REPRESENTATION OF INTEGERS
BY A FAMILY OF CUBIC FORMS
IN SEVEN VARIABLES

A Dissertation in
Mathematics
by
Manoj Verma

© 2013 Manoj Verma

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

May 2013
The dissertation of Manoj Verma was reviewed and approved* by the following:

Robert C. Vaughan  
Professor of Mathematics  
Dissertation Advisor, Chair of Committee

W. Dale Brownawell  
Distinguished Professor of Mathematics

Ae Ja Yee  
Associate Professor of Mathematics

Donald P. Richards  
Professor of Statistics

Yuxi Zheng  
Professor of Mathematics  
Head of the Department of Mathematics

*Signatures are on file in the Graduate School.
Abstract

Under certain conditions on the coefficients, we derive asymptotic formulas for the number of representations of zero inside a box $|x_i| \leq P$ where $P$ is a large positive integer and for the number of representations of a large positive integer $N$ with each $x_i \in I$ where $I = \{1, 2, \ldots, P\}$ or $\{0, 1, 2, \ldots, P\}$ or $\{-P, \ldots, -1, 0, 1, \ldots, P\}$ where $P = \lfloor N^{1/3} \rfloor$ by the cubic forms that can be written as

$$L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) + L_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) + a_7x_7^3$$

where $L_1$ and $L_2$ are linear forms, $Q_1$ and $Q_2$ are quadratic forms and $a_7$ is a non-zero integer.
# Table of Contents

Acknowledgments vi

Chapter 1  
**Introduction** 1  
1.1 Waring’s problem 1  
1.2 The Hardy-Littlewood method 3  
1.3 Additive equations 6  
1.4 General homogeneous equations 7  
1.5 Cubic forms 8

Chapter 2  
**The treatment of the minor arcs** 11  
2.1 The statement of the results 11  
2.2 The setup for the circle method 14  
2.3 Auxiliary transformations 16  
2.4 The contribution from the minor arcs 18

Chapter 3  
**The major arcs** 21  
3.1 The generating function 21  
3.2 The singular integral 24  
3.3 The singular series 24  
3.4 The proofs of theorems 1 and 3 30

Chapter 4  
**The $p$-adic problem** 31  
4.1 The congruence condition 31  
4.2 The congruence $L_1Q_1 \equiv N \pmod{p}$ 33  
4.3 The congruence $L_1Q_1 \equiv N \pmod{p^r}$ 37  
4.4 Completion of the proof of theorem 2 38
Acknowledgments

First and foremost, I would like to thank my adviser, Professor Robert C. Vaughan, for his continuous guidance and support, unlimited patience and understanding, and generosity in giving his time and new ideas. Only a little of what I have learned from him, inside and outside Mathematics, has come to materialization in this dissertation but I hope that this is a late blooming for me and more will come in future; I have reasons to be thankful to him throughout my life.

Being in a Graduate school anywhere and being in another country with a completely different culture—either of them would be some sort of challenge to anyone. Some of my old friends and some friends I made here provided me emotional support or a break from routine when I needed it; I would like to thank them all, especially Samarth Rastogi, Abhishek Agarwal, Gyan P. Srivastava, Brijesh K. Rai, Amit Priyadarshi, Yogender Singh, Vijaykumar H. Singh, Arun Kumar, Ganesh Kadu, Sartaj-ul-Hasan, Nolen Ryba, Jingjing Huang, Evegeny Mayanskiy and Shilpak Banerjee.

Although this dissertation might not seem to be an achievement at all to an accomplished mathematician, it was a long way from where I started and I owe most to my parents for it. Few people in the world are fortunate enough to have great parents who started poor but worked hard, made progress in their own lives and, with uncanny parenting skills, raised three kids each of whom has made a generation’s worth of advancement in life.
Chapter 1

Introduction

1.1 Waring’s problem

In his *Meditationes algebraicae* (1770), Edward Waring stated without proof that every natural number is a sum of at most nine positive integral cubes, also a sum of at most 19 biquadrates, and so on. It is assumed that he meant to assert that for every natural number $k \geq 2$ there exists a number $s$ such that every natural number is a sum of $s$ $k$th powers of non-negative integers and that if $g(k)$ denotes least such $s$, then $g(3) = 9$ and $g(4) = 19$.

Building on earlier work of Euler, Lagrange proved in 1770 that every positive integer is a sum of four squares. The square of any integer is congruent to 0, 1 or 4 modulo 8 and hence no natural number congruent to 7 modulo 8 can be a sum of three squares. Thus Lagrange’s Theorem implies that $g(2) = 4$. The existence of $g(k)$ for many values of $k$ was proved in the 19th century but the existence of $g(k)$ for all $k$ was proved only in 1909 by Hilbert [29]. However, his method does not give the value of $g(k)$ and indeed gives a very poor upper bound.

Incidentally, it was proved that $g(3) = 9$ by Weiferich [48] in 1909 (a mistake in his proof was corrected by Kempner [32] in 1912) and soon Landau [33] proved that all but finitely many natural numbers are a sum of eight cubes. Dickson [21] proved in 1939 that all natural numbers except 23 and 239 are a sum of eight cubes. Linnik [35] proved in 1943 that every sufficiently large positive integer is a sum of seven cubes and Watson [46] gave a very short and elegant proof of this. However, we seem to be quite far from being able to prove the conjecture that
every integer greater than 7373170279850 is a sum of four cubes [19].

A good lower bound on \( g(k) \) is easily obtained by considering the integer

\[
n = 2^k \left\lceil \left( \frac{3}{2} \right)^k \right\rceil - 1.
\]

Since \( n < 3^k \), any representation of \( n \) as a sum of \( k \)th powers can involve only \( k \)th powers of 1 and 2 and the minimal number of terms results by taking \( \left\lceil \left( \frac{3}{2} \right)^k \right\rceil - 1 \) \( k \)th powers of 2 and \( 2^k - 1 \) \( k \)th powers of 1. Thus

\[
g(k) \geq 2^k + \left\lceil \left( \frac{3}{2} \right)^k \right\rceil - 2.
\]

However, for larger natural numbers many more choices of summands are available in a representation as a sum of \( k \)th powers and thus the more interesting (and much more difficult) problem is the estimation of \( G(k) \), the smallest \( s \) such that every sufficiently large natural number is a sum of at most \( s \) \( k \)th powers of natural numbers. It can be shown easily that \( G(k) \geq k + 1 \). Thus \( G(2) = 4 \) and \( 4 \leq G(3) \leq 7 \).

In the 1920s Hardy and Littlewood developed an analytic method that can be adapted to attack many additive problems including Waring’s problem and the Goldbach ternary problem. The method has its origin in a paper of Hardy and Ramanujan [23] concerned mostly with the partitions of numbers but also with the representation of numbers as sums of squares. Hardy and Littlewood were able to prove that the number of representations of a natural number \( N \) as a sum of \( s \) \( k \)th powers of natural numbers, say \( R_{s,k}(N) \), satisfies

\[
R_{s,k}(N) = \frac{(\Gamma(1 + \frac{1}{k}))^s}{\Gamma(\frac{1}{k})} \mathfrak{S}_{s,k}(N) N^{s/k-1} + O(N^{s/k-1-\delta}) \tag{1.1}
\]

for some \( \delta > 0 \) provided \( s \geq (k - 2)2^{k-1} + 5 \). Here \( \mathfrak{S}_{s,k}(N) \) is an infinite series of purely arithmetical nature reflecting the density of solutions of some congruences and is bounded below uniformly in \( N \) for \( s \geq 4k \) (when \( s \) is not a power of 2, \( s \geq 2k \) is more than sufficient). This implies that \( G(k) \leq (k - 2)2^{k-1} + 5 \) and gives a more insightful and transparent proof of Hilbert’s theorem. Hardy and Littlewood were
able to find a better bound on $G(k)$ by proving the asymptotic formula for special type of representations of $N$ as a sum of $k$th powers. Some technical simplifications, mainly consisting of replacing power series by finite exponential sum, and further remarkable progresses were made later by Vinogradov. For references to the work of Hardy and Littlewood and of Vinogradov, see the bibliography in [44].

The fundamental work of Hardy and Littlewood became the basis for some rather tedious but often very ingenious calculations by Dickson, Pillai and others during the 1930s and early 1940s, and the values of $g(k)$ for all $k \geq 6$ were found. Chen [11] proved in 1964 that $g(5) = 37$; Balasubramanian, Deshouillers and Dress [2, 3] proved in 1986 that $g(4) = 19$. Incidentally, Davenport [14] had already proved in 1939 that $G(4) = 16$. Deshouillers, Kawada and Wooley [20] proved in 2005 that every integer greater than 13792 is a sum of 16 biquadrates. As of now, no improvement on Linnik’s result that $4 \leq G(3) \leq 7$ has been made though it was already proved by Davenport [13] that the number of natural numbers less than $X$ which are not a sum of four cubes is $O(X^{29/30+\varepsilon})$. Also, the value of $G(k)$ for no $k > 4$ is known though upper bounds on them have been improved greatly by Vaughan and Wooley over the past 25 years. See the survey article on Waring’s problem by Vaughan and Wooley [45] for references.

1.2 The Hardy-Littlewood method

Here we give a brief description of the Hardy-Littlewood method, as simplified by Vinogradov, in the context of Waring’s problem. For details, see [16] or [44].

In any representation of a positive integer $N$ in the form

$$N = x_1^k + \ldots + x_s^k \quad (1.2)$$

with $x_i$ positive integers, we must have each $x_i \leq \lfloor N^{1/k} \rfloor$. Accordingly, we define $P = \lfloor N^{1/3} \rfloor$ and

$$F(\alpha) = \sum_{x=1}^{P} e(\alpha x^k). \quad (1.3)$$
From the trivial orthogonality relation
\[
\int_0^1 e(\alpha h) \, d\alpha = \begin{cases} 1 & \text{for } h = 0 \\ 0 & \text{for } h \neq 0 \end{cases},
\]
it follows that the number of representations of \( N \) in the form (1.2) is
\[
R_{s,k}(N) = \int_0^1 F(\alpha)^s e(-N\alpha) \, d\alpha.
\] (1.4)

The plan for estimating this integral is to divide the unit interval into major arcs, which contribute to the main term in the asymptotic formula, and minor arcs, the contribution of which can be bounded by a term of smaller order and goes into the error term. The distinction between major and minor arcs depends on the problem at hand, the results available, and is also somewhat a matter of personal choice. In our case we can choose them as follows. Let \( \delta \) be a sufficiently small positive real number. For \( 1 \leq q \leq P^\delta, \ 1 \leq a \leq q, \ (a,q) = 1 \), define the major arc \( \mathcal{M}(q,a) \) by
\[
\mathcal{M}(q,a) = \left\{ \alpha : \left| \alpha - \frac{a}{q} \right| \leq P^{\delta-k} \right\}
\] (1.5)
and let \( \mathcal{M} \) be the union of the \( \mathcal{M}(q,a) \). The set \( \mathfrak{m} = (P^{\delta-k}, 1 + P^{\delta-k}] \setminus \mathcal{M} \) then forms the minor arcs.

For \( \alpha \in \mathcal{M}(q,a) \), writing \( \alpha = \frac{a}{q} + \beta \), dividing the sum (1.3) according to residue class of \( x \) modulo \( q \) it is seen that \( F(\alpha) \) can be approximated quite well by \( q^{-1} S(q,a) v(\beta) \) where
\[
S(q,a) = \sum_{\substack{a=1 \\ (a,q)=1}}^q e\left(\frac{ax^k}{q}\right)
\]
and
\[
v(\beta) = \int_0^P e(\beta \xi^k) \, d\xi.
\]
After some work, this leads to
\[
\int_{\mathfrak{m}} F(\alpha)^s e(-N\alpha) \, d\alpha = \mathfrak{G}_{s,k}(N) J_{s,k}(N) + O(N^{s/k-1-\delta})
\]
where
\[ J_{s,k}(N) = \int_{-\infty}^{\infty} v(\beta)^s e(-N\beta) d\beta \]
and
\[ \mathcal{S}_{s,k}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \atop (a,q)=1}}^{q} (q^{-1}S(q,a))^s e(-aN/q) \]
are what Hardy and Littlewood called the singular integral and the singular series, respectively. The singular integral contains the information about the density of real solutions of (1.2) while the singular series contains the information about the density of $p$-adic solutions of (1.2). It can be shown that, for some $\delta > 0$,
\[ J_{s,k}(N) = \left( \Gamma(1 + \frac{1}{k}) \right)^s \frac{N^{s/k-1}}{\Gamma(\frac{s}{k})} + O(N^{s/k-1-\delta}) \]
provided $s > k$, and that $1 \ll \mathcal{S}_{s,k}(N) \ll 1$ provided $s \geq 4k$.

Hardy and Littlewood were able to prove that $F(\alpha)$ is much smaller than $P$ for $\alpha \in m$ through an argument having its origin in Weyl’s [49] fundamental work on the uniform distribution of sequences of real numbers modulo 1. In 1938 Hua [31] proved that for $1 \leq j \leq k$ we have the mean value estimate
\[ \int_{0}^{1} (\alpha)^{2j} e(-N\alpha) d\alpha \ll P^{2j-j+\varepsilon}. \]
This leads to the minor arc estimate
\[ \int_{m} (\alpha)^{s} e(-N\alpha) d\alpha \ll N^{s/k-1-\delta} \]
valid for $s \geq 2^k + 1$ proving the asymptotic formula (1.1) and that $G(k) \leq 2^k + 1$.

