ON THE SQUAREFREE VALUES OF POLYNOMIALS

A Dissertation in
Mathematics
by
James M. Kowalski

© 2020 James M. Kowalski

Submitted in Partial Fulfillment
of the Requirements
for the Degree of

Doctor of Philosophy

May 2020
The dissertation of James M. Kowalski was reviewed and approved by the following:

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

Mihran Papikian  
Associate Professor of Mathematics

Yuriy Zarkhin  
Professor of Mathematics

Sean Hallgren  
Professor of Computer Science and Engineering

Alexei Novikov  
Professor of Mathematics  
Co-Chair of Graduate Program
Abstract

When considering the density of squarefree numbers among the values of a polynomial, one would expect a “local-to-global” type result to hold, involving the proportion of values not divisible by $p^2$ for each prime $p$. Such a result has been established in many cases in the existing literature, and in this dissertation we add several classes of degree three, multivariable polynomials.
# Table of Contents

List of Symbols vi  
Acknowledgments vii  

Chapter 1  
Introduction 1  
1.1 The Expected Result 1  
1.2 Previous Research 2  
1.3 Main Results 5  

Chapter 2  
Preliminary Results 6  
2.1 The Möbius Function 6  
2.2 Hua’s Lemma 7  
2.3 Other Necessary Results 10  

Chapter 3  
The General Procedure 11  
3.1 The Sum $S(1, D)$ 12  
3.2 The Sum $S(D, B^{3/2})$ 13  

Chapter 4  
Sums of Cubic Polynomials 15  
4.1 Required Estimates 16  
4.2 Proof of the Theorem 19  
4.3 Proofs of the Corollaries 21  

Chapter 5  
Sums of Two Cubes 23  
5.1 Proof of the Theorem 24  

Chapter 6  
A Special Case for Cubic Forms 26
### Chapter 6

6.1 Estimating $\rho(d^2)$ .................................................. 26
6.2 A Bound on the Number of Solutions to $F(x) = F(y)$ .......... 29
6.3 Estimating $\sum R(n)^2$ ................................................. 42
6.4 Proof of the Theorem ..................................................... 44

### Chapter 7

**General Cubic Forms** 46

7.1 Estimating $\rho(d^2)$ .................................................. 47
7.2 Estimating $\sum R(n)^2$ ................................................. 48
7.3 Proof of the Theorem ..................................................... 50

### Chapter 8

**Further Research** 52

**Bibliography** 53
List of Symbols

\( a \mid b \)  \( a \) divides \( b \); \( b = ma \) for some integer \( m \)

\( \mathbf{x}, \mathbf{y} \) \( \mathbf{x} = (x_1, x_2, \ldots, x_s) \) and \( \mathbf{y} = (y_1, y_2, \ldots, y_s) \)

\( e(x) \) \( e(x) = \exp(2\pi ix) = \sum_{n=0}^{\infty} \frac{(2\pi ix)^n}{n!} \)

\( \varepsilon \) a small positive real number which may be different each appearance

\( f(x) = O(g(x)) \) there are real numbers \( A > 0 \) and \( x_0 > 0 \) where \( |f(x)| \leq Ag(x) \) for all \( x > x_0 \)

\( f(x) \ll g(x) \) equivalent to \( f(x) = O(g(x)) \)

\( \#A \) the cardinality of the set \( A \)

\( \mathfrak{B} \) the box \( [a_1, b_1] \times \cdots \times [a_s, b_s] \) in \( \mathbb{Z}^s \)

\( \text{Vol}(\mathfrak{B}) \) \( \prod_{i=1}^{s}(b_i - a_i) \)

\( B\mathfrak{B} \) the box \( [Ba_1, Bb_1] \times \cdots \times [Ba_s, Bb_s] \) in \( \mathbb{Z}^s \), \( \mathfrak{B} \) scaled by \( B \)

\( N_g(B) \) the number of squarefree \( g(\mathbf{x}) \) where \( \mathbf{x} \in B\mathfrak{B} \)

\( \rho(d) \) the number of \( \mathbf{x} \in [1, d]^s \) with \( g(\mathbf{x}) \equiv 0 \pmod{d} \)

\( R(n) \) the number of \( \mathbf{x} \in B\mathfrak{B} \) with \( g(\mathbf{x}) = n \)
Acknowledgments

First, I’d like to thank my advisor, Professor Robert C. Vaughan, for his guidance and support throughout writing this dissertation. This dissertation would not have been possible without his expertise and assistance. I’d like to also thank the members of my committee for their feedback in reviewing this dissertation.

I’d like to thank Sid Graham for encouraging me to pursue higher mathematics. I’d like to thank the math faculty at Central Michigan University for preparing me for my studies.

