under study, we mean an } s\text{-tuple of prime numbers } (p_1, \ldots, p_s) \text{ satisfying (I).}

Define the generating function

$$f_i(\alpha, \beta) = \sum_{p<P} (\log p)e(\alpha u_i p^2 + \beta v_i p^3)$$

Let

$$R(P) = \int_0^1 \int_0^1 \prod_{i=1}^s f_i(\alpha, \beta) d\alpha d\beta$$

(4)

$$= \int_0^1 \int_0^1 \sum_{p_1, \ldots, p_s<P} \prod_{i=1}^s ((\log p)e(\alpha u_i p^2 + \beta v_i p^3)) d\alpha d\beta$$

Thus $R(P) > 0$ if and only if there is a solution to the system (I).

We divide the unit square into major and minor arcs. Let $A$ be a constant, whose value will be fixed later. For all $P > P(A)$, where $P(A)$ is a constant depending only on $A$, and for all $q < Q = (\log P)^A$, $1 \leq a \leq q$, $1 \leq b \leq q$, $(a, b, q) = 1$, let a typical major arc $M(a, b, q)$ consist of all $(\alpha, \beta)$ such that $|\alpha - a/q| \leq \frac{(\log P)^A}{qP^2}$ and $|\beta - b/q| \leq \frac{(\log P)^A}{qP^3}$. Let the major arcs $M$ be the union of all such $M(a, b, q)$, and let the minor arcs $m$ be the remainder of $(\mathbb{R}/\mathbb{Z})^2$. We will identify $(\mathbb{R}/\mathbb{Z})^2$ with $[0, 1)^2$ throughout.

3 A Minor Arc Bound Sensitive to Multiple Coefficients

Let $\alpha = (\alpha_1, \ldots, \alpha_k)$ and let

$$F_k(\alpha) = \sum_{n \leq P} \Lambda(n)e(\alpha_1 n + \alpha_2 n^2 + \ldots + \alpha_k n^k)$$

This section consists of the proof of the following lemma and corollary:
Lemma 3.1. For $D > 0$, where $D = D(A)$ can be made arbitrarily large by increasing $A$, if $(\alpha_2, \alpha_3) \in \mathcal{m}$, then

$$F_3(\alpha) \ll P(\log P)^{-D}$$

Corollary 3.1. Let $F(\alpha, \beta) = \sum \limits_{p \leq P}(\log p)e(\alpha p^2 + \beta p^3)$. Then

$$\sup_{(\alpha, \beta) \in \mathcal{m}} F(\alpha, \beta) \ll P(\log P)^{-D}$$

Proof. Take $\alpha_2 = \alpha$, $\alpha_3 = \beta$, and $\alpha_1 = 0$ in Lemma 3.1 and note that there are trivially $\ll P^{1/2} \log P$ prime powers $\leq P$ which contribute $\ll P^{1/2}(\log P)^2$ to the sum. \hfill \Box

For the proof of Lemma 3.1 we cite some known results on Vinogradov’s mean value theorem. Let

$$J_{s,k}(P) = \int_{[0,1)^k} |F_k(\alpha)|^{2s} d\alpha$$

We cite the bound

$$J_{3,2} \ll P^3 \log P \tag{5}$$

from [5] (cf. [7] chap. 7 exercise 2) and for $s > 6$

$$J_{s,3} \ll P^{2s-6} \tag{6}$$

from [1].

We approach this lemma by means of Vaughan’s identity. The purpose is to break the sum

$$\sum_{n \leq P} \Lambda(n)f(n)$$

into sums of two manageable types:

**Type I**: sums of the form

$$\sum_{k \leq Y} c(k) \sum_{l \leq P/k} f(kl)$$

**Type II**: sums of the form

$$\sum_{X < k \leq P/X} \sum_{l \leq P/k} a(k)b(l)f(kl)$$
with \(c(k), a(k), b(l), Y,\) and \(X\) not too large.

Let \(X = (\log P)^B\) for some \(B > 0\) to be fixed later. Vaughan’s identity gives

\[
\sum_{n \leq P} \Lambda(n) f(n) = S_1 + S_2 + S_3 + S_4
\]

where

\[
S_1 = \sum_{n \leq X} \Lambda(n) f(n),
\]

\[
S_2 = \sum_{n \leq P} \left( \sum_{k=1}^{\Lambda(n)} \mu(k) \log l \right) f(n),
\]

\[
S_3 = \sum_{n \leq P} \sum_{k \leq X^2} \left( \sum_{m,n} \Lambda(m) \mu(n) \right) f(n),
\]

\[
S_4 = \sum_{n \leq P} \left( \sum_{k \leq X, l > X} a(k)b(l) \right) f(n)
\]

with

\[
a(k) = \sum_{\substack{l \mid k \atop l > X}} \Lambda(l),
\]

\[
b(l) = \begin{cases} 
\mu(l) & l > X \\
0 & l \leq X 
\end{cases}
\]

If we take \(f(n) = e(\alpha_1 n + \alpha_2 n^2 + \alpha_3 n^3),\) \(\sum_{n \leq P} \Lambda(n) f(n) = F_3(\alpha).\) Now \(S_1\) is trivial, \(S_3\) and (after some manipulation) \(S_2\) are Type I sums, and \(S_4\) is a Type II sum, so we can bound each sum individually.

First consider \(S_1\): Since \(|f(n)| \ll 1,\)

\[
S_1 = \sum_{n \leq X} \Lambda(n) f(n) \ll \sum_{m \leq X} \Lambda(n) \ll X \tag{7}
\]

where the last bound is a classical result of Chebyshev.
Next we consider $S_3$:

$$S_3 = \sum_{n \leq P} \sum_{k \leq n \leq X^2} \left( \sum_{m,n, m\leq k, n \leq X} \Lambda(m) \mu(n) \right) f(n)$$

Let

$$c_3(k) := \sum_{m,n, m\leq k, n \leq X} \Lambda(m) \mu(n)$$

and note for future reference that

$$|c_3(k)| \leq \sum_{m \mid k} \Lambda(m) = \log k$$

Interchanging the order of summation:

$$S_3 = \sum_{k \leq X^2} c_3(k) \sum_{l \leq P/k} f(kl)$$

$$= \sum_{k \leq X^2} c_3(k) \sum_{l \leq P/k} e(\alpha_1 kl + \alpha_2 k^2 l^2 + \alpha_3 k^3 l^3)$$

Now by Dirichlet’s theorem on Diophantine approximation, we let $|\alpha_j - b_{q_j}| \leq \frac{(\log P)^A}{q_j P}$, $q_j \leq \frac{P^{j+1}}{(\log P)^j}$. Let $q = \gcd(q_2, q_3)$, $a_2 = b_2 q_3$, and $a_3 = b_3 q_2$. Then since $(\alpha_2, \alpha_3) \in \mathfrak{m}$, we have $q > (\log P)^A$, so $q_j > (\log P)^{A/2}$ for some $j \geq 2, 3$.