Using more complicated ideas and techniques, asymptotic formulas for $R_{s,k}(N)$ have been proved for $s = 2^k$ for $k \geq 3$ by Vaughan [40, 41, 42], for $s = \frac{7}{8}2^k + 1$ for $k \geq 6$ by Heath-Brown [26, 27] and for $s = \frac{7}{8}2^k$ for $k \geq 6$ by Boklan [7]. For larger $k$, better results are available due to work of Vinogradov, Vaughan, Wooley and others. See again the survey article on Waring’s problem by Vaughan and Wooley [45] for the history and references.
1.3 Additive equations

The solution of Waring’s problem via the Hardy-Littlewood method can be easily adapted to the problem of representation of a large positive integer \( N \) in the form

\[
N = c_1 x_1^k + \ldots + c_s x_s^k
\]

(1.6)

where \( c_1, \ldots, c_s \) are given positive integers with \( x_1, \ldots, x_s \) positive integers to obtain results of the same strength as in the case of Waring’s problem except that now, it does not matter how large one takes \( s \) to be, there are choices for \( c_1, \ldots, c_s \) so that for an infinite set of values of \( N \) there are no solutions. But for large enough \( s \) and \( N \) the obstruction is purely a local one, that is, the equation (1.6) has solutions if \( s \) and \( N \) are large enough in terms of \( k \) and for each prime \( p \) and positive integer \( \nu \) the congruence

\[
c_1 x_1^k + \ldots + c_s x_s^k \equiv N \pmod{p^\nu}
\]

has solutions with not all the terms \( c_1 x_1^k, \ldots, c_s x_s^k \) divisible by \( p \).

The equation

\[
c_1 x_1^k + \ldots + c_s x_s^k = 0
\]

(1.7)

where \( c_1, \ldots, c_s \) are given non-zero integers, not all of the same sign when \( k \) is even, with \( x_1, \ldots, x_s \) integers can also be treated in the same fashion except that now there are no natural restrictions on the sizes of the integers \( x_1, \ldots, x_s \) so we choose a large number \( P \) and consider the number of solutions of (1.7) either in the box \( |x_i| \leq \left[ P/(c_i^{1/k}) \right], 1 \leq i \leq s \) or in the box \( 1 \leq x_i \leq \left[ P/(c_i^{1/k}) \right], 1 \leq i \leq s \). Also, now the singular series depends only on \( k \) and the coefficients \( c_1, \ldots, c_s \). Davenport and Lewis [17] showed that the singular series corresponding to (1.7) is positive for any choice of the coefficients \( c_1, \ldots, c_s \) (all non-zero, not all of the same sign when \( k \) is even) if \( s \geq k^2 + 1 \) and pointed out that when \( k + 1 \) is a prime \( p \) the last condition is the best possible as can be seen from the congruence

\[
x_1^k + \ldots x_k^k + p(x_{k+1}^k + \ldots x_{2k}^k) + \ldots + p^{k-1}(x_{k^2-k+1}^k + \ldots x_{k^2}^k) \equiv 0 \pmod{p^k}.
\]
They also showed that (1.7) has non-trivial solutions when \( s \geq k^2 + 1 \) and either \( k \leq 6 \) or \( k \geq 18 \). This gap has been removed by Vaughan, and in fact methods of Vaughan and Wooley developed for dealing with Waring’s problem can be adapted to show that far fewer variables are sufficient to ensure that (1.7) has a non-trivial solution provided the congruence conditions are met. (See the foreword to [16] for references).

In case \( k = 3 \), using ideas from Vaughan [40], Baker [1] has shown that every diagonal cubic form in \( s \geq 7 \) variables has a non-trivial rational zero although an asymptotic formula has been proved only for diagonal cubic forms in \( s \geq 8 \) variables due to Vaughan [40]. In case \( k = 3, s = 7 \) only a lower bound of the expected order has been established by Vaughan [43]. Incidentally, the diagonal cubic form in six variables

\[
x_1^3 + 2x_2^3 + 7(x_3^3 + 2x_4^3) + 49(x_5^3 + 2x_6^3)
\]

has no non-trivial zero in \( \mathbb{Q}_7 \). However, Swinnerton-Dyer [39] has proved on the assumption of the finiteness of the Tate-Shafarevich group for elliptic curves over \( \mathbb{Q}(\sqrt{-3}) \) that (1.7) has non-trivial solutions when \( k = 3, s \geq 5 \) and the congruence conditions are satisfied. For \( k = 3, s = 4 \) Cassels and Guy [10] have found the example

\[5x_1^3 + 9x_2^3 + 10x_3^3 + 12x_4^3 = 0\]

which satisfies the congruence conditions but has no non-trivial solution in integers.

### 1.4 General homogeneous equations

Let \( f(x_1, \ldots, x_n) \) be a form of degree \( k \) with integer coefficients. It is natural to ask whether the equation \( f(x_1, \ldots, x_n) = 0 \) has a non-trivial solution. When \( k = 2 \), a complete answer is given by the Hasse-Minkowski theorem which asserts that a quadratic form has a non-trivial solution in integers if and only if it has non-trivial solutions in \( \mathbb{R} \) and in each \( p \)-adic field \( \mathbb{Q}_p \). There are counterexamples to such a “local-to-global” principle for forms of higher degree such as \( 3x_1^3 + 4x_2^3 + 5x_3^3 = 0 \) found by Selmer [38] but it is conjectured that such a principle might hold for \( k \) odd when \( n \) is large enough in terms of \( k \).
It so happens that non-trivial $p$-adic solutions always exist if $n$ is sufficiently large in terms of $k$; $n \geq 5$ is sufficient for $k = 2$, $n \geq 10$ is sufficient for $k = 3$ but no good upper bound is known for $k \geq 4$. (See chapters 11, 18 and the foreword to [16] for more details.) When $k$ is odd, non-trivial real solutions exist as soon as $n > 1$. In fact, building on the solubility of (1.7) for $s$ large enough in terms of $k$, Birch [5] proved the following: For any natural numbers $j, l$ and odd natural numbers $k_1, \ldots, k_j$, there exists a number $n_0(k_1, \ldots, k_j; l)$ such that any $j$ given forms in $(x_1, \ldots, x_n)$ of degrees $k_1, \ldots, k_j$ vanish simultaneously on some subspace of $\mathbb{Q}^n$ of dimension at least $l$ provided $n \geq n_0(k_1, \ldots, k_j; l)$. However, the $n_0$ produced via Birch’s proof are enormous even in case of a single cubic form.

### 1.5 Cubic forms

Before Birch gave his theorem, Lewis [34] had proved that any cubic form with integer coefficients in sufficiently many variables has a non-trivial rational zero by supplementing a result of Brauer with arguments from algebraic number theory. (Brauer [8] had shown that the solubility of a system of homogeneous equations of degrees $\leq k$ over any field in sufficiently large number of variables follows from the solubility of additive equations of degrees $\leq k$ in sufficiently large number of variables over that field.) Davenport, adapting the circle method to this non-additive context, proved in 1957 that 32 variables are in fact sufficient (although the result was not published until 1962) and improved it to 29 variables in 1962 and finally to 16 variables in 1963. The last result is considered one of Davenport’s finest achievements; it was improved only in 2007 by Heath-Brown [28] to 14 variables. It is conjectured that 10 variables are sufficient. Davenport and Heath-Brown used the circle method to establish their results. They do not obtain an asymptotic formula for the number of zeros of cubic forms in a box in all the cases. Instead they consider two alternatives: in one the cubic form has non-trivial zeros for “geometric reasons”, in the other they establish the asymptotic formula.

For non-singular cubic forms Heath-Brown [25] has shown that 10 variables are indeed sufficient. There are examples of non-singular cubic forms in 9 variables for which non-trivial $p$-adic zeros do not exist for all $p$. However, Hooley [30] has established the local-to-global principle for non-singular cubic forms in 9 variables.
Currently it is conjectured that the local-to-global principle holds for non-singular cubic forms in \( n \) variables if \( n \geq 5 \).

When \( n=3 \) or \( 4 \), a local-to-global principle is conjectured to hold for cubic forms (non-singular as well as singular) in case the Brauer-Manin obstruction is empty. For singular cubic forms with \( 5 \leq n \leq 9 \), the situation is more uncertain although, in an unpublished work, Salberger has shown that the Brauer-Manin obstruction for singular cubic forms is empty, for any \( n \), except perhaps when the singular locus has co-dimension 2 or 3.

The “square-root barrier” \([24]\) means that the circle method cannot be expected to give an asymptotic formula for a cubic form in less than 7 variables. Thus it is of interest to apply the method to some families of cubic forms in 7, or even 8, variables. Br"udern and Wooley \([9]\) considered the sum of four non-degenerate binary cubic forms and proved a lower bound of the order \( P^{5-\varepsilon} \) and an upper bound of the order \( P^{5+\varepsilon} \). In 1962 Birch, Davenport and Lewis \([6]\) found an asymptotic formula for the number representations of zero in a box \( |x_i| \leq P \) by cubic forms in seven variables of the type

\[
N_1(x_1, x_2, x_3) + N_2(x_4, x_5, x_6) + a_7x_7^3
\]

where \( N_1 \) and \( N_2 \) are norm forms of some cubic field extensions of \( \mathbb{Q} \). In 2010 Harvey \([24]\) considered the case in which the last two terms are replaced by a diagonal cubic form in four variables or a sum of two non-degenerate binary cubic forms; in the first case he obtained an asymptotic formula while in the second case only a lower bound of the order \( P^{4-\varepsilon} \) and an upper bound of the order \( P^{4+\varepsilon} \) were obtained.

After the work of Davenport \([13]\) and Linnik \([35]\) on Waring’s problem for cubes, the problem of representation of large positive integers by cubic forms has been considered albeit only occasionally. An asymptotic formula for the number of representations as a sum of eight cubes and a lower bound of the expected order for the number of representations as a sum of seven cubes have been established by Vaughan \([40, 43]\). In 1952 Watson \([47]\) studied the representation of large numbers by a class of diagonal cubic forms in seven variables. Davenport defined \( h(C) \), the \( h \)-invariant of a cubic form \( C \), as the smallest integer \( h \) such that \( C \) can be written
in the form

\[ C(\mathbf{x}) = L_1(\mathbf{x})Q_1(\mathbf{x}) + \ldots + L_h(\mathbf{x})Q_h(\mathbf{x}) \]

where \( L_i(\mathbf{x}) \) are linear forms and \( Q_i(\mathbf{x}) \) are quadratic forms. In 1967 Pleasants [37] studied the representation of integers by general cubic forms \( C(x_1, \ldots, x_n) \) when \( h^*(C) \geq 8 \) so that the techniques developed in Davenport [15] and Davenport and Lewis [18] could be applied; here \( h^*(C) \) is defined as the largest integer such that there is a non-singular linear transformation taking \( C(\mathbf{x}) \) into a cubic form \( C'(\mathbf{y}) \) such that

\[ C' = C'_1 + \ldots + C'_r \]

where \( C'_1, \ldots, C'_r \) are cubic forms in disjoint sets of variables and

\[ h(C'_1) + \ldots + h(C'_r) = h^*. \]

It follows that \( h(C) \leq h^*(C) \leq n \). Pleasants proved that a cubic form \( C \) represents almost all integers satisfying the congruence conditions provided \( h^*(C) \geq 12 \) and it represents a positive proportion of integers provided \( h^*(C) \geq 8 \). The work of Brüdern and Wooley [9] implies that a sum of two non-degenerate binary cubic forms represents almost all integers satisfying the congruence conditions.

In this dissertation, we consider the class of non-diagonal cubic forms in seven variables that can be written as

\[ f(\mathbf{x}) = L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) + L_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) + a_7x_7^3 \]

where \( L_1, L_2 \) are linear forms in three variables, \( Q_1, Q_2 \) are quadratic forms in three variables and \( a_7 \) is a non-zero integer. It might be interesting to note that this cubic form in singular and the \( h \)-invariant of this cubic form is 3. We apply the Hardy-Littlewood circle method and, under certain conditions on the coefficients, obtain asymptotic formulas for the number of representations of zero inside a box \( |x_i| \leq P \) where \( P \) is a large positive integer, and for the number of representations of a large positive integer \( N \) with each \( x_i \in I \) where \( I = \{1, 2, \ldots, P\} \) or \( \{0, 1, 2, \ldots, P\} \) or \( \{-P, \ldots, -1, 0, 1, \ldots, P\} \) where \( P = \lfloor N^{1/3} \rfloor \).
Chapter 2

The treatment of the minor arcs

2.1 The statement of the results

We consider the class of non-diagonal cubic forms in seven variables of the type

$$f(x) = L_1Q_1 + L_2Q_2 + a_7x_7^3$$  \hspace{1cm} (2.1)

where, in case the arguments are not mentioned explicitly, as here,

\[ L_1 = L_1(x_1, x_2, x_3) = a_1x_1 + a_2x_2 + a_3x_3, \]
\[ L_2 = L_2(x_4, x_5, x_6) = a_4x_4 + a_5x_5 + a_6x_6 \]

are linear forms in three variables,

\[ Q_1 = Q_1(x_1, x_2, x_3) = A_1x_1^2 + A_2x_2^2 + A_3x_3^2 + B_1x_2x_3 + B_2x_3x_1 + B_3x_1x_2, \]
\[ Q_2 = Q_2(x_4, x_5, x_6) = A_4x_4^2 + A_5x_5^2 + A_6x_6^2 + B_4x_5x_6 + B_5x_6x_4 + B_6x_4x_5 \]

are quadratic forms in three variables and \(a_7\) is a non-zero integer. We apply the Hardy-Littlewood circle method and, under certain conditions on the coefficients, obtain asymptotic formulas for the number of representations of zero inside a box \(|x_i| \leq P\) where \(P\) is a large positive integer, and for the number of representations of a large positive integer \(N\) with each \(x_i \in I\) where \(I = \{1, 2, \ldots, P\}\) or \(\{0, 1, 2, \ldots, P\}\) or \(\{-P, \ldots, -1, 0, 1, \ldots, P\}\) where \(P = \lfloor N^{1/3} \rfloor\).
Some conditions on $N$ for a given $f$, or on the coefficients of $f$ for a given $N$, are necessary in order that such a representation exist. The congruence conditions are described explicitly in Theorem 2. In view of the examples such as

$$(-x_1 - x_2 - x_3)(x_1^2 + x_2^2 + x_3^2) - x_4x_5x_6 - x_7^3,$$

when considering the representation of large positive integers with $x_i$ restricted to be positive or non-negative, we will assume that $f(x_1, \ldots, x_7)$ is positive for a positive proportion of 7-tuples $(x_1, \ldots, x_7)$ with $1 \leq x_i \leq P$. By homogeneity and continuity of $f$ as a function of 7 real variables, this is equivalent to assuming that $f(x_1, \ldots, x_7) > 0$ for some $(x_1, \ldots, x_7) \in \mathbb{R}_+^7$. No such condition would be needed if we allow the $x_i$ to take non-positive values as well and require only that $|x_i| \leq N^{1/3}$.