I’d like to thank my parents for encouraging me to keep learning. I’d like to thank my wife, Theresa, for tolerating the many years being the spouse of a grad student. Finally, I’d like to thank my friends for providing some much-needed distractions.
Dedication

To my son, J.
Chapter 1
Introduction

In this dissertation, we will explore the proportion of squarefree numbers among the values of certain multivariable polynomials, when the arguments are allowed to run over all integers. A squarefree number is one which has no square divisors (other than 1). For example, 14 = 2 · 7 is squarefree, while 12 = 2² · 3 is not.

For any polynomial \( g(x) \) in \( s \) variables, with no square factors or fixed square divisors, it would be reasonable to guess that \( g(x) \) should be squarefree infinitely often. Furthermore, one could expect an asymptotic formula for how often \( g(x) \) is squarefree.

1.1 The Expected Result

Let \( \rho(n) \) be the number of \( x \) in \((\mathbb{Z}/n\mathbb{Z})^s \) where \( g(x) \equiv 0 \pmod{n} \), and let \( \mathfrak{B} \) be some box \([a_1, b_1] \times \cdots \times [a_s, b_s]\) in \( \mathbb{Z}^s \). Then by \( B\mathfrak{B} \) we mean the box \([Ba_1, Bb_1] \times \cdots \times [Ba_s, Bb_s]\). We will define

\[
N_g(B) = \#\{x \in B\mathfrak{B} : g(x) \text{ is squarefree}\}.
\]

For a given prime \( p \), the proportion of \( x \) in \( \mathbb{Z}^s \) where \( p^2 \) divides \( g(x) \) is \( \frac{\rho(p^2)}{p^{2s}} \), which follows from the definition of \( \rho(p^2) \). If we assume that \( g(x) \) being divisible by \( p^2 \) is an independent event for each prime, then the proportion of \( x \) in \( \mathbb{Z}^s \) where \( g(x) \) is not divisible by any \( p^2 \) would be

\[
\prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right).
\]
It would follow then that
\[
\lim_{B \to \infty} \frac{N_g(B)}{\text{Vol}(\mathcal{B})B^s} = \prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right).
\]

While \textit{a priori} we cannot assume this independence, we would expect to have
\[
N_g(B) = \text{Vol}(\mathcal{B})B^s \prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right) + o(B^s). \tag{1.1}
\]

### 1.2 Previous Research

Indeed, for many classes of polynomials, results similar to 1.1 have been established in the literature. Early work in this subject pertained to single-variable polynomials. The first such result was that of Gegenbauer in 1885 [13,34], who gave an asymptotic formula for the number of squarefree integers in the interval $[1, B]$. This could be interpreted as $N_g(B)$ when $g(x) = x$. The next result was in 1922 by Nagel [36], who showed that there are infinitely many $k$-free values when $g(x)$ is a degree $k$ irreducible polynomial. Additionally, Nagel showed that if $g(x)$ is a linear polynomial, there are infinitely many squarefree values. In 1931, Estermann [8] showed that when $g(x) = x^2 + 1$ there is a positive proportion of squarefree values.

In 1933, Ricci [41] gave an asymptotic formula for the number of $k$-free values of $g(x)$ when $k$ is at least the degree of $g$. Erdős [7] in 1953 showed that when the degree $d$ of $g$ is at least 3, with no $(d - 1)$ power linear factors, and when $d$ is a power of 2 if $g$ is not identically divisible by $2^{d-1}$, then $g(x)$ is $(d - 1)$ power free infinitely often. Erdős further asked if the expected results still held when the domain of $g(x)$ was restricted to primes. In the same year, Cugilani [5] gave a bound on size of the gaps between integers $q_1 < q_2 < \ldots < q_n < \cdots$ where $g(q_i)$ is $k$-free.

Hooley, [23] gave an asymptotic formula similar to 1.1 for the number of $(d-1)$-free values of an irreducible polynomial of degree $d$. In 1977 [24,25], he made progress on Erdős’ conjecture, giving an asymptotic formula for the amount of $(d-1)$-free values of degree $d$ irreducible polynomials for prime inputs, when $d \geq 55$, and for smaller values of $d$ with some additional conditions.

Nair gave estimates on the $k$-free values of $g(x)$ on intervals $(x, x + h]$ in 1976 [37] and 1979 [38]. He and Huxley [29] improved on these in 1980, and established the same type of results from prime inputs. Filaseta [9–11] proceeded to improve these
results between 1988 and 1993.

In 1998, Granville [14] gave a formula for the proportion of squarefree values for $g(x)$ having any degree, provided there are no repeated roots or fixed square divisors, assuming the abc conjecture. In 2007, Lee and Murty [32] extend this result to $k$-free values, and giving an asymptotic formula with an error term. For $k = 2$, they required an “abscissa conjecture.” In 2014, Murty and Pasten [35] removed this dependence.