Since $k \leq X^2 = (\log P)^{2B}$, let $\alpha'_j = \alpha_j k$, $\alpha'_j = a_j \frac{k^j}{(k^j q_j)}$, $q'_j = \frac{q_j}{(k^j q_j)}$. Then

$$|\alpha'_j - \frac{a'_j}{q'_j}| \leq \frac{(\log P)^A k^j}{q'_j P}.$$ Thus

$$S_3 = \sum_{k \leq X^2} c_3(k) \sum_{l \leq P/k} e(\alpha'_1 l + \alpha'_2 l^2 + \alpha'_3 l^3)$$

We now need a bound on

$$H(\alpha', P/k) := \sum_{l \leq P/k} e(\alpha'_1 l + \alpha'_2 l^2 + \alpha'_3 l^3)$$
By Theorem 5.2 of [7], we have that it is
\[
\ll (\log P) \left( J_{3,2}(2P)(P/k)^3 \prod_{j=1}^3 \left( \frac{1}{q_j^j} + \frac{k}{P} + \frac{q_j^j k^j}{P^3} \right) \right)^{1/6}
\]

Now by (5), \( J_{3,2}(P) \ll P^3(\log P) \), so
\[
H(\alpha, P/k) \ll P^k (\log P)^2 \prod_{j=1}^3 \left( \frac{1}{q_j^j} + \frac{k}{P} + \frac{q_j^j k^j}{P^3} \right)^{1/6}
\]

Now \( \frac{k}{P} \ll P^{-1/2}, \frac{1}{q_j} \ll (\log P)^{2jB-A/2}, \frac{q_j^j k^j}{P} \ll (\log P)^{2jB-A} \), so
\[
S_3 \ll \sum_{k \leq X^2} (\log k) \frac{P}{k} (\log P)^{(6B-A)/6+2}
\]

\[
\ll P(\log P)^{B-A/6+4}
\]

So we have
\[
S_3 \ll P(\log P)^{B-A/6+4} \tag{8}
\]

Next we consider \( S_2 \):
\[
S_2 = \sum_{n \leq P} \left( \sum_{k \leq X, \ \mu(k) \log l} \right) f(n)
\]
\[
= \sum_{k \leq X} \mu(k) \sum_{l \leq P/k} f(kl) \int_{1}^{l} \frac{dt}{t}
\]
\[
= \sum_{k \leq X} \mu(k) \int_{1}^{P/k} \sum_{l \leq P/k} f(kl) \frac{dt}{t}
\]
\[
= \int_{1}^{P} \left( \sum_{k \leq X/t} \mu(k) \sum_{l \leq P/k} f(kl) \right) \frac{dt}{t}
\]

The term in the parentheses is now a Type I sum, so an argument parallel to the argument bounding \( S_3 \) above gives:
\[
S_2 \ll \int_{1}^{P} \frac{X}{t} \left( \frac{P}{k} (\log P)^{2+B-A/6} - t(\log P)^{2+B-A/6} \right) \frac{dt}{t}
\]
\[ \ll X \frac{P}{k} (\log P)^{2+B-A/6} \int_1^P \frac{dt}{t^2} \]
\[ \ll P (\log P)^{3+B-A/6} (1 - \frac{1}{P}) \ll P (\log P)^{3+B-A/6} \]

So we have
\[ S_2 \ll P (\log P)^{3+B-A/6} \quad (9) \]

Finally, we consider \( S_4 \). We begin by splitting into dyadic ranges. Let \( M = \{X 2^k : 0 \leq k, 2^k \leq P/X^2\} \). Then

\[ S_4 = \sum_{M \in M} S_4(M) \]

where
\[ S_4(M) = \sum_{M < k \leq 2M} \sum_{l \leq P/k} a(k)b(l)f(kl) \]

Our goal is now to replace the sum over the range \( l \leq P/k \) with one over the range \( l \leq P/M \). We begin by considering the integral

\[ I(x) := \int_R \frac{\sin(2\pi R t)}{\pi t} e(-xt) dt \]

where \( R > 0 \) is a constant. Computing the integral via the residue theorem gives

\[ I(x) = \begin{cases} 1 & |x| < R \\ 0 & |x| > R \end{cases} \]

Now for \( x \neq R \), \( t \geq 1 \),

\[ \int_{|t| > T} \frac{\sin(2\pi R t)}{\pi t} e(-xt) dt = \int_{|t| > T} \frac{e((R-x)t) - e(-(R+x)t)}{2\pi it} dt \]

Integrating by parts gives:

\[ \ll \frac{1}{T|R-x|} + \frac{1}{T|R+x|} + \frac{1}{T^3} \ll \frac{1}{T|R-|x||} \]

Thus we can support the integrand on \([ -T, T ]\) with acceptable error:

\[ I(x) = \int_{-T}^T \frac{\sin(2\pi R t)}{\pi t} e(-xt) dt + O \left( \frac{1}{T|R-|x||} \right) \]
We now take $R = \log([P] + \frac{1}{2})$, $x = \log(kl)$, giving us

$$S_4(M) = \sum_{M < k \leq 2M} \sum_{l \leq P/M} a(k) b(l) f(kl) I(\log(kl))$$

$$= \int_{-T}^{T} \sum_{M < k \leq 2M} \sum_{l \leq P/M} \frac{a(k) b(l)}{(kl)^{2\pi it}} f(kl) \frac{\sin(2\pi R t)}{\pi t} dt + O \left( \frac{P^2 \log P}{T} \right)$$

Now

$$\frac{\sin(2\pi R t)}{\pi t} \ll \frac{1}{\pi t} \ll \frac{1}{|t|}$$

and

$$\frac{\sin(2\pi R t)}{\pi t} \ll \frac{2\pi R t}{\pi t} \ll R,$$

so

$$\frac{\sin(2\pi R t)}{\pi t} \ll \min(R, 1/|t|)$$

We now take $T = P^3$, $a(k, t) = a(k) k^{-2\pi it}$, $b(l, t) = b(l) l^{-2\pi it}$, and

$$S_4(M, t) := S_4(M) = \sum_{M < k \leq 2M} \sum_{l \leq P/k} a(k) b(l, t) f(kl)$$

Then

$$S_4(M) \ll \sup_{|t| < T} |S_4(M, t)| \int_{-T}^{T} \frac{\sin(2\pi R t)}{\pi t} dt$$

$$\ll 1 + (\log P) \sup_{|t| < T} |S_4(M, t)|$$

We now consider $S_4(M, t)$. Let $b > 6$. By Hölder’s inequality

$$S_4(M, t)^{2b} \ll \left( \sum_{M < k \leq 2M} |a(k, t)|^{2b} \right)^{2b-1} \left( \sum_{M < k \leq 2M} \left| \sum_{l \leq P/M} b(l, t) f(kl) \right|^{2b} \right)^{2b}$$