For our proof of the minor arc estimate to work we need to assume that the quantity $\Delta_1\Delta_2$ is non-zero where

$$\Delta_1 = a_1M_1a_1^T \quad (2.2)$$

where $a_1 = (a_1, a_2, a_3)$ and $M_1$ is the matrix of the adjoint of the quadratic form $2Q_1$, that is,

$$M_1 = \begin{bmatrix}
B_1^2 - 4A_2A_3 & 2A_3B_3 - B_1B_2 & 2A_2B_2 - B_1B_3 \\
2A_3B_3 - B_1B_2 & B_2^2 - 4A_1A_3 & 2A_1B_1 - B_2B_3 \\
2A_2B_2 - B_1B_3 & 2A_1B_1 - B_2B_3 & B_3^2 - 4A_1A_2
\end{bmatrix},$$

and $\Delta_2$ is defined similarly. We intend to pursue the case in which $\Delta_1\Delta_2 = 0$ but $L_1Q_1, L_2Q_2$ are non-degenerate cubic forms in future. Since our assumptions about $L_1Q_1$ and $L_2Q_2$ are similar, any statement proved for $L_1Q_1$ applies to $L_2Q_2$ as well with a similar proof.

In what follows, as is usual in analytic number theory, $e(\alpha) = e^{2\pi i \alpha}$ and $\varepsilon$ can take any positive real value in any statement in which it appears. The symbols $\ll$ and $O$ have their usual meanings with the implicit constants depending on the cubic form $f$ and $\varepsilon$; any other dependence will be mentioned explicitly through subscripts. We prove the following.
Theorem 1. If $\Delta_1, \Delta_2 \neq 0$ for the cubic form $f$ in (2.1), then the number of representations $R(N)$ of a large positive integer $N$ by $f$ with $x_i \in I$ satisfies

$$R(N) = N_1N_2\chi(N) + N^{4/3}\mathcal{G}(N)J_i + O(N^{4/3-1/48+\varepsilon})$$

where

$$N_1 = N_1(I) = \text{Card}\{(x_1, x_2, x_3) : x_1, x_2, x_3 \in I \text{ and } L_1Q_1 = 0\}, \quad (2.3)$$

$$N_2 = N_2(I) = \text{Card}\{(x_4, x_5, x_6) : x_4, x_5, x_6 \in I \text{ and } L_2Q_2 = 0\}, \quad (2.4)$$

$$\chi(N) = \begin{cases} 1 & \text{if } N = a_7x^3 \text{ for some } x \in I \\ 0 & \text{otherwise} \end{cases} \quad (2.5)$$

is the indicator function of the set $T = \{a_7x^3 : x \in I\}$,

$$\mathcal{G}(N) = \sum_{q=1}^{\infty} \sum_{\substack{a=1 \\ (a,q)=1}} q^{-7}S(q,a)e(-aN/q) \text{ with } S(q,a) = \sum_{z \mod q} e\left(\frac{aq}{q}f(z)\right),$$

$$i = \begin{cases} 1 & \text{if } I = \{1,2,\ldots,P\} \text{ or } \{0,1,2,\ldots,P\} \\ 2 & \text{if } I = \{-P,\ldots,-1,0,1,\ldots,P\} \end{cases},$$

$$J_1 = \int_{-\infty}^{\infty} \left(\int_{[0,1]^7} e(\gamma f(\xi)) d\xi\right) e(-\gamma)d\gamma$$

and

$$J_2 = \int_{-\infty}^{\infty} \left(\int_{[-1,1]^7} e(\gamma f(\xi)) d\xi\right) e(-\gamma)d\gamma.$$ 

Here, $J_2 > 0$; $J_1 > 0$ if $f(x_1,\ldots,x_7) > 0$ for some $(x_1,\ldots,x_7) \in \mathbb{R}^T_{\geq 0}$, $J_1 = 0$ otherwise; $1 \ll \mathcal{G}(N) \ll 1$ if the equation $f(x) = N$ has $p$-adic solutions for all primes $p$, $\mathcal{G}(N) = 0$ otherwise.

Note that $N_1, N_2$ defined in (2.3), (2.4) depend not only on $L_1Q_1$ and $L_2Q_2$ but also on $I$ and can change significantly depending on whether we allow $x_i$ to be zero (e.g. consider $L_1Q_1 = x_1x_2x_3$, $L_2Q_2 = x_4x_5x_6$). In case $I = \{-P,\ldots,P\}$, $N_1(I) = C_1P^2 + O(P^{1+\varepsilon})$ and $N_2(I) = C_2P^2 + O(P^{1+\varepsilon})$ with $C_1, C_2$ positive constants that depend on $L_1Q_1$ and $L_2Q_2$ respectively. In any case, $0 \leq N_1, N_2 \ll P^2$. 
Theorem 2. If \( f(x) = c(L_1'Q_1' + c_2L_2'Q_2' + c_3x_3^3) \) where \( c \) is the content of \( f \) while \( L_1'Q_1' \), \( L_2'Q_2' \) have content \( 1 \), then the equation \( f(x) = N \) has \( p \)-adic solutions for all primes \( p \) if the congruence

\[
f(x) \equiv N \pmod{c \prod_{p|3c_1c_2c_3} p^{\gamma(p)}}
\]

has a solution; such a solution does exist if \( N \) is divisible by \( c \prod_{p|3c_1c_2c_3} p^{\gamma(p)} \). For each prime \( p|3c_1c_2c_3 \), \( \gamma(p) \) and \( \gamma'(p) \) are defined explicitly in terms of the coefficients of \( f \) through equations (4.11), (4.12) and lemma 4.3.1.

Theorem 3. If \( \Delta_1, \Delta_2 \neq 0 \) for the cubic form (2.1), then the number \( R(0; P) \) of solutions of \( f(x) = 0 \) in the box \( |x_i| \leq P \) satisfies

\[
R(0; P) = N_1(P)N_2(P) + P^4 \mathcal{G}_0J_0 + O(P^{4-1/16+\varepsilon})
\]

where

\[
N_1(P) = \text{Card}\{(x_1, x_2, x_3) : |x_1|, |x_2|, |x_3| \leq P \text{ and } L_1Q_1 = 0\}, \quad (2.6)
\]

\[
N_2(P) = \text{Card}\{(x_4, x_5, x_6) : |x_4|, |x_5|, |x_6| \leq P \text{ and } L_2Q_2 = 0\}, \quad (2.7)
\]

\[
\mathcal{G}_0 = \sum_{q=1}^{\infty} \sum_{a=1}^{q} q^{-7}S(q,a) \text{ with } S(q,a) = \sum_{z \mod q} e\left(\frac{aq}{q}f(z)\right)
\]

and

\[
J_0 = \int_{-\infty}^{\infty} \left( \int_{[-1,1]^7} e(\gamma f(\xi)) d\xi \right) d\gamma.
\]

Note that in (2.3), (2.4) and also in (2.6), (2.7) we have

\[
0 \leq N_1, N_2 \ll P^2. \quad (2.8)
\]

2.2 The setup for the circle method

In what follows, we take \( P \) to be any large positive number when considering representations of zero; we take \( P = \lfloor N^{1/3} \rfloor \) when considering representations of a large positive integer \( N \). \( I \) denotes the set of values \( x_i \) are allowed to take;
$\mathfrak{B} = [0,1]^7$ in case $I = \{1,2,\ldots,P\}$ or $\{0,1,2,\ldots,P\}$; $\mathfrak{B} = [-1,1]^7$ in case $I = \{-P,\ldots,-1,0,1,\ldots,P\}$; $N_1,N_2,\chi(\cdot)$ are as defined in (2.3),(2.4),(2.5).

Let $B = I^7$ and

$$F(\alpha) = \sum_{x \in B} e(\alpha f(x)).$$

Then the number of representations of $N$ by the cubic form $f$ with $x_i \in I$ is

$$R(N) = R(N;I) = \int_0^1 F(\alpha) e(-N\alpha) \, d\alpha.$$  

Note that

$$F(\alpha) = (N_1 + F_1(\alpha))(N_2 + F_2(\alpha))F_3(\alpha)$$

$$= N_1N_2F_3(\alpha) + N_1F_2(\alpha)F_3(\alpha) + N_2F_1(\alpha)F_3(\alpha) + F_1(\alpha)F_2(\alpha)F_3(\alpha)$$

where for $i = 1,2$

$$F_i(\alpha) = \sum_{x,y,z \in I \atop L_i(x,y,z)Q_i(x,y,z) \neq 0} e(\alpha L_i(x,y,z)Q_i(x,y,z)) = \sum_{|n| \leq P^3} c_i(n) e(\alpha n)$$

with $c_i(0) = 0$ and

$$c_i(n) = \text{Card}\{(x,y,z) \in I^3 : L_i(x,y,z)Q_i(x,y,z) = n\} \text{ for } n \neq 0,$$

and

$$F_3(\alpha) = \sum_{x \in I} e(\alpha a_7x^3) = \sum_{n \in T} e(\alpha n).$$

We need to estimate the contribution of each term on the right in (2.11) to the integral in (2.10). We note here that

$$\int_0^1 N_1N_2F_3(\alpha) e(-N\alpha) \, d\alpha = N_1N_2\chi(N),$$

$$\int_0^1 N_1F_2(\alpha)F_3(\alpha) e(-N\alpha) \, d\alpha = N_1 \sum_{n \in T} c_2(N-n) = N_1 \sum_{x \in I} c_2(N - a_7x^3),$$

$$\int_0^1 N_2F_1(\alpha)F_3(\alpha) e(-N\alpha) \, d\alpha = N_2 \sum_{n \in T} c_1(N-n) = N_2 \sum_{x \in I} c_1(N - a_7x^3).$$
and, since $N_1, N_2 \ll P^2$, the trivial bounds on $F_1, F_2, F_3$ give

$$F(\alpha) - F_1(\alpha)F_2(\alpha)F_3(\alpha) \ll P^6. \quad (2.17)$$

Equation (2.14) shows that the term $N_1N_2\chi(N)$ comes from the minor arcs and corresponds to the solutions of $L_1Q_1 = L_2Q_2 = 0$. This conforms to the philosophy that the “degenerate” solutions come from the minor arcs while the “non-degenerate” solutions come from the major arcs.

### 2.3 Auxiliary transformations

At various steps in the application of the circle method, it will be useful to apply some linear transformation to the term $L_1Q_1$ or an equation of the form $L_1Q_1 = n$ while still maintaining the integrality of the coefficients (and do the same for $L_2Q_2$). We collect here the result of applying these transformations and of various cases that arise and will refer to them later.

Consider the equation $L_1Q_1 = n$. Substitute

$$x'_1 = L_1 = L_1(x_1, x_2, x_3) \quad (2.18)$$

and note that, by renaming the variables if necessary, we can assume that $a_1 \neq 0$. Then $x_1 = (x'_1 - a_2x_2 - a_3x_3)/a_1$ and we have

$$a_1^2n = a_1^2x'_1Q_1 = x'_1Q_1(a_1x_1, a_1x_2, a_1x_3) = x'_1Q_1(x'_1 - a_2x_2 - a_3x_3, a_1x_2, a_1x_3).$$

Thus

$$a_1^2n = a_1^2x'_1Q_1 = x'_1(A'x_2^2 + B'x_2x_3 + C'x_3^2 + G'x'_1x_2 + F'x'_1x_3 + A_1x_1^2) \quad (2.19)$$

where

$$A' = A_1a_1^2 + A_2a_1^2 - B_3a_1a_2, \quad B' = 2A_1a_2a_3 + B_1a_1^2 - B_2a_1a_2 - B_3a_1a_3,$$

$$C' = A_1a_3^2 + A_3a_1^2 - B_2a_1a_3, \quad F' = B_2a_1 - 2A_1a_3, \quad G' = B_3a_1 - 2A_1a_2. \quad (2.20)$$
By a tedious but straightforward calculation, \( B'^2 - 4A'C' = a_1^2 a_1 M_1 a_1^T = a_1^2 \Delta_1 \).

Since we are assuming that \( \Delta_1 \neq 0 \), we have \( B'^2 - 4A'C' \neq 0 \).