In 2004, Helfgott [20] gave an unconditional asymptotic formula for squarefree values of irreducible polynomials of degree 3, and in 2007 [21] gave the probability that $g(p)$ is $(d - 1)$-free when $g$ has degree $d$. In 2014 [22], he gave an asymptotic formula for the number of primes where $g(p)$ is squarefree for any cubic polynomial without repeated roots.

Heath-Brown [18] established the formula for $k$-free values of polynomials of degree $d \geq 3$ given that $k \geq (3d + 2)/4$. In 2011, Browning [4] improved this restriction to $k \geq (3d + 1)/4$, and gave the corresponding formula for prime inputs. In 2013, Heath-Brown [19] established the formula for $g(x) = x^d + c$ when $g(x)$ is irreducible and $k \geq (5d + 3)/9$. Finally, in 2018 Reuss [40] gave an asymptotic formula for the number of primes $p$ where $g(p)$ is $(d - 1)$-free if $g$ has degree $d$ and has no fixed divisor $p^{d-1}$.

Recently, progress has been made toward establishing this asymptotic formula for multi-variable polynomials. The first such result was by Greaves [15] in 1992, where he established the formula for binary forms with nonzero discriminants, nonzero diagonal terms, and irreducible factors of bounded degree. In 1994, Filaseta [12] showed that if $g(x, y)$ is a binary form with degree $d$ and no fixed $k$-th power factors, then the asymptotic formula holds for $k$-free values when $k \geq (2\sqrt{2} - 1)d/4$.

Granville, in 1998 [14] gave the proportion of squarefree values for a binary form of any degree with no repeated linear factors and no fixed square divisor, assuming the abc conjecture. In 2003 Poonen [39] showed that if $B = \{ x \in \mathbb{Z}^s : 0 \leq x_i \leq B_i \}$ then

$$\lim_{B_1 \to \infty} \cdots \lim_{B_s \to \infty} \frac{N_g}{\text{Vol} B} = \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right),$$

a slightly different formula than 1.1, so long as $g$ has no square factor in $\mathbb{Q}[x]$ assuming the abc conjecture. He also notes that the abc conjecture is unnecessary if each irreducible factor of $g$ has degree at most 3. In 2004, Helfgott established the asymptotic formula unconditionally for squarefree values of binary forms with degree
at most 6.

Later, in 2009, Hooley [26,27] gave the asymptotic formula for the $k$-free values of a polynomial in two variables (not necessarily a form) provided that $g(x, y)$ is irreducible of degree $d$, not a polynomial in some linear combination of $x$ and $y$, has no fixed $k$-power divisors, and is a product of linear factors in some extension field of $\mathbb{Q}$, and $k \geq d/2 - 1$.

Browning, in his 2011 paper [4], shows that for $g(x, y)$ there is a positive proportion of $(x,y)$ where $g(x,y)$ is $k$-free when

$$k > \begin{cases} 
\frac{7d}{16} & \text{if } g \text{ is homogeneous} \\
\frac{39d}{64} & \text{otherwise.}
\end{cases}$$

This is an improvement over previous results when $d \geq 18$ in the homogeneous case and when $d = 5, 11$ or $d \geq 13$ in the non-homogeneous case.

Recently Xiao has obtained several results of this type. In 2017 [46], he showed that if a form of degree $d$ in $s$ variables factors into a product of linear forms, and has nonzero discriminant, then the asymptotic formula holds for $k$-free values when $k \geq (d - 2)/s$. In the same year [45] he established the asymptotic formula for $k$-free values of binary forms of degree at least 2 with nonzero discriminant, no fixed $k$-th power divisor, $d$ the largest degree among the irreducible factors, and

$$k > \min \left\{ \frac{7d}{18}, \left\lfloor \frac{d}{2} \right\rfloor - 2 \right\}.$$ 

He and Stewart [43] gave a formula for the number of $k$-free $h \leq Z$ that were represented by a degree $D$ form with largest irreducible factor degree $d$, under the same restrictions as his previous result. Note that this formula counts elements of the range as opposed to the domain, and so differs from the usual result by the number of representations of $h$. Lastly, he and Lapkova [31] gave a general version of the formula for $k$-free values as long as $g$ has degree $d$, no fixed square factors, and $k \geq (3d + 1)/4$.

Other results have recently been established for specific classes of multi-variable polynomials. In 2014, Bhargava [2] gave a formula for squarefree values of “invariant polynomials” arising from certain algebraic invariants. In 2016, Bhargava, Shankar, and Wang [3] gave a formula for the squarefree values of discriminants of monic integer
polynomials. Ordering by height, they obtained a slightly different density

\[
\prod_p \left( 1 - \frac{1}{p} + \frac{(p-1)^2}{p^2(p+1)} \right).
\]

For “incomplete norm forms,” a type of multivariable polynomial determined by irreducible one variable polynomials, Maynard [33] gave a formula for the number of primes represented.