Now $|a(k, t)| = |a(k)| \leq \log k \ll \log M \ll \log P$, so

$$\ll \left( M (\log P)^{\frac{2b}{2b-1}} \right)^{2b-1} \left( \sum_{M < k \leq 2M} \left| \sum_{l \leq P/M} b(l, t) f(kl) \right|^{2b} \right)^{2b}$$
\[
\ll (\log P)^{2b} M^{2b-1} \sum_{M < k \leq 2M} \left| \sum_{l \leq P/M} b(l, t) f(kl) \right|^{2b}
\]

Expanding the \(2b\)-th power yields

\[
\left| \sum_{l \leq P/M} b(l, t) f(kl) \right|^{2b} = \sum_{l_j \leq P/M} \left( \prod_{i=1}^{b} b(l_i, t) \prod_{i=b+1}^{2b} \overline{b(l_i, t)} \right) e(\alpha_1 k s_1(1) + \alpha_2 k^2 s_2(1) + \alpha_3 k^3 s_3(1))
\]

where

\[
s_j(1) = l_1^j + \ldots + l_b^j - l_{b+1}^j - \ldots - l_{2b}^j
\]

Collecting terms with the same values of the \(s_j\):

\[
= \sum_{|v_j| \leq b P^j} R_1(v) e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3)
\]

where

\[
R_1(v) = \sum_{l_j \leq P/M} \prod_{i=1}^{b} b(l_i, t) \prod_{i=b+1}^{2b} \overline{b(l_i, t)} \ll J_{b,3}(P/M) \ll (P/M)^{2b-6}
\]

by (6). We now substitute this back into the sum above

\[
S_4(M, t)^{2b} \ll (\log P)^{2b} M^{2b-1} \sum_{|v_j| \leq b P^j M^{-j}} R_1(v) \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3)
\]

\[
\ll (\log P)^{2b} M^3 P^{2b-6} \sum_{|v_j| \leq b P^j M^{-j}} \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3)
\]
We now repeat this procedure. By Hölder’s inequality

\[ S_4(M, t)^{4b^2} \ll \left( (\log P)^{2b} M^{5} P^{2b-6} \right)^{2b} \left( \sum_{|v_j| \leq bP^j M^{-j}} 1^{2b} \right)^{2b-1} \]

\[ \times \sum_{|v_j| \leq bP^j M^{-j}} \left| \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3) \right|^{2b} \tag{10} \]

\[ \ll (\log P)^{4b} M^{10b} P^{4b^2 - 12b} (b^3 P^6 M^{-6})^{2b-1} \sum_{|v_j| \leq bP^j M^{-j}} \left| \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3) \right|^{2b} \]

\[ \ll (\log P)^{4b^2} M^{6-2b} P^{4b^2 - 6} \sum_{|v_j| \leq bP^j M^{-j}} \left| \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3) \right|^{2b} \]

As before, we expand the 2b-th power and collect like terms. Thus

\[ \left| \sum_{M < k \leq 2M} e(\alpha_1 k v_1 + \alpha_2 k^2 v_2 + \alpha_3 k^3 v_3) \right|^{2b} \]

\[ = \sum_{M < k_j \leq 2M} e(\alpha_1 s_1(k)v_1 + \alpha_2 s_2(k) v_2 + \alpha_3 s_3(k) v_3) \]

\[ = \sum_{|u_j| \leq b^2 M^j} R_2(u) e(\alpha_1 u_1 v_1 + \alpha_2 u_2 v_2 + \alpha_3 u_3 v_3) \]

where

\[ R_2(u) = \sum_{M < k_j \leq 2M \atop s(k) = u} 1 \ll J_{b,3}(2M) \ll M^{2b-6} \]

by (3). Substituting this back into the above sum, we obtain

\[ S_4(M, t)^{4b^2} \ll (\log P)^{4b^2} P^{4b^2 - 6} \sum_{|u_j| \leq b^2 M^j} \left| \sum_{|v_j| \leq bP^j M^{-j}} e(\alpha_1 u_1 v_1 + \alpha_2 u_2 v_2 + \alpha_3 u_3 v_3) \right| \]
Summing over each of the $v_j$ gives

$$S_4(M, t)^{4b^2} \ll (\log P)^{4b^2} P^{4b^2-6} \sum_{|u_j| \leq 2^j M_j} \prod_{j=1}^3 \min\left( \frac{P_j}{M_j}, \frac{1}{\|\alpha_j u_j\|} \right)$$

which by Lemma 2.2 of [7] is

$$\ll (\log P)^{4b^2+3} P^{4b^2} \prod_{j=1}^3 \left( \frac{1}{q_j} + \frac{1}{X_j} + \frac{M_j}{P_j} + \frac{q_j}{P_j} \right)$$

Taking a power of $1/4b^2$, recovering the $\log P$ from $I(x)$ and the $\log P$ from the number of elements of $\mathcal{M}$, we obtain

$$S_4 \ll P(\log P)^4 \prod_{j=1}^3 \left( \frac{1}{q_j} + \frac{1}{X_j} + \frac{q_j}{P_j} \right)^{1/(4b^2)}$$

Recalling that $q_j > (\log P)^A$ for some $j$ and $X = (\log P)^B$, this is

$$S_4 \ll P(\log P)^{4-\min(A,B)/(4b^2)}$$

for $b > 6$.

Proof of Lemma 3.1: Putting together our estimates for each $S_i$, we obtain

$$F_3(\alpha) = S_1 + S_2 + S_3 + S_4$$

$$\ll (\log P)^B + P(\log P)^{3+B-A/6} + P(\log P)^{B-A/6+4} + P(\log P)^{4-\min(A,B)/(4b^2)}$$

So if we take $B > 4b^2 D(D + 4)$ and $A > 6(B + D + 4)$, we have

$$F_3(\alpha) \ll P(\log P)^{-D}$$

□

4 Minor Arc Bounds

The necessary bounds on the minor arcs come from Lemma 3.1 and Wooley’s work on the corresponding problem over the integers in [11]. Let
\[ F(P) = \sum_{1 \leq x < P} e(\alpha x^2 + \beta x^3), \]
\[ \Sigma_r(P) = \int_0^1 \int_0^1 |F(P)|^{2r} d\alpha d\beta \]

Note that by this definition, \( \Sigma_r(P) \) counts the number of positive integer solutions to
\[ x_1^2 + \ldots + x_r^2 = x_1^2 + \ldots + x_r^2 \]
\[ x_1^3 + \ldots + x_r^3 = x_1^3 + \ldots + x_r^3 \]
with all \( x_i < P \). We cite the bound:

**Theorem 4.1.** If \( r \geq \frac{16}{3} \), \( \Sigma_r(P) \ll P^{2r-5} \).

**Proof.** This is the relevant portion of Theorem 1.3 of [11].

So we have, for integer \( r \geq 6 \),
\[ T_r(P) \ll P^{2r-5} \]

Now we consider our minor arcs. We have
\[ \int_m \prod_{i=1}^s f_i(\alpha, \beta) d\alpha d\beta \ll \int_m |f_i(\alpha, \beta)|^s d\alpha d\beta \]
for some \( i \). Since \( s > 12 \), this is now
\[ \ll \int_0^1 \int_0^1 |f_i(\alpha, \beta)|^{12} d\alpha d\beta \left( \sup_{(\alpha, \beta) \in m} |f_i(\alpha, \beta)| \right)^{s-12} \]

Now the integral \( \int_0^1 \int_0^1 |f_i(\alpha, \beta)|^{12} d\alpha d\beta \) counts prime solutions of the system
\[ p_1^2 + \ldots + p_6^2 = p_7^2 + \ldots + p_{12}^2 \]
\[ p_1^3 + \ldots + p_6^3 = p_7^3 + \ldots + p_{12}^3 \]
with the solution \( \{p_1, \ldots, p_6, \ldots, p_{12} \} \) weighted by \( \prod_{i=1}^{12} (\log p_i) \). Since the number of prime solutions of the system is bounded by the number of integer solutions
to the system, which is $\ll P^7$ by Theorem 4.1, and $\prod_{i=1}^{12} (\log p_i) \leq (\log P)^{12}$, we have

$$\int \prod_{m}^{s} f_i(\alpha, \beta) d\alpha d\beta \ll (\log P)^{12} P^7 \left( \sup_{\alpha, \beta \in m} |f_i(\alpha, \beta)| \right)^{s-12}$$

Now by Lemma 3.1,

$$\sup_{\alpha, \beta \in m} |f_i(\alpha, \beta)| \ll P (\log P)^{-D}$$

Thus

$$\int \prod_{m}^{s} f_i(\alpha, \beta) d\alpha d\beta \ll P^{s-5} (\log P)^{-E} \quad (12)$$

for $E > D(s - 12) - 12$.

## 5 Major Arc Approximations

On a typical major arc $\mathfrak{M}(a, b, q)$, let $\alpha = \frac{a}{q} + \theta$, $\beta = \frac{b}{q} + \phi$, with $\theta < \frac{(\log P)^A}{qP^2}$, $\phi < \frac{(\log P)^A}{qP^2}$, and $q < (\log P)^A$. For ease of notation, let $\frac{(\log P)^A}{qP^2} = \Theta$, $\frac{(\log P)^A}{qP^2} = \Phi$. Let

$$W_i(q, a, b) = \sum_{\substack{r=1 \\ (r, q)=1}}^{q} \frac{e \left( \frac{au_i r^2 + bv_i r^3}{q} \right)}{\varphi(q)}$$

$$f_i^*(\alpha, \beta) = \frac{1}{\varphi(q)} W_i(q, a, b) \int_{0}^{P} e(\theta u_i m^2 + \phi v_i m^3) dm$$

**Lemma 5.1.** On $\mathfrak{M}(q, a, b)$,

$$f_i(\alpha, \beta) = f_i^*(\alpha, \beta) + O(P \exp(-C(\log P)^{1/2}))$$

for some positive constant $C$.

**Proof.**

$$|f_i(\alpha, \beta) - f_i^*(\alpha, \beta)|$$
\[ \begin{aligned}
= \left| \sum_{p<P} (\log p) e(\alpha u_i p^2 + \beta v_i p^3) - \frac{1}{\phi(q)} W_i(q, a, b) \int_0^P e(\theta u_i x^2 + \phi v_i x^3) \, dx \right| \\
= \left| W_i(q, a, b) \sum_{p<P \equiv r(\text{mod } q)} (\log p) e(\theta u_i p^2 + \phi v_i p^3) \right. \\
- \left. \frac{1}{\phi(q)} W_i(q, a, b) \int_0^P e(\theta u_i x^2 + \phi v_i x^3) \, dx \right| \\
= \sum_{m<P} \left[ (\log p) e\left( \frac{a u_i p^2 + b v_i p^3}{q} \right) \mathbbm{1}_p \\
- \frac{1}{\phi(q)} W_i(q, a, b) \right] e(\theta u_i m^2 + \phi v_i m^3) \ (14)\end{aligned} \]

where \( \mathbbm{1}_p \) is the indicator function of the primes.

We now apply Abel summation, with the term in square brackets above serving as the coefficient:

\[ \begin{aligned}
= e(\theta u_1 P^2 + \phi v_1 P^3) \left( \sum_{p<P} (\log p) e\left( \frac{a u_i p^2 + b v_i p^3}{q} \right) - \frac{1}{\phi(q)} \sum_{m<P} W_i(q, a, b) \right) \\
- \int_0^P 2\pi i (2\theta u_i x + 3\phi v_i x^2) \left( \sum_{p<x} (\log p) e\left( \frac{a u_i p^2 + b v_i p^3}{q} \right) - \frac{1}{\phi(q)} \sum_{m<x} W_i(q, a, b) \right) \, dx.
\end{aligned} \]

Now by the Siegel-Walfisz theorem we have that

\[ \begin{aligned}
\sum_{p<x} (\log p) e\left( \frac{a u_i p^2 + b v_i p^3}{q} \right) \\
= W_i(q, a, b) \sum_{p<P \equiv r(\text{mod } q)} (\log p) \\
= \frac{x}{\phi(q)} W_i(q, a, b) + O(\phi(q) \exp(-C(\log x)^{1/2})).
\end{aligned} \]
So, returning to the main computation:

\[ |f_i(\alpha, \beta) - f_i^*(\alpha, \beta)| \]

\[
= e(\theta u_1 P^2 + \phi v_1 P^3) \left( \frac{P}{\phi(q)} W_i(q, a, b) - \frac{P}{\phi(q)} W_i(q, a, b) \\
+ O(\phi(q)P \exp(-C(\log P)^{1/2})) \right) \\
- 2\pi i \int_0^P (2\theta u_i x + 3\phi v_i x^2) \left( \frac{x}{\phi(q)} W_i(q, a, b) \\
- \frac{x}{\phi(q)} W_i(q, a, b) + O(\phi(q) \exp(-C(\log P)^{1/2})) \right) dx \\
\ll (1 + |\theta| P^2 + |\phi| P^3) \phi(q) P \exp(-C(\log P)^{1/2})) \\
\ll (\log P)^4 \frac{\phi(q)}{q} P \exp(-C(\log P)^{1/2})) \\
\ll P \exp(-C(\log P)^{1/2})) \]