If \( A' \neq 0 \), (2.19) becomes

\[
x_1'(a_1^2 \Delta_1 x_2^2 - x_3^2) = 4A' a_1^4 \Delta_1 n - D' x_1^3 = 4A' a_1^4 \Delta_1 x_1' Q_1 - D' x_1^3 \quad (2.21)
\]

where

\[
x'_2 = 2A' x_2 + B' x_3 + G' x_1', \quad x'_3 = a_1^2 \Delta_1 x_3 + (B'G' - 2A'F') x_1',
\]

and

\[
D' = a_1^2 \Delta_1 (4A' A_1 - C'G') + (2A'F' - B'C')^2.
\]

If \( A' = 0 \) but \( C' \neq 0 \), we can again complete the square to get

\[
x_1'(a_1^2 \Delta_1 x_3^2 - x_2^2) = 4a_1^4 \Delta_1 C' n - D' x_1^3 = 4a_1^4 \Delta_1 C' x_1' Q_1 - D' x_1^3 \quad (2.22)
\]

where

\[
x'_2 = a_1^2 \Delta_1 x_2 + (B'F' - 2C'G') x_1', \quad x'_3 = 2C' x_3 + B' x_2 + F' x_1',
\]

and

\[
D' = a_1^2 \Delta_1 (4C' A_1 - F'^2) + (2C'G' - B'F')^2.
\]

If \( A' = C' = 0 \), \( B' \) must be non-zero. Multiplying (2.19) by \( B' \) and adding a suitable multiple of \( x_1^3 \) to both sides we get,

\[
x_1' x_2' x_3' = B' a_1^2 n - D' x_1^3 = B' a_1^2 x_1' Q_1 - D' x_1^3 \quad (2.23)
\]

where

\[
x'_2 = B' x_2 + F' x_1', \quad x'_3 = B' x_3 + G' x_1', \quad D' = B' A_1 - F' G'.
\]
2.4 The contribution from the minor arcs

Let \( \delta \) be a sufficiently small positive real number to be specified later. For \( 1 \leq q \leq P^{\delta} \), \( 1 \leq a \leq q \), \( (a, q) = 1 \), define the major arcs \( \mathcal{M}(q, a) \) by

\[
\mathcal{M}(q, a) = \left\{ \alpha : \left| \alpha - \frac{a}{q} \right| \leq P^{\delta - 3} \right\}
\]

(2.24)

and let \( \mathcal{M} \) be the union of the \( \mathcal{M}(q, a) \). The set \( m = (P^{\delta - 3}, 1 + P^{\delta - 3}) \backslash \mathcal{M} \) forms the minor arcs.

**Lemma 2.4.1.** For \( i = 1, 2 \), if \( \Delta_i \neq 0 \), then

\[
\int_{0}^{1} |F_i(\alpha)|^2 d\alpha \ll P^{3+\varepsilon}.
\]

(2.25)

**Proof.** We have

\[
\int_{0}^{1} |F_i(\alpha)|^2 d\alpha = \sum_{|n| \ll P^3} c_1(n)^2 = \sum_{|n| \ll P^3, n \neq 0} c_1(n)^2
\]

(2.26)

with \( c_1(n) \) as defined in (2.12), \( c_1(0) = 0 \). If \( L_1Q_1 = n \), we must have \( x'_1 = L_1 = l \) and \( Q_1 = n/l \) for some (positive or negative) divisor \( l \) of \( n \).

If \( A' \neq 0 \), dividing (2.21) by \( x'_1 = L_1 = l \) we get

\[
a^2_1 \Delta_1 x_2'^2 - x_3'^2 = 4A'a_1^4 \Delta_1 \frac{n}{l} - D'l^2.
\]

(2.27)

Note that as soon as \( x_2' \) and \( x_3' \) in (2.27) are fixed, so are \( x_2 \) and \( x_3 \) and then \( x_1 = (l - a_2x_2 - a_3x_3)/a_1 \). For any fixed positive integers \( a, b, r \) the number of solutions in non-negative integers of the equation \( as^2 + bt^2 = r \) is \( \leq 8d(r) \) and the number of solutions of the equation \( as^2 - bt^2 = r \) in integers \( s, t \) with \( 0 \leq s, t \leq P \) is \( \leq 8d(r) \log P \) where \( d(r) \) is the number of positive divisors of \( r \). (See the Appendix of Estermann [22] for a proof.) Hence, for an \( n \) for which the right-hand side of (2.27) never becomes zero, we have

\[
c_1(n) \ll \sum_{l|n} P^{3\varepsilon} = 16d(|n|)P^{3\varepsilon} \ll |n^\varepsilon P^{3\varepsilon} \ll P^{6\varepsilon}.
\]
The right-hand side in (2.27) is zero only if \( n = \frac{D'l^3}{4A'a_1^2\Delta_1} \). Such a case can arise only if \( n \) is a cube times the constant \( D'/4A'a_1^4\Delta_1 = \frac{D''}{E''} \), say (where the relatively prime integers \( D'' \), \( E'' \) depend on the coefficients of the form \( L_1Q_1 \) only), and can arise for at most one value of \( l \) for a given \( n \). For such \( n \) and \( l \), we have no solution in integers \( x_2', x_3' \) unless \( \Delta_1 \) is a square in which case we have \( O(P) \) solutions. There can be at most \( O(P) \) such \( n \ll P^3 \) and for such \( n \) we still have \( c_1(n) \ll P \). Hence,

\[
\int_0^1 |F_1(\alpha)|^2 d\alpha = \sum_{|n| \ll P^3} c_1(n)^2 = O(P^2P^2) + \sum_{|n| \ll P^3} O(P^{12\varepsilon}) \ll P^{3+12\varepsilon}.
\]

If \( A' = 0 \), \( C' \neq 0 \), a similar argument works. If \( A' = C' = 0 \), we have \( B' \neq 0 \) (as \( B'^2 - 4A'C' \neq 0 \)) and dividing (2.21) by \( x_1' = L_1 = l \) we get

\[
x_2'x_3' = (B'x_2 + F'l)(B'x_3 + G'l) = B'a_1^2n/l - D'l^2.
\]

If the right-hand side is not zero, the factors on left hand side have to be divisors of the right-hand side, giving \( O(P^\varepsilon) \) solutions. The right-hand side in the above equation is zero only if \( n = \frac{D'l^3}{B'a_1^2} \). Such a case can arise only if \( n \) is a cube times the constant \( D'/B'a_1^2 = \frac{D''}{E''} \), say (where the relatively prime integers \( D'' \), \( E'' \) depend on the coefficients of the form \( L_1Q_1 \) only), and can arise for at most one value of \( l \) for a given \( n \). For such \( n \) and \( l \), one of the factors on the left has to be zero while other can take any value \( \ll P \), giving \( O(P) \) solutions. There can be at most \( O(P) \) such \( n \ll P^3 \) and for such \( n \) we still have \( c_1(n) \ll P \). Hence, in this case also (2.25) holds.

From the proof of the lemma above we have

\[
\sum_{x \in I} c_2(N - a_7x^3) \ll PP^\varepsilon + P \cdot \text{Card}\{(x, y) : N - a_7x^3 = \frac{D''}{E''}y^3\}.
\]

By Corollary 1.5 of Bennett [4],

\[
\text{Card}\{(x, y) : N - a_7x^3 = \frac{D''}{E''}y^3\} \leq 10 \cdot 3^{6\varepsilon(E''N)} \ll N^\varepsilon \ll P^{3\varepsilon}.
\]
Hence, from (2.15), (2.8)

\[ \int_0^1 N_1 F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha \ll N_1 P^{1+3\varepsilon} \ll P^{3+3\varepsilon}. \]  \quad (2.28)

Similarly,

\[ \int_0^1 N_2 F_1(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha \ll N_2 P^{1+3\varepsilon} \ll P^{3+3\varepsilon}. \]  \quad (2.29)

**Lemma 2.4.2.** We have

\[ \int_m F_1(\alpha) F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha \ll P^{4+\varepsilon-(\delta/4)}. \]

**Proof.** For \( \alpha \in m \), by Dirichlet’s theorem on Diophantine approximation, there exist \( a, q \) with \( (a, q) = 1 \), \( q \leq P^{3-\delta} \) and \( \left| \alpha - \frac{a}{q} \right| \leq q^{-1} P^{3-3} \ll q^{-2} \). Since \( \alpha \in m \subseteq (P^{3-3}, 1 - P^{3-3}) \), we must have \( 1 \leq a < q \) and \( q > P^{3} \) (otherwise \( \alpha \) would be in \( \mathfrak{M}(q,a) \)). By Weyl’s inequality (See [16] or [44]),

\[ F_3(\alpha) \ll P^{1+\varepsilon-(\delta/4)}. \]

This, with lemma 2.4.1 and Cauchy’s inequality, gives

\[ \int_m F_1(\alpha) F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha \leq \left( \sup_{\alpha \in m} |F_3(\alpha)| \right) \left( \int_m |F_1(\alpha)||F_2(\alpha)| \, d\alpha \right) \]

\[ \leq \left( \sup_{\alpha \in m} |F_3(\alpha)| \right) \left( \int_0^1 |F_1(\alpha)|^2 \, d\alpha \right)^{\frac{1}{2}} \left( \int_0^1 |F_2(\alpha)|^2 \, d\alpha \right)^{\frac{1}{2}} \ll P^{4+\varepsilon-\frac{\delta}{4}}. \]

Since the total length of the major arcs is less that \( P^{3-3} \), from (2.17),

\[ \int_0^1 F_1(\alpha) F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha = \left( \int_m + \int_{\mathfrak{M}} \right) F_1(\alpha) F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha \]

\[ = \int_m F_1(\alpha) F_2(\alpha) F_3(\alpha) e(-N\alpha) \, d\alpha + \int_{\mathfrak{M}} F(\alpha) e(-N\alpha) \, d\alpha + O(P^{3+3\delta}). \]

Along with (2.11), (2.14), (2.28), (2.29) and lemma 2.4.2, this gives

\[ R(N) = N_1 N_2 \chi(N) + \int_{\mathfrak{M}} F(\alpha) e(-N\alpha) \, d\alpha + O(P^{3+\varepsilon} + P^{3+3\delta} + P^{4+\varepsilon-\frac{\delta}{4}}). \]  \quad (2.30)
Chapter 3

The major arcs

3.1 The generating function

The crucial step in dealing with the major arcs is to obtain an approximation to the generating function $F$, (2.9), in terms of the auxiliary functions

$$S(q, a) = \sum_{z \mod q} e\left( \frac{a}{q} f(z) \right)$$

and

$$I(\beta) = \int_{P^B} e(\beta f(\xi)) \, d\xi.$$ \hspace{1cm} (3.1)

Lemma 3.1.1. For $\alpha \in \mathcal{M}(q, a)$, writing $\alpha = (a/q) + \beta$, we have

$$F(\alpha) = q^{-7} S(q, a) I(\beta) + O(P^{6+2\delta}).$$ \hspace{1cm} (3.3)

Proof. We have

$$F\left( \frac{a}{q} + \beta \right) = \sum_{x \in B} e\left( \left( \frac{a}{q} + \beta \right) f(x) \right)$$

$$= \sum_{z \mod q} \sum_{y: qy + z \in B} e\left( \left( \frac{a}{q} + \beta \right) f(qy + z) \right)$$

$$= \sum_{z \mod q} \sum_{y: qy + z \in B} e\left( \frac{a}{q} f(qy + z) \right) e(\beta f(qy + z))$$
\[= \sum_{z \mod q} \sum_{y: qy + z \in B} e\left(\frac{q}{q} f(z)\right) e(\beta f(qy + z)) \]
\[= q^{-7} \sum_{z \mod q} e\left(\frac{a}{q} f(z)\right) \sum_{y: qy + z \in B} q^7 e(\beta f(qy + z)). \]

The inner sum is a Riemann sum of the function \(e(\beta f(\xi))\) over a 7-dimensional cuboid which depends on \(z\). We want to replace it by the integral over the 7-dimensional cube \(P \mathfrak{B}\) and estimate the error in doing so. Firstly, any first-order partial derivative of \(e(\beta f(\xi))\) is of the form \(2\pi i \beta Q(\xi) e(\beta f(\xi))\) where \(Q(\xi)\) is a quadratic form (in seven real variables) whose coefficients are bounded and which itself is, therefore, \(O(P^2)\) on the cube \(P \mathfrak{B}\). Therefore, \(e(\beta f(\xi))\) does not vary by more than \(O(|\beta| q P^2)\) on a cube of side \(q\). There are \(\ll (P/q)^7\) terms in the inner sum so the error in replacing the sum by the integral over the corresponding cuboid is \(O(|\beta| q P^2 q^7 (P/q)^7) = O(|\beta| q P^9)\). Secondly, each side of this cuboid depends on \(z\) but is within length \(q\) of the sides of \(P \mathfrak{B}\). Since the integrand is bounded by 1 in absolute value, the error in replacing the region of integration by \(P \mathfrak{B}\) is \(O(q P^6)\). Since we have \(q \leq P^\delta\) and \(|\beta| \leq P^\delta - 3\), the total error is \(O(P^{6+2\delta}) + O(P^{6+\delta}) = O(P^{6+2\delta})\). Hence,
\[F\left(\frac{a}{q} + \beta\right) = q^{-7} \sum_{z \mod q} e\left(\frac{a}{q} f(z)\right) (I(\beta) + O(P^{6+2\delta}))\]
which gives the lemma.

In lemmas 3.1.2 and 3.2.1 below we consider the case which \(N\) is a large positive integer; in case \(N = 0\), the factors \(e(-Na/q)\) in the singular series and \(e(-\gamma)\) in the singular integral disappear.