1.3 Main Results

In this text, we establish formulas in the form of 1.1 for various classes of polynomials. In Chapter 4, we will consider sums of single-variable polynomials of degree 3, that is

\[ g(x) = f_1(x_1) + \cdots + f_s(x_s) \]

where each \( f_i \) is a cubic polynomial in \( x_i \). We are able to obtain the desired asymptotic formula when \( s \) is at least 3. In Chapter 5, we examine the specific case when \( s = 2 \) and \( f_1(x) = x^3 \), \( f_2(y) = y^3 \).

In Chapters 6 and 7, we establish the formula for cubic forms. In Chapter 6, we consider the special case where one variable appears only as a cube, that is

\[ g(x) = x_1^3 + F(x_2, \ldots, x_s) \]

where \( F \) is a cubic form in \( s-1 \) variables. For this class of cubic forms, we are able to obtain the desired formula when \( s \) is at least three (although note that \( s = 2 \) is essentially equivalent to the case discussed in Chapter 5). In Chapter 7, we consider more general cubic forms, but still need to insist on some conditions, including nonsingularity, for our method to yield results.
Chapter 2  
Preliminary Results

Throughout this dissertation, we will make use of several common results from analysis and number theory. We will list the most common ones here.

2.1 The Möbius Function

When studying squarefree numbers, the Möbius function, given by

$$\mu(n) = \begin{cases} (-1)^k & n = p_1p_2\cdots p_k \text{ (all distinct)} \\ 0 & \text{otherwise} \end{cases}$$

is quite useful. We can immediately see that $|\mu(n)| = 1$ if and only if $n$ is squarefree. Another identity that $\mu(n)$ satisfies is

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1. \end{cases}$$

We give the proof for this identity from [1]. When $n = 1$, the identity is obviously true. If $n > 1$, then $n$ can be written as a product of primes $n = p_1^{a_1} \cdots p_k^{a_k}$. In the sum $\sum_{d|n} \mu(d)$, the only nonzero terms will come from $d = 1$ and when $d$ is a product of distinct primes. Therefore,

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2\cdots p_k)$$
\[ = 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k = (1 - 1)^k = 0 \]

From this identity, we obtain
\[ \sum_{d|n} \mu(d) = |\mu(n)| \]
which we make use of in our method. If \( n < 0 \), this identity also holds, as \( \mu(-n) = \mu(n) \).

### 2.2 Hua’s Lemma

There are two versions of Hua’s Lemma that we make use of in this text. The first version deals with sums of \( k \)th powers.

**Lemma 2.1.** Let \( f(\alpha) = \sum_{m=1}^{N} e(\alpha m^k) \). Then for \( 1 \leq j \leq k \)
\[ \int_0^1 |f(\alpha)|^{2j} d\alpha \ll N^{2j-j+\varepsilon} \]

The proof is from Chapter 2 of [44] and makes use of Weyl’s Lemma.

**Lemma 2.2 (Weyl).** Let \( T(\phi) = \sum_{x=1}^{Q} e(\phi(x)) \) where \( \phi \) is an arbitrary arithmetical function. Then
\[ |T(\phi)|^{2j} \leq (2Q)^{2j-j-1} \sum_{|h_1|<Q} \cdots \sum_{|h_j|<Q} T_j \]
where
\[ T_j = \sum_{x \in I_j} e(\Delta_j(\phi(x); h_1, \ldots, h_j)) \]
and the intervals \( I_j = I_k(h_1, \ldots, h_j) \) (possibly empty) satisfy
\[ I_1(h_1) \subset [1, Q], I_j(h_1, \ldots, h_j) \subset I_{j-1}(h_1, \ldots, h_{j-1}). \]

Here \( \Delta_j \) is the \( j \)th iterate of the forward difference operator, so that
\[ \Delta_1(\phi(\alpha); \beta) = \phi(\alpha + \beta) - \phi(\alpha) \]
and
\[ \Delta_{j+1}(\phi(\alpha); \beta_1, \ldots, \beta_{j+1}) = \Delta_1(\Delta_j(\phi(\alpha); \beta_1, \ldots, \beta_j); \beta_{j+1}). \]

It follows that
\[ \Delta_j(\alpha^k; \beta_1, \ldots, \beta_j) = \beta_1 \cdots \beta_j p_j(\alpha; \beta_1, \ldots, \beta_j) \]
where \( p_j \) is a polynomial in \( \alpha \) with degree \( k - j \) which has leading coefficient \( k!/(k - j)! \).

First we prove Weyl’s Lemma.

**Proof.** By induction on \( j \). For brevity, write \( \Delta_j(x) \) for \( \Delta_j(\phi(x); h_1, \ldots, h_j) \). Obviously
\[
|T(\phi)|^2 = \sum_{x=1}^{Q} \sum_{h_1=1-x}^{Q-x} e(\Delta_1(x)) = \sum_{h_1=1-Q}^{Q-1} \sum_{x \in I_1} e(\Delta_1(x))
\]
where \( I_1 = [1, Q] \cap [1 - h_1, Q - h_1] \).