Now we have

\[
\left| \prod_{i=1}^{s} f_i(\alpha, \beta) - \prod_{i=1}^{s} f_i^*(\alpha, \beta) \right| \ll P^s \exp(-C(\log P)^{1/2})
\]

Summing over all major arcs gives

\[
\int_{2\mathbb{R}} \left| \prod_{i=1}^{s} f_i(\alpha, \beta) - \prod_{i=1}^{s} f_i^*(\alpha, \beta) \right| \\
= \sum_{q<Q} \sum_{a=1}^{q} \sum_{b=1}^{q} \int_{2\mathbb{R}(a, b, q)} \left| \prod_{i=1}^{s} f_i(\alpha, \beta) - \prod_{i=1}^{s} f_i^*(\alpha, \beta) \right|
\]

17
\[
\sum_{q<Q} \sum_{a=1}^q \sum_{b=1}^q \int_{-Q^{-1}P^{-2}}^{Q^{-1}P^{-2}} \int_{-Q^{-1}P^{-2}}^{Q^{-1}P^{-3}} P^s \exp(-C(\log P)^{1/2}) d\alpha d\beta
\]
\[
\ll P^{s-5} \exp(-C(\log P)^{1/2})
\]
So we have
\[
\int \prod_{i=1}^s f_i(\alpha, \beta) = \int \prod_{i=1}^s f_i^*(\alpha, \beta) + O(P^{s-5} \exp(-C(\log P)^{1/2}))
\]
\[
= \sum \sum \sum \frac{1}{\phi(q)} \prod_{i=1}^s W_i(q, a, b) \int_{\theta} e(\theta u_i m^2 + \phi v_i m^3) dm
\]
\[
= \sum \sum \sum \frac{1}{\phi(q)^s} \prod_{i=1}^s W_i(q, a, b)
\]
\[
\times \int_{|\theta|<\Theta} \int_{|\phi|<\Phi} \prod_{i=1}^s \int_{\theta} e(\theta u_i m^2 + \phi v_i m^3) dmd\phi d\theta \quad (15)
\]
For clarity of notation, let
\[
A(q) = \sum_{a=1}^q \sum_{b=1}^q \frac{1}{\phi(q)} \prod_{i=1}^s W_i(q, a, b),
\]
\[
\mathcal{G}(Q) = \sum_{q<Q} A(q),
\]
\[
J(Q) = \int_{|\theta|<\Theta} \int_{|\phi|<\Phi} \prod_{i=1}^s \int_{\theta} e(\theta u_i m^2 + \phi v_i m^3) dmd\phi d\theta
\]
So by combining (4), Lemma 3.1 and (15) we have
\[
R(P) = \mathcal{G}(Q) J(Q) + O(P^{s-5}(\log P)^{-E})
\]
The singular integral \(J(Q)\) is the same as the one Wooley obtains in the corresponding problem over the integers, so by Lemma 7.4 of [11], there exists a positive constant \(C\) such that
\[
J(Q) = CP^{s-5} + O(P^{s-5}Q^{-1/2})
\]
So we have
\[ R(P) = CP^{s-5}S(Q) + O(P^{s-5}(\log P)^{-E}) \] (16)

6  Convergence of the Singular Series

Lemma 6.1. Let \((q_1, q_2) = 1\). Then
\[ W_i(q_1 q_2, a, b) = W_i(q_2, a q_1, b q_1^2) W_i(q_1, a q_2, b q_2^2) \]

Proof. Each residue class \(r\) modulo \(q_1 q_2\) with \((r, q_1 q_2) = 1\) is uniquely represented as \(cq_1 + dq_2\) with \(1 \leq c \leq q_2\), \((c, q_2) = 1\), \(1 \leq d \leq q_1\), \((d, q_1) = 1\), and \(cq_1, dq_2\) run over all residue classes modulo \(q_2\), \(q_1\) with \((cq_1, q_2) = 1\), \((dq_2, q_1) = 1\) respectively. Thus
\[ W_i(q_1 q_2, a, b) = \sum_{c=1}^{q_2} \sum_{d=1}^{q_1} e\left( \frac{a u_i(c q_1 + d q_2)^2 + b v_i(c q_1 + d q_2)^3}{q_1 q_2} \right) \]
\[ = \sum_{c=1}^{q_2} \sum_{d=1}^{q_1} e\left( \frac{a u_i c^2 + b v_i c^3}{q_2} \right) e\left( \frac{a u_i d^2 + b v_i d^3}{q_1 q_2} \right) \]
\[ = W_i(q_2, a q_1, b q_1^2) W_i(q_1, a q_2, b q_2^2) \]

Lemma 6.2. \(A(q)\) is multiplicative.

Proof. Let \((q_1, q_2) = 1\). Then
\[ A(q_1 q_2) = \sum_{\substack{a=1 \to q_1 q_2 \atop (a, b, q_1 q_2) = 1}} \sum_{b=1}^{q_1 q_2} \frac{1}{\phi(q_1 q_2)^s} \prod_{i=1}^{s} W_i(q_1 q_2, a, b) \]

Now \(a\) and \(b\) can be represented by \(a_1 q_2 + a_2 q_1\) and \(b_1 q_2 + b_2 q_1\) respectively, with \(1 \leq a_1, b_1 \leq q_1\), \(1 \leq a_2, b_2 \leq q_2\). So we can rewrite our sum as
\[ A(q_1 q_2) = \sum_{a_1=1}^{q_1} \sum_{b_1=1}^{q_1} \sum_{a_2=1}^{q_2} \sum_{b_2=1}^{q_2} \frac{1}{\phi(q_1 q_2)^s} \prod_{i=1}^{s} W_i(q_2, a_2 q_1^2, b_2 q_1^2) W_i(q_1, a_2 q_1^2, b_2 q_1^2) \]
Now, since \((q_1, q_2) = 1\), \(a_2q_1^2, b_2q_1^3, a_2q_1^2, b_2q_1^3\) run through complete sets of residue classes modulo \(q_1, q_2, q_1, q_2\) respectively, so we can rewrite the sum as

\[
= \sum_{a=1}^{q_1} \sum_{b=1}^{q_1} \sum_{c=1}^{q_2} \sum_{d=1}^{q_2} \frac{1}{\phi(q_1 q_2)^s} \prod_{i=1}^{s} W_i(q_2, a, b) W_i(q_1, c, d)
\]

\[
= A(q_1) A(q_2)
\]

Let

\[
\mathcal{S} = \sum_{q=1}^{\infty} A(q)
\]

Since \(A(q)\) is multiplicative,

\[
\mathcal{S} = \prod_{p} \left(1 + \sum_{k=1}^{\infty} A(p^k)\right)
\]  \hspace{1cm} (17)

**Lemma 6.3.** If \((a, b, q) = 1\), \(W_i(q, a, b) \ll q^{1+\epsilon}\).

This is an adaptation of Lemma 8.5 of [4].