**Lemma 3.1.2.** We have
\[\int_{\mathbb{R}} F(\alpha) e(-N\alpha) \, d\alpha = P^4 \mathfrak{G}(N, P^\delta) J(P^\delta) + O(P^{3+5\delta})\]
where
\[\mathfrak{G}(N, Q) = \sum_{q \leq Q} \sum_{\substack{a=1 \\ (a,q)=1}} q^{-7} S(q,a) e(-aN/q) \quad (3.4)\]
and

\[ J(\mu) = \int_{|\gamma|<\mu} \left( \int_{\mathbb{R}} e(\gamma f(\xi)) d\xi \right) e(-\gamma) d\gamma. \] (3.5)

**Proof.** Note that \( \mathcal{M}(q,a) = [(a/q) - P^{\delta-3}, (a/q) + P^{\delta-3}] \) has length \( 2P^{\delta-3} \). The change of variable \( \alpha = (a/q) + \beta \) and lemma 3.1.1 give

\[
\int_{\mathcal{M}(q,a)} F(\alpha)e(-N\alpha) d\alpha = \int_{-P^{\delta-3}}^{P^{\delta-3}} q^{-7} S(q,a) I(\beta)e(-N((a/q) + \beta)) d\beta + O(P^{3+3\delta})
\]

\[
= q^{-7} S(q,a) e(-aN/q) \int_{-P^{\delta-3}}^{P^{\delta-3}} I(\beta)e(-N\beta) d\beta + O(P^{3+3\delta}).
\]

Since \( P = [N^{1/3}] \) (so that \( 0 \leq N - P^3 \leq 3P^2 + 3P \ll P^2 \)), we have

\[ |e(-N\beta) - e(-P^3\beta)| \ll |N - P^3||\beta| \ll P^2 P^{\delta-3} = P^{\delta-1}. \]

We have the bounds \( |I(\beta)| \leq P^7, |S(q,a)| \leq q^7 \) trivially, so the error in replacing \( e(-N\beta) \) by \( e(-P^3\beta) \) in the above integral is \( O(P^7 P^{\delta-3} P^{\delta-1}) = O(P^{3+3\delta}) \). Hence,

\[
\int_{\mathcal{M}(q,a)} F(\alpha)e(-N\alpha) d\alpha = q^{-7} S(q,a) e(-aN/q) \int_{-P^{\delta-3}}^{P^{\delta-3}} I(\beta)e(-P^3\beta) d\beta + O(P^{3+3\delta}).
\]

Summing over \( 1 \leq q \leq P^\delta, \ 1 \leq a \leq q, \ (a,q) = 1 \), we get

\[
\int_{\mathcal{M}} F(\alpha)e(-N\alpha) d\alpha = \mathcal{G}(N, P^\delta) \int_{-P^{\delta-3}}^{P^{\delta-3}} I(\beta)e(-P^3\beta) d\beta + O(P^{3+5\delta}).
\]

Applying the change of variable \( \gamma = P^3\beta \), the integral in the above equation becomes

\[
P^{-3} \int_{-P^\delta}^{P^\delta} I(P^{-3}\gamma)e(-\gamma) d\gamma.
\]

Noting that \( f \) is a homogeneous function of degree 3 and applying the change of variable \( \xi' = P^{-1}\xi \) we get

\[
I(P^{-3}\gamma) = \int_{\mathbb{R}} e(\gamma P^{-3}f(\xi)) d\xi = \int_{\mathbb{R}} e(\gamma f(P^{-1}\xi)) d\xi = P^7 \int_{\mathbb{R}} e(\gamma f(\xi')) d\xi',
\]

which completes the proof of the lemma. \( \square \)
3.2 The singular integral

Note that the inner integral appearing in the definition of $J(\mu)$, (3.5), is bounded trivially by 1. Applying the change of variable $\xi' = \gamma^{1/3}\xi$ we see that

$$
\int_{\mathcal{B}} e(\gamma f(\xi)) d\xi = \gamma^{-7/3} \int_{\gamma^{1/3}\mathcal{B}} e(f(\xi')) d\xi'.
$$

We think of the last integral as an iterated integral and apply Lemma 7.3 of Vaughan [44] to each iteration to get the bound

$$
\int_{\mathcal{B}} e(\gamma f(\xi)) d\xi \ll \min(1, \gamma^{-7/3}).
$$

This implies that $J(\mu)$ converges as $\mu \to \infty$. Furthermore, the convergence is fast enough to give us the following result.

**Lemma 3.2.1.** For $\mu \geq 1$,

$$
J(\mu) = J + O(\mu^{-4/3}) \tag{3.6}
$$

where

$$
J = \int_{-\infty}^{\infty} \left( \int_{\mathcal{B}} e(\gamma f(\xi)) d\xi \right) e(-\gamma) d\gamma. \tag{3.7}
$$

3.3 The singular series

Recall that

$$
\mathcal{S}(N, Q) = \sum_{q \leq Q} S(q; N) \tag{3.8}
$$

where, with $S(q, a)$ as in (3.1),

$$
S(q; N) = \sum_{\substack{a \equiv 1 \pmod{q} \\ (a, q) = 1}} q^{-7} S(q, a)e(-aN/q). \tag{3.9}
$$

We have the following factorization.

$$
S(q, a) = S_1(q, a)S_2(q, a)S_3(q, a) \tag{3.10}
$$
where
\[ S_i(q, a) = \sum_{x, y, z=1}^{q} e\left(\frac{a}{q} L_i(x, y, z) Q_i(x, y, z)\right) \]
for \( i = 1, 2 \) and
\[ S_3(q, a) = \sum_{x=1}^{q} e\left(\frac{aa_7}{q} x^3\right). \]

\( S(q; N) \) is a multiplicative function of \( q \). In fact, if \((q_1, q_2) = (a, q_1q_2) = 1\) and we choose \( a_1, a_2 \) so that \( a_2q_1 + a_1q_2 = 1 \) then for \( i = 1, 2, 3 \)
\[ S_i(q_1q_2, a) = S_i(q_1q_2, a_1q_2 + a_2q_1) = S_i(q_1, a_1) S_i(q_2, a_2). \] (3.11)

This follows from the fact that as \( r_1 \) and \( r_2 \) run through a complete (or reduced) set of residues modulo \( q_1 \) and \( q_2 \) respectively, \( r_2q_1 + r_1q_2 \) runs through a complete (or reduced) set of residues modulo \( q_1q_2 \). Thus it suffices to study \( S_i(q, a) \) when \( q \) is a prime power. We can also assume that \( L_1Q_1, L_2Q_2 \) have content 1. For, if \( g(x) \) is a polynomial in \( s \) variables with content \( c \), say \( g(x) = cg_1(x), (a, q) = 1, (c, q) = c_0 \) then \( c_0 \) is bounded in terms of \( g \) alone and writing \( c = c_0c' \) we have \((q/c_0, ac') = 1\) and
\[
\sum_{x \mod q} e\left(\frac{ag(x)}{q}\right) = \sum_{x \mod q} e\left(\frac{acg_1(x)}{q}\right) = \sum_{x \mod q} e\left(\frac{ac'g_1(x)}{q/c_0}\right) = c_0^s \sum_{x \mod (q/c_0)} e\left(\frac{ac'g_1(x)}{q/c_0}\right). 
\]

Thus a bound in content 1 case leads to a bound in the general case with a different implied constant which depends on the polynomial \( g \) alone. The bound
\[ |\sum_{x=1}^{q} e\left(\frac{ax^3}{q}\right)| \leq Cq^{2/3} \] for \((a, q) = 1\) (see [16] or [44]) gives
\[ |S_3(q, a)| \leq C(a_7, q)(q/(a_7, q))^{2/3} = C(a_7, q)^{1/3} q^{2/3} \leq Ca_7^{1/3} q^{2/3}. \] (3.12)
In the sum $S_1(p^k, a)$, by renaming the variables if needed, we can assume that $p \nmid a_1$. We have assumed $\Delta_1 \neq 0$, we let

$$\mathfrak{D}_1 = \begin{cases} 
2\Delta_1 A' & \text{if } A' \neq 0 \\
2\Delta_1 C' & \text{if } A' = 0 \text{ but } C' \neq 0 \\
B' & \text{if } A' = C' = 0 
\end{cases}$$

(3.13)

and consider first the primes $p$ not dividing $\mathfrak{D}_1$.

If $A' \neq 0$, we have, with $x'_1, x'_2, x'_3, D'$ as in (2.18), (2.21),

$$4a_1^4\Delta_1 A' L_1(x_1, x_2, x_3) Q_1(x_1, x_2, x_3) = x_1'(a_1^2\Delta_1 x_2'^2 - x_3'^2) + D'x_1'^3.$$ 

The determinant of the linear transformation $(x_1, x_2, x_3) \mapsto (x'_1, x'_2, x'_3)$ is $2a_1^2\Delta_1 A'$. Since $p \nmid \mathfrak{D}_1 = 2\Delta_1 A'$, as $(x_1, x_2, x_3)$ runs through a complete residue system modulo $p^k$ so does $(x'_1, x'_2, x'_3)$ and as $(u, v, w)$ runs through a complete residue system so does $(2a_1^2\Delta_1 A'u, 2v, 2a_1w)$. Hence,

$$S_1(p^k, a) = \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a}{p^k} L_1(x_1, x_2, x_3) Q_1(x_1, x_2, x_3) \right)$$

$$= \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a}{p^k} (a_1^2\Delta_1 x_2^2 - x_3^2) + D'x_1^3 \right)$$

$$= \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a}{p^k} (a_1^2\Delta_1 x_2^2 - x_3^2) + D'x_1^3 \right)$$

$$= \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a}{p^k} (a_1^2\Delta_1 x_2^2 - x_3^2) + D'x_1^3 \right)$$

$$= \sum_{u, v, w = 1}^{p^k} e \left( \frac{a}{p^k} (2a_1^2\Delta_1 A'u(a_1^2\Delta_1 (2v)^2 - (2a_1w)^2) + D'(2a_1^2\Delta_1 A'u)^3) \right)$$

$$= \sum_{u, v, w = 1}^{p^k} e \left( \frac{a}{p^k} \left( A''u^3 + B''uv^2 + C''uw^2 \right) \right)$$

$$= \sum_{u = 1}^{p^k} e \left( \frac{aA''u^3}{p^k} \right) \left\{ \sum_{v = 1}^{p^k} e \left( \frac{aB''uv^2}{p^k} \right) \sum_{w = 1}^{p^k} e \left( \frac{aC''uw^2}{p^k} \right) \right\}$$

where $A'' = 2a_1^2\Delta_1^2 A'^2 D'$, $B'' = 2\Delta_1$, $C'' = -2$ so that $p \nmid B''C''$.

For a fixed $u$ in the inner (double) sum with $p^i \parallel u$, we write $u = p^j u_1$ and
divide the sum over each of the indices \( v \) and \( w \) into \( p^j \) subsums by grouping \( p^{k-j} \) consecutive terms together. The sum over \( v \) becomes

\[
\sum_{v_1=1}^{p^j} \sum_{v_2=1}^{p^{k-j}} e \left( \frac{a B'' u_1 (p^{k-j} v_1 + v_2)^2}{p^{k-j}} \right) = p^j \sum_{v_2=1}^{p^{k-j}} e \left( \frac{a B'' u_1 v_2^2}{p^{k-j}} \right)
\]

and similarly the sum over \( w \) becomes

\[
\sum_{w_1=1}^{p^j} \sum_{w_2=1}^{p^{k-j}} e \left( \frac{a C'' u_1 (p^{k-j} w_1 + w_2)^2}{p^{k-j}} \right) = p^j \sum_{w_2=1}^{p^{k-j}} e \left( \frac{a C'' u_1 w_2^2}{p^{k-j}} \right).
\]

The sums over \( v_2, w_2 \) are Gauss sums modulo \( p^{k-j} \) and, since \( p \) is odd, have the absolute value \( p^{(k-j)/2} \). Then the sums over \( v \) and \( w \) have the absolute value \( p^{(k+j)/2} \).

For a fixed value of \( j \), there is only one value of \( u \) mod \( p^k \) if \( j = k \) while there are \( p^{k-j}(1-p^{-1}) \) values of \( u \) mod \( p^k \) if \( 0 \leq j \leq k - 1 \). Hence, if \( p^k = q \),

\[
|S_1(p^k, a)| \leq p^{2k} + \sum_{j=0}^{k-1} p^{k+j} p^{k-j}(1-p^{-1}) < (k+1)p^{2k} = q^2 d(q). \tag{3.14}
\]

In case \( A' = 0, C' \neq 0 \), a similar argument using (2.18), (2.22) applies. If \( A' = C' = 0 \) and \( B' \neq 0 \), with \( x_1', x_2', x_3', D' \) as in (2.18), (2.23), we have

\[
B' a_1^2 L_1(x_1, x_2, x_3) Q_1(x_1, x_2, x_3) = x_1' x_2' x_3' + D' x_3^3
\]

and the determinant of the linear transformation \((x_1, x_2, x_3) \mapsto (x_1', x_2', x_3')\) is \( B'^2 a_1 \). Since \( p \nmid \mathfrak{D}_1 = B' \), as \((x_1, x_2, x_3)\) runs through a complete residue system modulo \( p^k \) so does \((x_1', x_2', x_3')\) and as \((u, v, w)\) runs through a complete residue system so does \((B'a_1 u, v, w)\). Hence,

\[
S_1(p^k, a) = \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a}{p^k} L_1(x_1, x_2, x_3) Q_1(x_1, x_2, x_3) \right) = \sum_{x_1, x_2, x_3 = 1}^{p^k} e \left( \frac{a (x_1' x_2' x_3' + D' x_3^3)}{p^k B'a_1} \right) = \sum_{x_1', x_2', x_3' = 1}^{p^k} e \left( \frac{a (x_1' x_2' x_3' + D' x_3^3)}{p^k B'a_1} \right)
\]
\[
\sum_{u,v,w=1}^{p^k} e \left( \frac{a (B'a_1 u) v w + (B' a_1 u)^3}{p^k B'a_1} \right) = \sum_{u,v,w=1}^{p^k} e \left( \frac{a}{p^k} \left( A'' u^3 + u w v \right) \right)
\]
\[
= \sum_{u=1}^{p^k} e \left( \frac{a A'' u^3}{p^k} \right) \sum_{v=1}^{p^k} \sum_{w=1}^{p^k} e \left( \frac{a u v w}{p^k} \right) = \sum_{u=1}^{p^k} e \left( \frac{a A'' u^3}{p^k} \right) \sum_{v=1}^{p^k} p^k
\]

where \( A'' = B'^2 a_1^2 \). Since \( \sum_{u,v=1}^{p^k} 1 = p^k + k p^{k-1} (p - 1) < (k + 1) p^k \), (3.14) holds in this case as well.