Now if the conclusion of the lemma is assumed for a particular value of \( j \), then by Cauchy’s inequality,
\[
|T(\phi)|^{2j+1} \leq (2Q)^{2j+1-2j-2} (2Q)^j \sum_{h_1, \ldots, h_j} |T_j|^2
\]
and obviously
\[
|T_j|^2 = \sum_{|h| \leq Q} \sum_{x \in I_{j+1}} e(\Delta_j(x + h) - \Delta_j(x))
\]
with \( I_{j+1} = I_j \cap \{ x : x + h \in I_j \} \).

Now the proof of Hua’s Lemma follows.

**Proof.** By induction on \( j \). The case \( j = 1 \) is immediate from Parseval’s identity.

Now suppose the lemma holds for \( 1 \leq j \leq k-1 \). By Weyl’s lemma with \( \phi(x) = \alpha x^k \),
\[
|f(\alpha)|^2 \leq (2N)^{2j-j-1} \sum_{h_1, \ldots, h_j \in I_j} \sum_{|h_i| \leq N} e(\alpha h_1 \cdots h_j p_j(x; h_1, \ldots, h_j))
\]
where \( p_j(x; h_1, \ldots, h_j) \) is a polynomial in \( x \) of degree \( k - j \) with integer coefficients. Hence
\[
|f(\alpha)|^2 \ll (2N)^{2j-j-1} \sum_{h} c_h e(\alpha h) \tag{2.1}
\]
where \( c_h \) is the number of solutions of the equation

\[ h_1 \cdot h_j p_j(x; h_1, \ldots, h_j) = h \]

with \(|h_i| < N\) and \( x \in I_j \). Clearly

\[ c_0 \ll N_j, \quad c_h \ll N^\varepsilon(h \neq 0). \]

By writing

\[ |f(\alpha)|^{2^j} = f(\alpha)^{2^{j-1}} f(-\alpha)^{2^{j-1}} \]

one also obtains

\[ |f(\alpha)|^{2^j} = \sum_h b_h e(-\alpha h) \tag{2.2} \]

where \( b_h \) is the number of solutions of

\[ x_1^k + \cdots + x_{2j-1}^k - y_1^k - \cdots - y_{2j-1}^k = h \]

with \( x_i, y_i \leq N \). Thus

\[ \sum_h b_h = f(0)^{2^j} = N^{2^j} \]

and, on the inductive hypothesis,

\[ b_0 = \int_0^1 |f(\alpha)|^{2^j} d\alpha \ll N^{2^j - j + \varepsilon}. \]

By 2.1, Parseval’s identity, and 2.2,

\[ \int_0^1 |f(\alpha)|^{2^{j+1}} d\alpha \ll (2N)^{2^j - j - 1} \sum_h c_h b_h. \]

Moreover,

\[ \sum_h c_h b_h \ll c_0 b_0 + N^\varepsilon \sum_{h \neq 0} b_h \ll N^j N^{2^j - j + \varepsilon} + N^\varepsilon N^{2^j}, \]

which gives the desired conclusion.

\[ \square \]

The more general version, which applies to sums of polynomials, is Theorem 4 in
Hua’s book [28]. All of Chapter 3 in that book is dedicated to proving this version.

**Lemma 2.3.** Let \( f(x) \) be a polynomial of degree \( k \) with integer coefficients. Set

\[
T(\alpha) = \sum_{x=1}^{P} e(f(x)\alpha).
\]

Then for \( 1 \leq \nu \leq k \),

\[
\int_{0}^{1} |T(\alpha)|^{2\nu} \, d\alpha \ll P^{2\nu - \nu} \log(P)^A
\]

where \( A \) and the implicit constant depend on \( k, \nu, \) and the coefficients of \( f(x) \).

Note that when \( f(x) = x^k \), the two versions of the lemma agree.

### 2.3 Other Necessary Results

In Chapter 4, we need the following estimate for exponential sums, which is Corollary 2.1 in [42].

**Lemma 2.4.** Suppose \( p \) is a prime. Suppose \( g(X) = a_nX^n + \cdots + a_0 \) is a polynomial with integer coefficients having \( 0 < n < p \) and \( p \nmid a_n \). Then

\[
\left| \sum_{x=0}^{p-1} e(g(x)/p) \right| \leq (n - 1)p^{1/2}.
\]
Chapter 3  
The General Procedure