**Lemma 6.4.** \(\mathcal{S}\) converges.

**Proof.**

\[
A(p^k) = \sum_{a=1}^{p^k} \sum_{b=1}^{p^k} \frac{1}{\phi(p^k)^s} \prod_{i=1}^{s} W_i(p^k, a, b),
\]

By Lemma 6.3 and the fact that there are \(\ll p^{2k}\) choices for the pair \(a, b\), we have

\[
\ll p^{2k} \phi(p^k)^{-s} (p^k)^{\frac{1}{2}} s
\]

\[
\ll (p^k)^{2-\frac{1}{2}s+\epsilon}
\]

Since \(s \geq 7\), we have

\[
A(p^k) \ll (p^k)^{-\frac{1}{2}+\epsilon}
\]  \hspace{1cm} (18)

Thus

\[
\sum_{k=1}^{\infty} A(p^k) \ll \sum_{k=1}^{\infty} (p^k)^{-\frac{1}{2}+\epsilon} = \frac{p^{-3/2} + \epsilon}{1 - p^{-3/2} + \epsilon} \sim p^{-3/2+\epsilon}
\]

20
Then
\[ \sum_{p} \sum_{k=1}^{\infty} A(p^k) \ll \sum_{p} p^{-3/2+\epsilon} \]
converges, so
\[ \mathcal{G} = \prod_{p} \left( 1 + \sum_{k=1}^{\infty} A(p^k) \right) \]
converges.

\[ \square \]

### 7 Positivity of the Singular Series

To show that \( R(P) \) has the desired growth rate, we now need to show that \( \mathcal{G} \) is positive.

**Lemma 7.1.** There exists \( R > 0 \) such that
\[ \frac{1}{2} < \prod_{p \geq R} \left( 1 + \sum_{k=1}^{\infty} A(p^k) \right) \]

*Proof.* By [18], we have \( A(p^k) \ll (p^k)^{-3/2+\epsilon} \ll (p^k)^{-1/4} \). Choose \( C, R \) such that \( Cp^{-5/4} < Cp^{-1/4} < \frac{1}{8} \) for all \( p \geq R - 1 \). Then
\[ \prod_{p \geq R} (1 - Cp^{-5/4}) \geq 1 - \sum_{p \geq R} Cp^{-5/4} \]
\[ \geq 1 - C \int_{R-1}^{\infty} x^{-5/4} dx = 1 - 4C(R-1)^{-1/4} \geq \frac{1}{2} \]
\[ \square \]

We now need only show that for \( p \leq C \), \( (1 + \sum_{k=1}^{\infty} A(p^k)) > 0 \).

Define \( M(q) \) to be the number of solutions \( (x_1, \ldots, x_s) \) to the simultaneous equations
\[ \sum_{i=1}^{s} u_ix_i^2 \equiv 0 \pmod{q} \]
\[ \sum_{i=1}^{s} v_ix_i^3 \equiv 0 \pmod{q} \]
with \( (x_i, q) = 1 \) for all \( i \).
Lemma 7.2. For any positive integer $q$, 
\[
M(q) = \frac{\phi(q)^s}{q^2} \sum_{d|q} A(d)
\]

Proof.
\[
M(q) = \frac{1}{q^2} \sum_{r_1=1}^{q} \sum_{r_2=1}^{q} \sum_{x_1=1}^{q} \sum_{x_2=1}^{q} \cdots \sum_{x_s=1}^{q} e\left( \frac{r_1(u_1 x_1^2 + \ldots + u_s x_s) + r_2(v_1 x_1^3 + \ldots + v_s x_s^3)}{q} \right)
\]

\[
= \frac{1}{q^2} \sum_{r_1=1}^{q} \sum_{r_2=1}^{q} \prod_{i=1}^{s} \sum_{x_i=1}^{q} e\left( \frac{r_1 u_i x_i^2 + r_2 v_i x_i^3}{q} \right)
\]

Let $d = \frac{q}{(r_1, r_2, q)}$, $a_1 = \frac{r_1}{(r_1, r_2, q)}$, and $a_2 = \frac{r_2}{(r_1, r_2, q)}$. Then, rearranging according to the value of $d$, we have
\[
= \frac{1}{q^2} \sum_{d|q} \sum_{a_1=1}^{d} \sum_{a_2=1}^{d} \prod_{i=1}^{s} \phi(d) \sum_{x_i=1}^{d} e\left( \frac{a_1 u_i x_i^2 + a_2 v_i x_i^3}{d} \right)
\]

\[
= \frac{\phi(q)^s}{q^2} \sum_{d|q} A(d)
\]
\[
\square
\]

Lemma 7.3. For positive integers $t, \gamma$ with $t > \gamma$, 
\[
M(p^t) \geq M(p^\gamma) p^{(t-\gamma)(s-2)}
\]

Proof. This is [10], Lemma 6.7, with the added observation that
\[
\max |b_1 - a_1|_p, |b_2 - a_2|_p \leq p^{-\gamma} \Rightarrow p^\gamma |(b_1 - a_1), (b_2 - a_2)|.
\]
So if $a_1, b_1 \not\equiv 0 \pmod{p}$, then $a_2, b_2 \not\equiv 0 \pmod{p}$. Thus the argument lifts solutions over reduced residue classes modulo $p^\gamma$ to solutions over reduced residue classes modulo $p^t$, so it applies here without modification. \[
\square
\]

Lemma 7.4. For each prime $p$, there exists a positive integer $\gamma = \gamma(p)$ such that $M(p^\gamma) > 0$. 

22
This lemma is stated here to preserve the flow of the argument. It is proved in sections 8 and 9.

**Lemma 7.5.** For each prime \( p \),

\[
1 + \sum_{k=1}^{\infty} A(p^k) > 0
\]

**Proof.** By Lemma 7.2,

\[
1 + \sum_{k=1}^{\infty} A(p^k) = \lim_{t \to \infty} \frac{p^{2t}}{\phi(p^t)^s} M(p^t)
\]

\[
\geq \lim_{t \to \infty} p^{(2-s)t} M(p^t)
\]

By Lemmas 7.3 and 7.4, for some positive integer \( \gamma \),

\[
\geq \lim_{t \to \infty} p^{(2-s)t} M(p^\gamma) p^{(t-\gamma)(s-2)}
\]

\[
\geq \lim_{t \to \infty} p^{(-\gamma)(s-2)} > 0
\]

\[\square\]

**Theorem 7.1.** \( \mathcal{G} > 0 \).

**Proof.** This follows directly from (17), Lemma 7.1, and Lemma 7.5 \[\square\]

## 8 Solvability of the Local Problem

We now consider the local system

\[
u_1 x_1^2 + \ldots + u_s x_s^2 = 0 \pmod{p}
\]

\[
v_1 x_1^3 + \ldots + v_s x_s^3 = 0 \pmod{p}
\]

with \( x_i \neq 0 \) in \( \mathbb{Z}/p\mathbb{Z} \).