Now we consider the (finitely many) primes dividing \( D_1 \). From (2.18), (2.19), noting that as \((x_1, x_2, x_3)\) runs through a complete residue system modulo \( p^k \) so does \((x'_1, x_2, x_3)\) and writing \( u \) in place of \( x'_1 \), \( S_1(p^k, a) \) is equal to

\[
\sum_{u,x_2,x_3=1}^{p^k} e \left( \frac{\bar{a}_1 a u}{p^k} \left( A' x_2^2 + B' x_2 x_3 + C' x_3^2 + G' u x_2 + F' u x_3 + A_1 u^2 \right) \right)
\]

where \( \bar{a}_1 \) denotes the inverse of \( a_1 \) mod \( p^k \). Dividing the sum over \( u \) according to the highest power of \( p \) dividing \( u \) and writing \( u = p^j u_1 \) where \( p^j \parallel u \),

\[
S_1(p^k, a) = \sum_{j=0}^{k} \sum_{u_1=1}^{p^{k-j}} \sum_{x_2,x_3=1}^{p^{k-j}} e \left( \frac{\bar{a}_1 a u}{p^{k-j}} Q'(x_2, x_3, p^j u_1) \right) \quad (3.15)
\]

where

\[
Q'(x_2, x_3, p^j u_1) = A' x_2^2 + B' x_2 x_3 + C' x_3^2 + G' p^j u_1 x_2 + F' p^j u_1 x_3 + A_1 (p^j u_1)^2.
\]

We think of \( Q' \) as a function of \( x_2, x_3 \) and \( p^j u_1 \) as a parameter. Then, by Theorem 4 of Loxton and Smith [36], the square of the absolute value of the innermost sum is bounded by \( p^{2(k-j)} \) times the number of solutions mod \( p^{k-j} \) of the simultaneous congruences

\[
\left[ \begin{array}{cc} 2A' & B' \\ B' & 2C' \end{array} \right] \left[ \begin{array}{c} y_1 \\ y_2 \end{array} \right] \equiv \left[ \begin{array}{c} 0 \\ 0 \end{array} \right] \pmod{p^{k-j}}. \quad (3.16)
\]
Suppose that $p^r \|(2A', B', 2C')$ and write $(2A', B', 2C') = p^r (A'', B'', C'')$. Then for $k - j > r$, (3.16) reduces to

$$
\begin{bmatrix}
A'' & B'' \\
B'' & C''
\end{bmatrix}
\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^{k-j-r}}.
$$

(3.17)

The $2 \times 2$ matrix in (3.17) has rank at least 1 mod $p$, hence (3.17) has at most $p^{k-j-r}$ solutions mod $p^{k-j-r}$ whence (3.16) has at most $p^{k-j+r}$ solutions mod $p^{k-j}$. Hence, the sum over $x_2, x_3$ for any fixed $u = p^ju_1$ is at most $p^{(3k-3j+r)/2}$ in absolute value for $j < k - r$. Using trivial bound for $j \geq k - r$, we see that for $p|D_1$

$$
|S_1(p^k, a)| \leq p^r p^{2k} + \sum_{j=0}^{k-r-1} p^{2j} p^{k-j}(1 - p^{-1})p^{\frac{3k-3j+r}{2}} < p^{2k+r} + (1 + p^{-1})^{5k+r/2}
$$

$$
< p^{2k}(p^k, D_1) + 2p^{2k}(p^k, D_1)^{1/2} \ll p^{5k/2}
$$

(3.18)

with the implicit constant depending on the coefficients of the cubic form only.

**Lemma 3.3.1.** The series

$$
\mathcal{S}(N) = \sum_{q=1}^{\infty} S(q; N)
$$

(3.19)

converges absolutely and uniformly in $N$ (so that $\mathcal{S}(N) \ll 1$) and for any $Q \geq 1$ we have

$$
\mathcal{S}(N) = \mathcal{S}(N, Q) + O(Q^{(-1/3)+\varepsilon}).
$$

(3.20)

**Proof.** Writing $q = q_1 q_2$ where

$$
q_1 = \prod_{p^k \mid q, p \nmid D_1 D_2} p^k, \quad q_2 = \prod_{p^k \mid q, p \mid D_1 D_2} p^k,
$$

from (3.10)-(3.12), (3.14), (3.18), we have

$$
S(q; N) \ll q_1^{-1/3} d(q_1)^2 q_2^{-1/3} \ll q_1^{(-4/3)+\varepsilon} q_2^{-1/3}.
$$
Hence
\[ \sum_{q > Q} |S(q; N)| = \sum_{q_2} q_2^{-1/3} \sum_{q_1 > Q/q_2} q_1^{(-4/3) + \varepsilon} \ll \sum_{q_2} q_2^{-1/3} \left( \frac{Q}{q_2} \right)^{(-1/3) + \varepsilon} \]
\[ = Q^{(-1/3) + \varepsilon} \sum_{q_2} q_2^{-\varepsilon} = Q^{(-1/3) + \varepsilon} \prod_{p | D_1 D_2} (1 - p^{-\varepsilon})^{-1} \ll Q^{(-1/3) + \varepsilon}. \]

3.4 The proofs of theorems 1 and 3

We shall prove theorem 2 and the statements regarding the singular series \( \mathcal{S}(N) \) in theorems 1 and 3 in the next chapter. We are ready to prove all the other statements in theorems 1 and 3.

From (2.30) and lemmas 3.1.2, 3.2.1, 3.3.1 we get
\[ R(N) = N_1 N_2 \chi(N) + P^4(\mathcal{S}(N) + O(P^{-\frac{2}{3} + \varepsilon}))(J + O(P^{-\frac{4\delta}{3}})) + O(P^{3+5\delta} + P^{4+\varepsilon - \frac{2}{5}}) \]
\[ = N_1 N_2 \chi(N) + P^4 \mathcal{S}(N) J + O(P^{3+5\delta} + P^{4+\varepsilon - \frac{2}{5}}). \]
The optimal choice for \( \delta \) here is 3/16. This completes the proof of Theorem 3.

The values taken by \( f(x_1, \ldots, x_7) \) with \(-M \leq x_i \leq M\) are \( \ll M^3 \) and in case \( x_i \) are allowed to take only positive (or non-negative) integral values we are assuming that a positive fraction of these values is positive. Thus
\[ \sum_{0 \leq N \ll M^3} R(N) \gg M^7 \]

This cannot be accounted for by the error term or by the term \( N_1 N_2 \chi(N) \) (as \( N_1 N_2 \ll M^4 \) when \( N \ll M^3 \), \( \chi(N) = 1 \) for \( O(M) \) values of \( N \ll M^3 \), and \( \chi(N) = 0 \) for the rest). Therefore, we must have \( J > 0 \). This completes the proof of Theorem 1.
Chapter 4

The $p$-adic problem

4.1 The congruence condition

The absolute convergence of the sum $\mathcal{G}(N) = \sum_{q=1}^{\infty} S(q; N)$ along with the multiplicativity of $S(q; N)$ implies that we also have the infinite product representation

$$\mathcal{G}(N) = \prod_{p \text{ prime}} T(p; N)$$

(4.1)

where

$$T(p; N) = 1 + \sum_{k=1}^{\infty} S(p^k; N).$$

(4.2)

For the main term in the asymptotic formula to be larger than the error term for an $N$ we need the singular series $\mathcal{G}(N)$ to be bounded away from zero. Since the bound (3.20) is independent of $N$, it follows that there is a constant $p_0 \geq 0$, depending on our cubic form but independent of $N$, such that

$$\frac{1}{2} < \prod_{p \text{ prime}, \ p \geq p_0} T(p; N) < \frac{3}{2}.$$ 

Hence, $\mathcal{G}(N)$ is non-zero if and only if $T(p; N)$ is non-zero for all primes $p$. $T(p; N)$ and $S(q; N)$ are related to the numbers $M(q; N)$ of solutions of the congruences

$$f(x) \equiv N \pmod{q}$$

(4.3)
as described by the following lemma (see [16] or [44] for a proof).

**Lemma 4.1.1.** For any natural number \( q \),

\[
\sum_{q_1 | q} S(q_1; N) = M(q; N)/q^6. \tag{4.4}
\]

Some conditions on the coefficient \( a_7 \) and on the coefficients of \( L_1, L_2, Q_1, Q_2 \) (or on \( N \)) are necessary for the existence of solutions of (4.3) for all \( q \) as can be seen by considering, for any prime \( p \), \( p \nmid a_7 \), the forms

\[
p^2L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) + p^2L_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) + a_7x_7^3
\]

which do not take any values exactly divisible by \( p \). For primes \( p \equiv 1 \pmod{3}, p \nmid a_7 \), the cubic forms

\[
pL_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) + pL_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) + a_7x_7^3
\]

cannot take any values prime to \( p \) whose cubic character mod \( p \) is different from that of \( a_7 \). The examples

\[
x_1(Ax_1^2 + pQ_1(x_1, x_2, x_3)) + pL_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) + a_7x_7^3
\]

and

\[
x_1(x_1^2 + 63Q_1(x_1, x_2, x_3)) + x_4(x_4^2 + 63Q_2(x_4, x_5, x_6)) + 28x_7^3
\]

show that requiring one (or both in case of \( p= 3, 7 \)) of \( L_1Q_1, L_2Q_2 \) to have content 1 is not enough to ensure the existence of solutions of (4.3) for all \( q \) and all \( N \).

Taking \( q = p^l \) in (4.4) we get

\[
\sum_{k=1}^{l} S(p^k; N) = M(p^l; N)/p^{6l}.
\]

Hence,

\[
T(p; N) = \lim_{l \to \infty} M(p^l; N)/p^{6l}, \tag{4.5}
\]

the limit on the right existing due to the absolute convergence of \( \sum_{q=1}^{\infty} S(q; N) \).
For a polynomial \( g \) in \( n \) variables and an integer \( \nu \geq 1 \), by a non-singular solution of \( g \equiv N \pmod{p^{2\nu-1}} \) we will mean an \( n \)-tuple \( y = (y_1, \ldots, y_n) \) such that \( g(y) \equiv N \pmod{p^{2\nu-1}} \) and \( p^\nu \nmid \frac{\partial g(y)}{\partial y_i} \) for some \( i \in \{1, \ldots, n\} \). Replacing \( C(x) \) by \( f(x) - N \) in Lemma 17.5 of Davenport [16] shows that if \( f(x) \equiv N \pmod{p^{2\nu-1}} \) has a non-singular solution then \( M(p^{l}; N) \geq p^{6(l-2\nu+1)} \) for \( l \geq 2\nu - 1 \) so that \( T(p; N) \geq p^{-6(2\nu-1)} \). Thus \( T(p; N) \gg p \) 1 if the congruence \( f(x) \equiv N \pmod{p^{2\nu-1}} \) has a non-singular solution for some \( \nu \ll_p 1 \). Since \( \sum_{i=1}^n y_i \frac{\partial g(y)}{\partial y_i} = 3g(y) \) for any homogeneous polynomial \( g \) of degree 3 in \( n \) variables, any solution of \( f(x) \equiv N \pmod{p} \) with \( p \nmid L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \) or \( p \nmid L_2(x_4, x_5, x_6)Q_2(x_4, x_5, x_6) \) or \( p \nmid a_7x_7 \) is a non-singular solution if \( p \neq 3 \). In particular, if \( p \neq 3 \) and \( p \nmid N \), then any solution of \( f(x) \equiv N \pmod{p} \) is a non-singular solution. If \( 3^k \nmid N \) then \( 3^{k+1} \nmid \nabla f(x) \) so existence of a solution of \( f(x) \equiv N \pmod{3^{2k+1}} \) would imply that \( T(3; N) \gg 1 \). Also, since \( \nabla(L_1Q_1) = (a_1, a_2, a_3)Q_1 + L_1(\nabla Q_1) \), for any prime \( p \) and any \( N \) divisible by \( p \), an \( x \) such that \( L_1(x_1, x_2, x_3) \equiv 0 \pmod{p} \), \( Q_2(x_4, x_5, x_6) \equiv 0 \pmod{p} \) gives a non-singular solution of \( f(x) \equiv 0 \pmod{p} \) (by choosing the rest of the variables as zero) unless \( p \) divides all the coefficients of \( L_1 \). Similarly, an \( x \) such that \( L_2(x_4, x_5, x_6) \equiv 0 \pmod{p} \), \( Q_2(x_4, x_5, x_6) \equiv 0 \pmod{p} \) gives a non-singular solution of \( f(x) \equiv 0 \pmod{p} \) unless \( p \) divides all the coefficients of \( L_2 \). We start by considering the congruence \( L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p} \).