For each of the primary cases described in this dissertation, our procedure begins in the same manner. Given a polynomial $g(x)$ in $s$ variables and a box $\mathcal{B} = \left[ a_1, b_1 \right] \times \cdots \times \left[ a_s, b_s \right]$, we want to find an asymptotic formula for

$$N_g(B) = \# \{ x \in B\mathcal{B} : g(x) \text{ is squarefree} \}.$$

Setting $R(n) = \# \{ x \in B\mathcal{B} : g(x) = n \}$, we can use the previously described properties of the Möbius function to write

$$N_g(B) = \sum_{n \ll B^3} \mu(n)^2 R(n) = \sum_{n \ll B^3 \atop n \neq 0} \left( \sum_{d \mid n} \mu(d) \right) R(n)$$

where the sums in $n$ are taken over all possible values of $g(x)$ with $x \in B\mathcal{B}$, with $n = 0$ excluded as $\mu(0) = 0$. Note that there is a constant $A$ where $|g(x)| \leq AB^3$ for all $x \in B\mathcal{B}$. Interchanging the order of summation gives us

$$N_g(B) = \sum_{d \ll B^{3/2}} \mu(d) \sum_{n \ll B^3 \atop d \mid n \atop n \neq 0} R(n).$$

We then introduce a parameter $D$ to split the domain of $d$:

$$N_g(B) = \sum_{d \leq D} \mu(d) \sum_{n \ll B^3 \atop d \mid n \atop n \neq 0} R(n) + \sum_{D < d \ll B^{3/2}} \mu(d) \sum_{n \ll B^3 \atop d \mid n \atop n \neq 0} R(n).$$
We will refer to these sums as

\[ S(1, D) = \sum_{d \leq D} \mu(d) \sum_{\substack{n \ll B^3 \dfrac{d^2}{n} \atop n \neq 0}} R(n) \]

and

\[ S(D, B^{3/2}) = \sum_{D < d \ll B^{3/2}} \mu(d) \sum_{\substack{n \ll B^3 \dfrac{d^2}{n} \atop n \neq 0}} R(n) \]

and will analyze them individually. Note that there is an implicit constant involved in the domain of \( S(D, B^{3/2}) \), but in each application this will end up in the error term, so there is no need to write it explicitly.

### 3.1 The Sum \( S(1, D) \)

For a given value of \( d \), we can expand the inner sum according to residue classes mod \( d^2 \) as

\[
\sum_{\substack{n \ll B^3 \dfrac{d^2}{n} \atop d^2 | n}} R(n) = \sum_{\substack{x \in B \dfrac{g(x)}{d^2} \atop d^2 | g(x)}} \sum_{\substack{1 \leq y_1, y_2, \ldots, y_s \leq d^2 \atop y_i \equiv y_i (mod \ d^2)}} 1
\]

\[ = \sum_{\substack{1 \leq y_1, y_2, \ldots, y_s \leq d^2 \atop d^2 | g(y)}} \prod_{i=1}^{s} \left( \frac{B(b_i - a_i)}{d^2} + O(1) \right) \]

\[ = \rho(d^2) \prod_{i=1}^{s} \left( \frac{B(b_i - a_i)}{d^2} + O(1) \right) \]

\[ = \rho(d^2) \frac{B^s \text{Vol}(B)}{d^{2s}} + O \left( \rho(d^2) \left( \frac{B^{s-1}}{d^{2s-2}} + 1 \right) \right). \]

It follows, then, that

\[ S(1, D) = \sum_{d \leq D} \mu(d) \sum_{\substack{n \ll B^3 \dfrac{d^2}{n} \atop n \neq 0}} R(n) - \sum_{\substack{d \leq D \atop d^2 | n}} \mu(d) R(0) \]
\[ B^s \text{Vol}(\mathcal{B}) \sum_{d \leq D} \frac{\mu(d) \rho(d^2)}{d^{2s}} + O \left( \sum_{d \leq D} \mu(d)^2 \rho(d^2) \left( \frac{B^{s-1}}{d^{2s-2}} + 1 \right) + DR(0) \right) \]

\[ = B^s \text{Vol}(\mathcal{B}) \sum_{d=1}^{\infty} \frac{\mu(d) \rho(d^2)}{d^{2s}} + O \left( \sum_{d \leq D} \mu(d)^2 \rho(d^2) \left( \frac{B^{s-1}}{d^{2s-2}} + 1 \right) + DR(0) \right) \]

In later chapters, we will obtain estimates for \( \rho(d^2) \) for each case that allow us to express the error term as a power of \( B \). We will also need to justify the convergence of the infinite sum in the last line above. Additionally, we will show that \( R(0) \ll B^{s-1} \) so that \( DR(0) \) is absorbed into the rest of the error term.