We will prove the following result:

**Theorem 8.1.** The system

\[
u_1 x_1^2 + \ldots + u_s x_s^2 = U \pmod{p}
\]

\[
v_1 x_1^3 + \ldots + v_s x_s^3 = V \pmod{p}
\]

has a solution \( (x_1, \ldots, x_s) \) with \( x_1 \neq 0 \) modulo every prime \( p \) if
1. \[ \sum_{i=1}^{s} u_i = U \pmod{2} \quad \text{and} \quad \sum_{i=1}^{s} v_i = V \pmod{2} \]

2. \[ \sum_{i=1}^{s} u_i = U \pmod{3} \]

3. For each prime \( p \) at least 7 of the \( u_i, v_i \) are not zero modulo \( p \).

Observe that if the system

\[
\begin{align*}
    u_1 x_1^2 + \ldots + u_t x_t^2 &= U \pmod{p} \\
    v_1 x_1^3 + \ldots + v_t x_t^3 &= V \pmod{p}
\end{align*}
\]

has a solution for all \( u_1, \ldots, u_t, v_1, \ldots, v_t \neq 0 \), then so does the system

\[
\begin{align*}
    u_{i_1} x_{i_1}^2 + \ldots + u_{i_t} x_{i_t}^2 &= U \pmod{p} \\
    v_{j_1} x_{j_1}^3 + \ldots + v_{j_t} x_{j_t}^3 &= V \pmod{p}
\end{align*}
\]

for any \( \{i_1, \ldots, i_t\}, \{j_1, \ldots, j_t\} \subset \{1, \ldots, s\} \). Also observe that the conditions of Theorem 8.1 guarantee solvability modulo \( p = 2 \) and \( p = 3 \): \( p = 2 \) is immediate and for \( p = 3 \), the condition guarantees that the quadratic equation is satisfied, and each term \( v_i x_i^3 \) of the cubic equation can be independently set to 1 or \(-1\), allowing us to set \( v_1 x_1^3 = V \) if \( V \neq 0 \pmod{3} \) and partition the remainder of \( \{1, \ldots, t\} \) into groups of 2 and 3, which can be zeroed by setting them to \( \{1, -1\} \) and \( \{1, 1, 1\} \).

Thus we have reduced Theorem 8.1 to this lemma:

**Lemma 8.1.** For all \( u_i, v_i \neq 0 \pmod{p} \), \( p \geq 5, t \geq 7, U, V, \) there exist \( \{x_1, \ldots, x_s\} \) with \( x_i \neq 0 \pmod{p} \) such that

\[
\begin{align*}
    u_1 x_1^2 + \ldots + u_t x_t^2 &= U \pmod{p} \\
    v_1 x_1^3 + \ldots + v_t x_t^3 &= V \pmod{p}
\end{align*}
\]

**Lemma 8.2.** For \( p > 3, a, b \) not both \( p \), \( |W_i(p, a, b)| \leq 2\sqrt{p} + 1 \)

**Proof.** Corollary 2F of \([6]\) gives

\[
\left| \sum_{r=0}^{p-1} e\left( \frac{au_i r^2 + bv_i r^3}{p} \right) \right| \leq 2p^{1/2}
\]

Now

\[
|W_i(p, a, b)| = \left| \sum_{r=1}^{p-1} e\left( \frac{au_i r^2 + bv_i r^3}{p} \right) \right|
\]

24
\[ \leq \left| \sum_{r=0}^{p-1} e\left(\frac{ar^2 + br^3}{p}\right) \right| + 1 \leq 2\sqrt{p} + 1 \]

Let \( M_t(q) \) be the number of solutions of the system

\[ u_1 x_1^2 + \ldots + u_t x_t^2 \equiv 0 \pmod{q} \]
\[ v_1 x_1^3 + \ldots + v_t x_t^3 \equiv 0 \pmod{q} \]

**Lemma 8.3.** \( M_t(p) \geq \frac{1}{p^2} \left( (p - 1)^t - (p^2 - 1)(2\sqrt{p} + 1)^t \right) \)

**Proof.**

\[ M_t(p) = \frac{1}{p^2} \sum_{r_1=1}^{p} \sum_{r_2=1}^{p} \prod_{i=1}^{t} W_i(p, r_1, r_2) \]

We have \( W_i(p, p, p) = p - 1 \) and for \( r_1, r_2 \) not both \( p, W_i(p, r_1, r_2) \leq 2\sqrt{p} + 1 \) by Lemma 8.2. Thus

\[ M(p) - \frac{(p - 1)^t}{p^2} = \frac{1}{p^2} \sum_{r_1=1}^{p} \sum_{r_2=1}^{p} \prod_{i=1}^{t} W_i(p, r_1, r_2) \]

\[ \leq \frac{1}{p^2} (p^2 - 1)(2\sqrt{p} + 1)^t \]

So we have

\[ M(p) \geq \frac{1}{p^2} \left( (p - 1)^t - (p^2 - 1)(2\sqrt{p} + 1)^t \right) \]

Taking \( t = 7 \), we get

\[ M(p) \geq \frac{1}{p^2} \left( (p - 1)^7 - (p^2 - 1)(2\sqrt{p} + 1)^7 \right) \]

This gives that \( M(p) > 0 \) for \( p > 40.58 \). This means that we now need only check that Lemma 8.1 holds for each prime smaller than 41. This is now a finite number of cases to check and thus can be verified by computer. In the following section, we note several techniques that may be employed to bring
the computational difficulty of the task into the realm of feasibility, and in Appendix A we provide Sage code for performing the computation.

It is worth noting that $t = 7$ appears to only be required for $p = 7$. It seems highly probable that $t = 5$ will suffice for all other primes; however, reducing $t$ to 5 weakens the bound of Lemma 8.3 to requiring us to check all primes less than 1193, which would require more computation than is feasible.

9 Computational Techniques

First, we note that if every pair $U, V$ modulo $p$ can be represented by the form in $t_0$ variables, then every pair can be represented by $t$ variables for $t > t_0$. So we will start our search with $t = 3$ and store the forms that represent all pairs $(U, V)$ of residue classes mod $p$. We then need only search higher values of $t$ for the forms that failed to represent all pairs of residue classes with a smaller $t$.

(The methods in this paragraph are closely modeled after those of [9].) By independently substituting $c_i x_i$ for each $x_i$, we can assume each $x_i$ is either 1 or a fixed quadratic nonresidue $c$ modulo $p$. By rearranging and multiplying by $b^{-1}$ as needed, we can assume that $u_1, \ldots, u_r = 1, u_{r+1}, \ldots, u_t = c$ with $r \geq \lceil t/2 \rceil$. By multiplying the cubic equation by $v_1^{-1}$ and rearranging, we may assume $1 = v_1 \leq v_2 \leq \ldots \leq v_t$. By substituting $-x_i$ for $x_i$ as needed, we can assume $1 \leq v_i \leq (p-1)/2$ for each $v_i$ without affecting the $u_i$.