### 4.2 The congruence \( L_1Q_1 \equiv N \pmod{p} \)

**Lemma 4.2.1.** Suppose that \( L_1Q_1 \) has content 1 and \( p \nmid a_1 \). Then the congruence

\[
L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p}
\]

has a non-singular solution except in the following cases:

1. \( a_1^2L_1Q_1 \equiv A_1L_1^3 \pmod{p} \), i.e., \( L_1^2|Q_1 \pmod{p} \), and one of the following holds:
   (a) \( p|N \) (Solutions mod \( p \) do exist in this case.)
   (b) \( p \nmid N \), \( p \equiv 1 \pmod{6} \) and \( a_1^2A_1^2N \) is a cubic non-residue mod \( p \). (In this case \( L_1Q_1 \equiv N \pmod{p} \) has no solution.)
   (c) \( p = 3, 3 \nmid N \) (Solutions mod 3 with 9 \nmid \nabla(L_1Q_1) exist in this case but they do not lift to all residue classes mod 9 hence mod \( 3^l \) for \( l \geq 2 \).)
(ii) $p = 2$, $2 \nmid N$ and $L_1Q_1$ is equivalent to one of the following three forms mod 2:

$$L_1x_2(L_1 + x_2), \; L_1x_3(L_1 + x_3) \; or \; L_1x_2(L_1 + x_2) + L_1x_3(L_1 + x_3). \tag{4.6}$$

(In these cases $L_1Q_1 \equiv 1 \pmod{2}$ has no solution.)

(iii) $p = 3$, $3 \nmid N$ and $L_1Q_1$ is equivalent mod 3 to

$$L_1(L_1^2 + 2x_2^2) \; or \; 2L_1(L_1^2 + 2x_2^2) \tag{4.7}$$

for some linear combination $x'_2$ of $x_1, x_2, x_3$. (Solutions mod 3 with $9 \nmid \nabla(L_1Q_1)$ exist in these cases but they do not lift to all residue classes mod 9 hence mod $3^l$ for $l \geq 2$.)

Proof. Making the invertible substitution $u = L_1(x_1, x_2, x_3) = a_1x_1 + a_2x_2 + a_3x_3,$

$$a_1^2Q_1(x_1, x_2, x_3) = A'x_2^2 + B'x_2x_3 + C'x_3^2 + G'x_2u + F'u_3u + A_1u^2 \tag{4.8}$$

where $A', B', C', F', G'$ are as in (2.20).

If $p \nmid A', \; p \nmid \Delta_1 = B'^2 - 4A'C'$ and $p \neq 2$, an invertible linear change of variables takes (4.8) into the form

$$4A'a_1^4\Delta_1Q_1(x_1, x_2, x_3) = a_1^2\Delta_1x_2^2 - x_3^2 + D'x_2u^2.$$ 

Also, in this case, a box argument shows that the quadratic form $a_1^2\Delta_1x^2 - y^2$ takes all the values mod $p$ as $x$ and $y$ take all values mod $p$. If $p|N$, we choose $u = L_1(x_1, x_2, x_3)$ to be zero mod $p$ and then choose any values for $x'_2, x'_3$ so that $Q_1(x_1, x_2, x_3)$ is non-zero mod $p$ (possible since $Q_1$ is not identically zero mod $p$) to get a non-singular solution of $L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p}$. If $p \nmid N$ we can choose any non-zero value mod $p$ for $u = L_1(x_1, x_2, x_3)$ and then choose $x'_2, x'_3$ so that $L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p}$ to get a solution which is non-singular except, perhaps, if $p = 3$ and $x'_2 \equiv x'_3 \equiv 0 \pmod{3}$. However, in the last case, by choosing a different value of $u$, we need to choose a different value of $a_1^2\Delta_1x_2^2 - x_3^2$ forcing $(x'_2, x'_3) \neq (0, 0) \pmod{3}$ and hence the solution to be
non-singular since, in this case,

\[ \frac{\partial(4a_1^4\Delta_1 A'L_1Q_1)}{\partial x_2'} = 2a_1^2\Delta_1 x_2'u, \quad \frac{\partial(4a_1^4\Delta_1 A'L_1Q_1)}{\partial x_3'} = 2a_1^2\Delta_1 x_3'u. \]

If \( p \nmid A' \), \( p|\Delta_1 = B'^2 - 4A'C' \) and \( p \neq 2 \), we have

\[ 4A'a_1^2Q_1(x_1, x_2, x_3) = x_2'^2 + (4A'F' - 2B'G')x_3'u + (4A'A_1 - G'^2)u^2 \pmod{p} \]

where

\[ x_2' = 2A'x_2 + B'x_3. \]

If \( 2A'F' - B'G' \neq 0 \pmod{p} \) then if \( p|N \) we choose \( u, x_3 \) to be zero mod \( p \) and \( x_2' \) to be any non-zero value mod \( p \) while if \( p \nmid N \) we can choose any non-zero values mod \( p \) for \( u \) and \( x_2' \) and then choose \( x_3 \) so that \( L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p} \) to get a non-singular solution. If \( 2A'F' - B'G' \equiv 0 \pmod{p} \) then if \( p|N \) we choose \( u \) to be zero mod \( p \) and choose \( x_2' \neq 0 \pmod{p} \) to get a non-singular solution. If \( p \nmid N \) first we choose any non-zero value mod \( p \) for \( u \) such that \( 4A'a_1^2N\overline{u} - (4A'A_1 - G'^2)u^2 = a\overline{u} - bu^2 \), say, is zero or a quadratic residue mod \( p \) (here \( \overline{u} \) denotes the inverse of \( u \) mod \( p \)) and then choose \( x_2' \) to be a square root mod \( p \) of \( a\overline{u} - bu^2 \). (That it is possible to choose such a \( u \) can be seen by applying the Weil bound to the character sum \( \sum_{0 \leq u \leq p-1} \left( \frac{au-bu^2}{p} \right) \) which is the Legendre symbol mod \( p \), for \( p > 7 \) and checking all the cases for smaller values of \( p \) directly.) This solution is non-singular except, perhaps, if \( p = 3 \) and \( x_2' \equiv 0 \pmod{3} \). Checking all possible values of \( 4A'A_1 - G'^2 \pmod{3} \) we find that non-singular solutions exist except in case \( 4A'A_1 - G'^2 \equiv 2 \pmod{3} \), i.e., when \( L_1Q_1 \) is of the form \( bL_1(x_2'^2 + 2L_1^2) \), \( b = 1 \) or \( 2 \), when reduced mod \( 3 \). Note that \( L_1(x_2'^2 + 2L_1^2) \equiv 2L_1(L_1^2 + 2x_2'^2) \pmod{3} \) and \( 2L_1(x_2'^2 + 2L_1^2) \equiv L_1(2x_2'^2 + L_1^2) \pmod{3} \).

A similar argument holds in the case \( p|A', p \nmid C', p \neq 2 \).

If \( p = 2 \), not both \( A', C' \) are even and \( 2|N \), we can choose \( u \) to be even and choose \( x_2, x_3 \) so that \( A'x_2'^2 + B'x_2x_3 + C'x_3^2 \) is odd to get a non-singular solution of \( L_1Q_1 \equiv 0 \pmod{2} \). A solution of \( L_1Q_1 \equiv 1 \pmod{2} \), if it exists, would be non-singular. However, any solution of \( L_1Q_1 \equiv 1 \pmod{2} \) must have \( u \equiv 1 \pmod{2} \) and \( Q_1(x_1, x_2, x_3) \equiv 1 \pmod{2} \). But when \( u \equiv 1 \pmod{2} \), \( Q_1(x_1, x_2, x_3) \equiv A'x_2 + B'x_2x_3 + C'x_3 + G'x_2 + F'x_3 + A_1 \pmod{2} \) so we can choose \( x_2, x_3 \) so that it takes
value 1 (mod 2) if and only if not all of $A' + G', B', C' + F', A_1$ are even. Since $L_1Q_1$ has content 1, not all of $A', B', C', F', G', A_1$ are even. Thus, when not all of $A', B', C'$ are even, $L_1Q_1 \equiv 1$ (mod 2) has no solutions precisely when $L_1Q_1$ is one of the following when reduced mod 2:

$$L_1x_2(L_1 + x_2), \ L_1x_3(L_1 + x_3), \ L_1x_2(L_1 + x_2) + L_1x_3(L_1 + x_3).$$

If $p|A', C'$ but $p \nmid B'$ we have

$$B'a_1^2Q_1 = B'^2x_2x_3 + B'G'x_2u + B'F'x_3u + B'A_1u^2 = x'_2x'_3 + D''u^2 \pmod p$$

where

$$x'_2 = B'x_2 + F'u, \ x'_3 = B'x_3 + G'u, \ D'' = B'A_1 - F'G'.$$

If $p|N$ we choose $u$ to be zero and $x_2, x_3$ to be any non-zero values mod $p$ while if $p \nmid N$ we choose any non-zero value mod $p$ for $u$ and then choose $x_2, x_3$ so that $L_1Q_1 \equiv N \pmod p$.

If $A' \equiv B' \equiv C' \equiv 0 \pmod p$, (4.8) reduces to

$$a_1^2Q_1(x_1, x_2, x_3) = G'x_2u + F'x_3u + A_1u^2 = u(G'x_2 + F'x_3 + A_1u) \pmod p.$$  

Hence, in this case,

$$a_1^2L_1Q_1 = u^2(G'x_2 + F'x_3 + A_1u) \pmod p,$$

$$\frac{\partial(a_1^2L_1Q_1)}{\partial u} = 2u(G'x_2 + F'x_3) + 3A_1u^2 \pmod p, \ \frac{\partial(a_1^2L_1Q_1)}{\partial x_2} = G'u^2 \pmod p,$$

and

$$\frac{\partial(a_1^2L_1Q_1)}{\partial x_3} = F'u^2 \pmod p.$$  

Unless $F' \equiv G' \equiv 0 \pmod p$ as well, we can choose any non-zero value mod $p$ for $u$ and then choose $x_2, x_3$ so that $u^2(G'x_2 + F'x_3 + A_1u) \equiv a_1^2N \pmod p$ to get a non-singular solution.

If $A' \equiv B' \equiv C' \equiv F' \equiv G' \equiv 0 \pmod p$ (so we must have $A_1 \not\equiv 0 \pmod p$ as
Let $L_1Q_1$ has content $1$, $a_1^2Q_1(x_1, x_2, x_3) \equiv A_1 u^2 \pmod{p}$ so that

$$a_1^2L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv A_1 u^3 = A_1 L_1^3 \pmod{p}.$$ 

If $p \equiv 2 \pmod{3}$, as $u$ takes all the non-zero values mod $p$ so does $A_1 u^3$, hence the conclusion of the lemma in this case follows.

\[\square\]

### 4.3 The congruence $L_1Q_1 \equiv N \pmod{p^\nu}$

**Lemma 4.3.1.** Suppose that $L_1Q_1$ has content $1$ and $p \nmid a_1$. Let $A', B', C', F', G'$ be as in (2.20). Define $\gamma_1 = \gamma_1(p, L_1Q_1)$ and $\gamma'_1 = \gamma'_1(p, L_1Q_1)$ as follows.

(i) If $L_1^2 | Q_1 \pmod{p}$, choose $\alpha_1, \beta_1$ so that $p^{\alpha_1} || (A', B', C')$, $\beta_1 = 0$ if $(F', G') = (0, 0)$, $p^{\beta_1} || (F', G')$ if $(F', G') \neq (0, 0)$, and let

$$\gamma_1 = \begin{cases} \frac{\lfloor \frac{5\alpha_1+1}{3} \rfloor}{\max\{\lfloor \frac{5\alpha_1+1}{3} \rfloor, \lfloor \frac{4\alpha_1+1-\beta_1}{2} \rfloor \}} & \text{if } \beta_1 = 0, \\ \frac{2\gamma_1+1}{2} & \text{if } \beta_1 \geq 1, \\ 2\gamma_1 - 1 & \text{if } p \neq 3. \end{cases}$$

(ii) If $p = 2$ and $L_1Q_1$ is one of the forms in (4.6) mod $2$, define $\gamma_1 = \gamma'_1 = 1$.

(iii) If $p = 3$ and $L_1Q_1$ is one of the forms in (4.7) mod $3$, define $\gamma_1 = 3, \gamma'_1 = 1$.

(iv) In other cases, let $\gamma_1 = \gamma'_1 = 0$.

If the congruence

$$L_1(x_1, x_2, x_3)Q_1(x_1, x_2, x_3) \equiv N \pmod{p^{\max\{1, \gamma_1\}}}$$

has a solution, it has a non-singular solution. Such a solution does exist if $p^{\gamma_1} | N$. In particular, $L_1Q_1 \equiv 0 \pmod{p^{\max\{1, \gamma_1\}}}$ has a non-singular solution.

**Proof.** For $a = 2, 3$ define $\delta_a = \delta_a(p)$ to be $1$ if $p = a$ and $0$ otherwise. If $p^{t} || N$ and $x_1$ is a solution of the congruence (4.10) then $p^{t + \delta_3 + 1} || (\nabla(L_1Q_1))(x_1)$ so the solution is non-singular if $2t + 2\delta_3 + 1 \leq \gamma_1$, i.e., $t \leq \gamma'_1 - 1$. Now we show that a non-singular solution of $L_1Q_1 \equiv N \pmod{p^{\gamma_1+1}}$ exists in case $t \geq \gamma'_1$. In cases (ii), (iii) and (iv) it follows from lemma 4.2.1. In case (i), write $u = L_1 = L_1(x_1, x_2, x_3)$ and

$$a_1^2Q_1(x_1, x_2, x_3) = p^{\alpha_1}(A''x_2^2 + B''x_2x_3 + C''x_3^2) + p^{\beta_1}(G''x_2 + F''x_3)u + A_1 u^2.$$
Then $\alpha_1 \geq 1$, $\beta_1 \geq 0$, $p \nmid (A'', B'', C'')$, $p \nmid A_1$. Note that we cannot have $A'' = B'' = C'' = 0$ as that would make $L_1 Q_1$ degenerate. We have

$$a_1^2 L_1 Q_1 = p^{\alpha_1}(A''x_2^2 + B''x_2x_3 + C''x_3^2)u + p^{\beta_1}(G''x_2 + F''x_3)u^2 + A_1u^3,$$

$$\frac{\partial(a_1^2 L_1 Q_1)}{\partial u} = p^{\alpha_1}(A''x_2^2 + B''x_2x_3 + C''x_3^2) + 2p^{\beta_1}(G''x_2 + F''x_3)u + 3A_1u^2,$$

$$\frac{\partial(a_1^2 L_1 Q_1)}{\partial x_2} = p^{\alpha_1}(2A''x_2 + B''x_3)u + p^{\beta_1}G''u^2$$

and

$$\frac{\partial(a_1^2 L_1 Q_1)}{\partial x_3} = p^{\alpha_1}(B''x_2 + 2C''x_3)u + p^{\beta_1}F''u^2.$$

Choose

$$(x_2, x_3) = \begin{cases} (1, 0) & \text{if } p \nmid A'' \\ (0, 1) & \text{if } p|A'' \text{ but } p \nmid C'' \\ (1, 1) & \text{if } p|A'', C'' \text{ but } p \nmid B'' \end{cases}$$

so that $p \nmid A''x_2^2 + B''x_2x_3 + C''x_3^2$ and let $u = p^\lambda u_0$ with $p \nmid u_0$.