### 3.2 The Sum \( S(D, B^{3/2}) \)

We apply the Cauchy-Schwarz inequality to \( S(D, B^{3/2}) \) to write

\[
S(D, B^{3/2}) = \sum_{D < d \leq B^{3/2}} \mu(d) \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} R(n) \\
\leq \left( \sum_{D < d \leq B^{3/2}} \mu(d) \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} 1 \right)^{1/2} \left( \sum_{D < d \leq B^{3/2}} \mu(d) \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} R(n)^2 \right)^{1/2}.
\]

For the first factor, we have the simple estimate

\[
\sum_{D < d \leq B^{3/2}} \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} 1 \ll \frac{B^3}{D},
\]

and for the second factor, we note that

\[
\sum_{D < d \leq B^{3/2}} \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} R(n)^2 = \sum_{n \leq B^3 \atop d^2 | n \atop n \neq 0} R(n)^2 \sum_{D < d \leq B^{3/2} \atop d^2 | n} 1 \ll B^s \sum_{n \leq B^3} R(n)^2
\]
where the term with \( n = 0 \) is included in the final sum. Therefore, we have

\[
S(D, B^{3/2}) \ll \frac{B^{3/2+\varepsilon}}{D^{1/2}} \left( \sum_{n \ll B^3} R(n)^2 \right)^{1/2}.
\]

As with \( S(1, D) \) the sum \( \sum_{n \ll B^3} R(n)^2 \) will be approximated separately for each type of polynomial. Then these estimates will be combined and a suitable choice for \( D \) will be made.
Chapter 4  
Sums of Cubic Polynomials

In this chapter, we will establish the desired asymptotic formula when \( g(x) \) is the sum of at least three cubic polynomials.

**Theorem 4.1.** Suppose \( s \geq 3 \), \( g(x) = f_1(x_1) + \cdots + f_s(x_s) \) with each \( f_i \) a polynomial of degree 3 with integer coefficients. Then for \( s \geq 4 \) we have

\[
N_g(B) = B^s \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{s-\frac{2s-1}{4s-1}+\varepsilon})
\]

and

\[
N_g(B) = B^3 \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^6} \right) + O(B^{3-\frac{1}{4}+\varepsilon})
\]

when \( s = 3 \).

We also establish the following two corollaries.

**Corollary 4.2.** If

\[
\prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) = 0,
\]

it must be the case that there exists a prime \( p_1 \) where \( f_i(x) \equiv f_i(0) \pmod{p_1^2} \) for each \( i \) and for all \( x \), and \( f_1(0) + \cdots + f_s(0) \) is divisible by \( p_1^2 \).

**Corollary 4.3.** If \( f_i(x_i) = x_i^3 \) for each \( i \), then

\[
\prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) > 0
\]

and so there are infinitely many integer \( s \)-tuples \( x \) for which \( g(x) = x_1^3 + \cdots + x_s^3 \) is squarefree.
4.1 Required Estimates

In Chapter 3, we saw that our method requires estimates for $\rho(d^2)$ and $\sum_{n \leq B^3} R(n)^2$. We will obtain those estimates here.

**Lemma 4.4.** There is a prime $p_0$ such that when $p > p_0$ and $s \geq 2$, we have

$$\rho(p^2) \ll p^{2s-2}.$$  

**Proof.** Note that

$$\rho(p^2) = \frac{1}{p^2} \sum_{a=1}^{p^2} \sum_{y_1=1}^{y_2} \ldots \sum_{y_s=1}^{y_s} e((f_1(y_1) + f_2(y_2) + \cdots + f_s(y_s))a/p^2)$$

$$= \frac{1}{p^2} \sum_{a=1}^{p^2} \prod_{i=1}^{s} \left( \sum_{y=1}^{y_s} e(f_i(y)a/p^2) \right).$$

Now, letting

$$S_i(q, a) = \sum_{y=1}^{q} e(f_i(y)a/q),$$

the above is equivalent to

$$\frac{1}{p^2} \left( \sum_{(a,p)=1}^{p^2} \prod_{i=1}^{s} S_i(p^2, a) + \sum_{b=1}^{p-1} \prod_{i=1}^{s} S_i(p^2, pb) + \prod_{i=1}^{s} S_i(p^2, p^2) \right).$$

Clearly $S_i(p^2, p^2) = p^2$ and $S_i(p^2, pb) = pS_i(p, b)$. It follows from Lemma 2.4 that $S_i(p, b) \ll p^{1/2}$. For the remaining term, there must be a prime $p_0$ so that when $p > p_0$, $p$ does not divide any of the coefficients of any of the $f_i$. In this case, we have

$$S_i(p^2, a) = \sum_{u=1}^{p} \sum_{v=0}^{p-1} e(f_i(u + vp)a/p^2)$$

$$= \sum_{u=1}^{p} \sum_{v=0}^{p-1} e(f_i(u)a/p^2 + f_i'(u)av/p)$$

$$= \sum_{u=1}^{p} e(f_i(u)a/p^2) \sum_{v=0}^{p-1} e(f_i'(u)av/p)$$

16
\[= p \sum_{u=1}^{p} e(f_i(u)a/p^2)\]

and so

\[|S_i(p^2, a)| \leq 2p.\]

This gives us

\[
\rho(p^2) \ll \frac{1}{p^2} \left(p^{2+s} + p^{3s/2} + p^{2s}\right)
\]

\[
\ll p^s + p^{3s/2-1} + p^{2s-2}.
\]