As a final optimization, we note that if the form

\begin{align*}
  u_1 x_1^2 + \ldots + u_t x_t^2 &= U \pmod{p} \\
  v_1 x_1^3 + \ldots + v_t x_t^3 &= V \pmod{p}
\end{align*}

(24)

represents $p^2 - 1$ of the possible $p^2$ pairs of residue classes $(U, V)$ modulo $p$, then

\begin{align*}
  u_1 x_1^2 + \ldots + u_{t+1} x_{t+1}^2 &= U \pmod{p} \\
  v_1 x_1^3 + \ldots + v_{t+1} x_{t+1}^3 &= V \pmod{p}
\end{align*}

(25)

will necessarily represent all $p^2$ residue classes, since $(u_{t+1} x_{t+1}^2, v_{t+1} x_{t+1}^3)$ must represent at least two distinct pairs of residue classes, so

\begin{align*}
  u_1 x_1^2 + \ldots + u_t x_t^2 &= U - u_{t+1} x_{t+1}^2 \pmod{p} \\
  v_1 x_1^3 + \ldots + v_t x_t^3 &= V - v_{t+1} x_{t+1}^3 \pmod{p}
\end{align*}

(26)

26
will be solvable for some \((u_{t+1}, v_{t+1})\). This turns out to be quite useful: a substantial number of forms represent \(p^2 - 1\) pairs of residue classes modulo \(p\).

Using these techniques to minimize the computation needed, running the Sage code in Appendix A verifies that Lemma 8.1 holds for \(p < 41\).

10 Conclusion

Equation (16) gives us that \(R(P) \sim \mathcal{G} P^{s-5}\), and Theorem 7.1 shows that \(\mathcal{G} > 0\) uniformly over all \(u, v\) satisfying the conditions of Theorem 1.1 or Theorem 1.2. Thus \(R(P)\) is eventually positive. This can only be true if there is a solution of (1) over the primes, so we can conclude Theorems 1.1 and 1.2.

11 Acknowledgements

The author is greatly indebted to Professor Robert Vaughan for suggesting the problem, for a great deal of guidance and assistance, and for the proof of Lemma 3.1.

A Sage Code

Code: (SageMath 8.6)

```python
for p in prime_range(5,41):
    # Find a quadratic non-residue modulo p
    for i in range(1,p):
        if i not in quadratic_residues(p):
            c = i
            break
    uv_done = []
    print("p = " + str(p))

    for t in range(3,8):
        u = [0] * t
        v = [0] * t
```
for number_of_c in range(floor(t/2) + 1): # Set u
    for u_index in range(t):
        if u_index < t - number_of_c:
            u[u_index] = 1
        else:
            u[u_index] = c
skip_v = False
for v_counter in range(((p-1)/2)^(t-1)): # Set v
    v[0] = 1
    for v_index in range(1,t):
        v[v_index] = floor(v_counter % ((p-1)/2)^(v_index) / ((p-1)/2)^(v_index-1)) + 1
        if u[v_index] == u[v_index-1] and v[v_index] < v[v_index-1]:
            skip_v = True
    if skip_v == True:
        skip_v = False
    else:
        # If removing the last coefficients yields a smaller form that
        # has already passed, add this form to that list and continue
        if (u[:t-1], v[:t-1]) in uv_done:
            uv_done.append((deepcopy(u),deepcopy(v)))
        else:
            L = []
            done = False
            for i in range((p-1)^t):
                if done:
                    break;
                x = [None] * t
                for j in range(t): # Set x
                    x[j] = floor(i % (p-1)^(j+1) / (p-1)^j) + 1
                a = 0
                b = 0
                for k in range(t):
                    a = mod(a + u[k]*x[k]^2, p)
                    b = mod(b + v[k]*x[k]^3, p)
                inL = False
                for pair in L:
                    if (pair[0] == a and pair[1] == b):
                        inL = True
                        break;
                # If the pair (a, b) has not already been represented
                L.append((a, b))
                break;
# by this form, store that it can be
if inL == False:
    L.append((a,b))
    if len(L) == p^2:
        done = True

# Uncomment this line to print information on each form
#print("u: " + str(u) + " v: " + str(v) + " " + str(len(L)))

# If the form represents all pairs (a, b), add it to the list
if done:
    uv_done.append((deepcopy(u), deepcopy(v)))
# If the form represents all pairs (a, b) but one, add it
elif len(L) == p^2-1 and t < 7:
    uv_done.append((deepcopy(u), deepcopy(v)))
else:
    if t == 7:
        print("u: " + str(u) + " v: " + str(v) + "fails.")
print("Search complete")

Output:

p = 5
p = 7
p = 11
p = 13
p = 17
p = 19
p = 23
p = 29
p = 31
p = 37
Search complete

References

[1] Bourgain, J., Demeter, C. & Guth, L., Proof of the main conjecture in Vinogradov’s Mean Value Theorem for degrees higher than three, Annals of Mathematics, 184, no. 2, 633-682, 2016.
[2] Brdern, J. & Cook, R., *On simultaneous diagonal equations and inequalities*, Acta Arith., 62, no. 2, 125-149, 1992.

[3] Cook, R. J. *Simultaneous quadratic equations*, J. London Math. Soc. (2) 4, 319-326, 1971.

[4] Hua, L. K., *Additive Theory of Prime Numbers*, American Math. Soc., Providence, Rhode Island, 1965.

[5] Rogovskaya, N. N., *An asymptotic formula for the number of solutions of a system of equations*. Diophantine approximations, Part II (Russian), 7884, Moskov. Gos. Univ., Moscow, 1986.

[6] Schmidt, W. M., *Equations over finite fields. An elementary approach*. Lecture notes in Mathematics, 536 Springer-Verlag, Berlin, 1976.

[7] Vaughan, R. C., *The Hardy-Littlewood Method*, 2nd edition, Cambridge University Press, Cambridge, 1997.

[8] Wooley, T. D., *The cubic case of the main conjecture in Vinogradov’s mean value theorem*, Advances in Mathematics, 294, 532-561, 2016.

[9] Wooley, T. D., *On simultaneous additive equations, I*, Proc. London Math. Soc. (3) 63 (1991), no. 1, 1-34.

[10] Wooley, T. D., *On simultaneous additive equations, II*, J. Reine. Angew. Math. 419 (1991), 141-198.

[11] Wooley, T. D., *Rational Solutions of Pairs of Diagonal Equations, One Cubic and One Quadratic*, Proc. Lond. Math. Soc. (3) 110 (2015) 325-356.