In case $\beta_1 = 0$ we have $p^{\alpha_1}\|\frac{\partial(a_1^2 L_1 Q_1)}{\partial u}\|$ if $\lambda > \frac{\alpha_1 - \delta_1}{2}$ and $L_1 Q_1 \equiv \overline{a}_1^2 p^{\alpha_1 + \lambda}(A''x_2^2 + B''x_2x_3 + C''x_3^2)u_0 \pmod{p^{2\alpha_1 + 1}}$ (where $\overline{a}_1^2$ denotes the inverse of $a_1^2 \pmod{p^{2\alpha_1 + 1}}$) provided $\lambda \geq \frac{2\alpha_1 + 1}{3}$. Choosing $\lambda = t - \alpha_1$ and a suitable $u_0$ we get a non-singular solution of $L_1 Q_1 \equiv N \pmod{p^{2\alpha_1 + 1}}$ provided $t \geq \frac{5\alpha_1 + 1}{3}$.

If $\beta_1 \geq 1$ then $p^{\alpha_1}\|\frac{\partial(a_1^2 L_1 Q_1)}{\partial u}\|$ provided $\lambda > \max\{\alpha_1 - \beta_1 - \delta_2, \frac{\alpha_1 - \delta_1}{2}\}$ and $L_1 Q_1 \equiv \overline{a}_1^2 p^{\alpha_1 + \lambda}(A''x_2^2 + B''x_2x_3 + C''x_3^2)u_0 \pmod{p^{2\alpha_1 + 1}}$ (where $\overline{a}_1^2$ denotes the inverse of $a_1^2 \pmod{p^{2\alpha_1 + 1}}$) provided $\lambda \geq \max\{\frac{2\alpha_1 + 1 - \beta_1}{3}, \frac{2\alpha_1 + 1 - \delta_1}{2}\}$. Both the inequalities on $\lambda$ are satisfied if $\lambda \geq \max\{\frac{\alpha_1 - \delta_1 + 1}{2}, \frac{2\alpha_1 + 1}{3}, \frac{2\alpha_1 + 1 - \delta_1}{2}\}$. Choosing $\lambda = t - \alpha_1$ and a suitable $u_0$ we get a non-singular solution of $L_1 Q_1 \equiv N \pmod{p^{2\alpha_1 + 1}}$ provided $t \geq \max\{\frac{5\alpha_1 + 1}{3}, \frac{4\alpha_1 + 1 - \delta_1}{2}\}$. \hfill \Box

### 4.4 Completion of the proof of theorem 2

Let $c$ be the content of $f$ and choose $c_i$, $i = 1, 2, 3$ so that $cc_i$ is the content of $L_i Q_i$ for $i = 1, 2$ and $cc_3 = a_7$. Then $(c_1, c_2, c_3) = 1$ and

$$f(x) = c(c_1 L_1 Q_1' + c_2 L_2 Q_2' + c_3 x_7^3) = c(c_1 L_1 Q_1' + c_2 L_2 Q_2' + c_3 L_3 Q_3')$$
with $L_1'Q_1'$ and $L_2'Q_2'$ having content 1; here we have written $L_i'$ for $x_7$ and $Q_i'$ for $x_7^2$ in the last expression. If $c > 1$, $c \nmid N$ then $T(p; N) = 0$ for all $p | c$, $\mathcal{G}(N) = 0$ and $f(x) = N$ has no solutions. So we assume that $c | N$ in the remainder of this section and write $N = cN'$ for any prime $p > 2$ and $i = 1, 2, 3$, $L_i'Q_i'$ takes a value relatively prime to $p$; (this is not true for $p = 2$ as can be seen by the forms in $(4.6)$; if $L_i'Q_i'$ takes a value $b_i$ then it takes all the values $b_iy_i^3$ for $p \neq 3$ the congruence $b_1y_1^3 + b_2y_2^3 + b_3y_3^3 \equiv N' \pmod{p}$ has non-singular solutions for all $N'$ if $p \nmid b_1b_2b_3$ (see [5] for a proof). In fact, for $p \equiv 2 \pmod{3}$, the congruence $b_1y_1^3 + b_2y_2^3 \equiv N' \pmod{p}$ has non-singular solutions for all $N'$ if $p \nmid b_1b_2$. Also, if $f_1$ is one of the forms in $(4.6)$ and $2 \nmid b_1b_2$, the congruence $b_1f_1(y_1, y_2, y_3) + b_2y_2^3 \equiv N' \pmod{2}$ has non-singular solutions for all $N'$. Hence it follows that if $p \equiv 1 \pmod{6}$, $p \nmid c_1c_2c_3$ or if $p \equiv 5 \pmod{6}$, $p \nmid (c_1c_2c_3c_2c_3)$ or if $p = 2$, $p \nmid (c_1c_3, c_2c_3)$, then congruence

$$f(x)/c = c_1L_1'Q_1' + c_2L_2'Q_2' + c_3x_7^3 \equiv N' \pmod{p}$$

has a non-singular solution for all $N'$ so that $T(p; N) \gg_p 1$ for all $N = cN'$. Now consider a prime $p$ dividing $3c_1c_2c_3$ and let $j_1, j_2, j_3 \geq 0$ be integers such that $p^{3j_i} || c_i$ for $i = 1, 2, 3$ and let $\nu_0 = \max\{j_1, j_2, j_3\}$.

**Lemma 4.4.1.** Suppose that $N' = c_1N_1 + c_2N_2 + c_3N_3$ and that for some $\nu \ll_p 1$ the congruences $L_i'Q_j' \equiv N_j \pmod{p^{\alpha + 2\nu - 1}}$ have solutions for $j = 1, 2, 3$ and one of the congruences $L_i'Q_j' \equiv N_j \pmod{p^{2\nu - 1}}$ has a non-singular solution. Then $T(p; N) \gg_p 1$.

**Proof.** Write $x = (x_1, \ldots, x_7), x_1 = (x_1, x_2, x_3), x_2 = (x_4, x_5, x_6), x_3 = x_7,

L_1'(x) = L_1'(x_1) = L_1, L_2'(x) = L_2'(x_2) = L_2, L_3'(x) = L_3'(x_3) = x_7,

Q_1'(x) = Q_1'(x_1) = Q_1, Q_2'(x) = Q_2'(x_2) = Q_2, Q_3'(x) = Q_3'(x_3) = x_7^3,

h_1 = h_2 = 3, h_3 = 1$. For $l \geq \nu_0 + 2\nu - 1$, given any simultaneous solution $x = (x_1, x_2, x_3)$ of $L_i'(x)Q_j'(x) \equiv N_j \pmod{p^{\alpha + 2\nu - 1}}, j = 1, 2, 3$ with $x_i$ a non-singular solution of $L_i'(x)Q_j'(x) \equiv N_i \pmod{p^{2\nu - 1}}$, we choose solutions $x'$ of $f(x') \equiv N \pmod{p^l}$ as follows. For $m$ such that the variable $x_m$ does not appear in $L_i'Q_j'$, assign any values to $x'_m$ congruent to $x_m \pmod{p^{\alpha + 2\nu - 1}}$; this can be done in $p^{(7-h_i)(\nu_0 + 2\nu - 1)}$ ways. Then for $j \neq i$, $L_j'(x'_j)Q_j'(x'_j) \equiv N_j \pmod{p^{\alpha + 2\nu - 1}}$ so that $N' - \sum_{j \neq i} L_j'(x'_j)Q_j'(x'_j) \equiv c_iN_i \pmod{p^{\alpha + 2\nu - 1}}$. Then the congruence $c_iL_i'(x'_i)Q_i'(x'_i) \equiv N' - \sum_{j \neq i} L_j'(x'_j)Q_j'(x'_j) \pmod{p^l}$ is equivalent to the congru-
ence $L'_i(x'_i)Q'_i(x'_i) \equiv c_i^{-1}(N' - \sum_{j \neq i} L'_j(x')Q'_j(x')) \pmod{p^{l-i}}$ and hence has at least $p^{(h_i-1)(l-j_i-2\nu+1)}$ solutions mod $p^{l-i}$ and hence at least $p^{(h_i-1)(l-j_i-2\nu+1)+h_ij_i}$ solutions mod $p^l$. Hence, $M(p^l; N) \geq C_pp^{6d}$ with $C_p = C_{p,f} = p^{-6(2\nu-1)-(7-h_i)\nu_0+j_i}$ implying that $T(p; N) \geq C_p \gg_p 1$ with the lower bound depending only on the coefficients of the cubic form $f$ and the prime $p$. \hfill \square

Let $\gamma_1 = \gamma_1(p, L'_1Q'_1)$, $\gamma'_1 = \gamma'_1(p, L'_1Q'_1)$ be defined as in lemma 4.3.1 (with $L_1Q_1$ replaced by $L'_1Q'_1$) and let $\gamma_2 = \gamma_2(p, L'_2Q'_2)$, $\gamma'_2 = \gamma'_2(p, L'_2Q'_2)$ be defined similarly. If $p^{\gamma'_1+j_1}|N'$, applying lemma 4.3.1 to $N_1 = d_1N'/p^{j_1}$ where $d_1$ is the inverse of $c_1/p^{j_1}$ mod $p^{\nu_0+\gamma_1}$ and choosing $N_2 = N_3 = 0$ in lemma 4.4.1, we see that $T(p; N) \gg_p 1$. A similar argument holds if $p^{\gamma'_2+j_2}|N'$. Let

$$\gamma' = \gamma'(p, f) = \min\{\gamma'_1 + j_1, \gamma'_2 + j_2\}. \quad (4.11)$$

Then, if $p^{\gamma'}|N'$, $T(p; N) \gg_p 1$. Let

$$\gamma = \gamma(p, f) = \min\{\gamma_1 + \nu_0, \gamma_2 + \nu_0, 2\gamma' + 2\delta_3 - 1\}. \quad (4.12)$$

If $p^{\gamma'} \nmid N'$ and $\mathbf{x} = (x_1, \ldots, x_7)$ is a solution of the congruence $f(\mathbf{x})/c = c_1L'_1Q'_1 + c_2L'_2Q'_2 + c_3x_3^2 \equiv N' \pmod{p^\gamma}$, let $N_1 = L'_1Q'_1(x_1, x_2, x_3)$, $N_2 = L'_2Q'_2(x_4, x_5, x_6)$ and $N_3 = c_3x_3^2$. Then $p^{\gamma'_1+j_1+\delta_3} \nmid (\nabla(f(\mathbf{x}))/c)$ hence the solution is non-singular (and thus $T(p; N) \gg_p 1$) if $\gamma = 2\gamma' + 2\delta_3 - 1$. By lemma 4.3.1, $L'_1Q'_1 \equiv N_1 \pmod{p^{\nu_0}}$ has a non-singular solution if $\gamma = \gamma_1 + \nu_0$, $L'_2Q'_2 \equiv N_2 \pmod{p^{\nu_2}}$ has a non-singular solution if $\gamma = \gamma_2 + \nu_0$. In the last two cases, $T(p; N) \gg_p 1$ by lemma 4.4.1. Thus $\mathcal{S}(N) \gg 1$ or $\mathcal{S}(N) = 0$ according as

$$f(\mathbf{x}) \equiv N \pmod{c \prod_{p|3c_1c_2c_3} p^{\gamma(p)}}$$

has a solution or not. This completes the proof of theorem 2.
Bibliography


[5] B. J. Birch, Homogeneous forms of odd degree in a large number of variables, Mathematika 4, 102-105 (1957)


[34] D. J. Lewis, Cubic forms over algebraic number fields, Mathematika, 4, 97-101 (1957)

[35] Yu. V. Linnik, On the representations of large numbers as sums of seven cubes, Mat. Sbornik 12, 218-224 (1943)


[38] E. Selmer, The diophantine equation $ax^3 + by^3 + cz^3 = 0$, Acta Math. 85, 203-362 (1951)


Manoj Verma was born in Barabanki district of Uttar Pradesh, India in 1978. He attended six different schools in small towns in the first twelve years of his education and then, at the time unaware of the possibilities he found out about only later, went to IITK (Indian Institute of Technology, Kanpur) for a Bachelor’s in Electrical Engineering. Then he worked for a software company for a short period of time before deciding to go back to IITK for a Master’s in Mathematics. During that time he found out about a fascinating but hopelessly difficult problem called Waring’s problem; the most important work on this problem in past three decades or so has been done by Vaughan and Wooley. He was at IIT Bombay when some of his teachers there helped him get a chance to become a student of Vaughan. His dream, his lifetime goal, is to make some progress on Waring’s problem someday. He is not “gifted” and has to work hard for long to have any chance at realizing his dream. While striving for this, he wants to contribute to teaching Mathematics to some young people in India where few are fortunate to have good, inspiring teachers.