As long as \(s \geq 2\), we then have \(\rho(p^2) \ll p^{2s-2}\).

\[\square\]

**Lemma 4.5.** The series

\[
\sum_{d=1}^{\infty} \frac{\mu(d)\rho(d^2)}{d^{2s}}
\]

converges absolutely, since \(\rho(d^2) \ll d^{2s-2+\varepsilon}\) for squarefree \(d\), and so is equal to the product

\[
\prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right).
\]

**Proof.** Since \(\rho(d)\) is a multiplicative function, for squarefree \(d\) we have

\[
\rho(d^2) = \prod_{p|d} \rho(p^2).
\]

From the previous lemma, each \(\rho(p^2) \ll p^{2s-2}\), and so \(\rho(d^2) \ll d^{2s-2+\varepsilon}\) since the product of the implicit constants is \(O(d^\varepsilon)\). Then, when \(s \geq 2\),

\[
\sum_{d=1}^{N} \left|\frac{\mu(d)\rho(d^2)}{d^{2s}}\right| \ll \sum_{d=1}^{N} \frac{1}{d^{2+\varepsilon}}
\]

and so the series converges absolutely. \(\square\)

Next we estimate the sum of \(R(n)^2\). The result is different when \(s = 3\) than when \(s \geq 4\).

**Lemma 4.6.** For \(s = 3\), we have

\[
\sum_n R(n)^2 \ll B^{7/2+\varepsilon}
\]
and for $s \geq 4$
\[ \sum_n R(n)^2 \ll B^{2s-3+\varepsilon}. \]

**Proof.** Since the sum represents the solutions for $g(x) = g(y)$, that is,
\[ \sum_n R(n)^2 = \# \{ x, y \in B \mathcal{B} : f_1(x_1) + \cdots + f_s(x_s) = f_1(y_1) + \cdots + f_s(y_s) \} \]

we can express it as
\[
\int_0^1 \sum_{x, y \in B \mathcal{B}} e(\alpha(f_1(x_1) + \cdots + f_s(x_s) - f_1(y_1) - \cdots - f_s(y_s))) \, d\alpha
\]

\[= \int_0^1 \prod_{i=1}^s \left( \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right) \prod_{i=1}^s \left( \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(-\alpha f_i(y_i)) \right) \, d\alpha \]

\[\ll \prod_{i=1}^s \left( \int_0^1 \left| \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} \, d\alpha \right)^{1/s} \]

by Hölder’s inequality. We will consider two cases on $a_i$ and $b_i$.

**Case 1:** If $0 \leq a_i \leq b_i$ or $a_i \leq b_i \leq 0$, then
\[ \left| \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} \ll \left| \sum_{1 \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} + \left| \sum_{1 \leq x_i \leq B_{a_i}} e(\alpha f_i(x_i)) \right|^{2s} \]

or
\[ \ll \left| \sum_{1 \leq x_i \leq -B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} + \left| \sum_{1 \leq x_i \leq -B_{a_i}} e(\alpha f_i(x_i)) \right|^{2s}. \]

For $s = 3$, integrating gives us an expression of the form
\[ \int_0^1 \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right|^6 \, d\alpha \]

which is
\[ \ll \left( \int_0^1 \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right|^4 \, d\alpha \right)^{1/2} \left( \int_0^1 \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right|^8 \, d\alpha \right)^{1/2} \]

by the Cauchy-Schwarz inequality. Applying Hua’s lemma (Lemma 2.3), this is
\[ O(Q^{7/2+\varepsilon}). \] Therefore, in this case, for \( s = 3 \)

\[ \int_0^1 \left| \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^6 \ll B^{7/2+\varepsilon}. \]

For larger \( s \), we use the trivial estimate

\[ \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right| \leq Q \]

and write

\[ \int_0^1 \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right|^{2s} d\alpha \ll Q^{2s-8} \int_0^1 \left| \sum_{1 \leq x_i \leq Q} e(\alpha f_i(x_i)) \right|^{8} d\alpha \ll Q^{2s-3+\varepsilon} \]

and so in this case

\[ \int_0^1 \left| \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} \ll B^{2s-3+\varepsilon}. \]

Case 2: When \( a_i < 0 < b_i \), we have

\[ \left| \sum_{B_{a_i} \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} \ll \left| \sum_{1 \leq x_i \leq -B_{a_i}} e(\alpha f_i(x_i)) \right|^{2s} + \left| \sum_{1 \leq x_i \leq B_{b_i}} e(\alpha f_i(x_i)) \right|^{2s} \]

and so the argument is the same as in the first case. \( \Box \)

### 4.2 Proof of the Theorem

If \( x_2, \ldots, x_s \) are chosen in advance, since \( f_1 \) is a cubic polynomial, there are at most 3 choices for \( x_1 \) so that \( f_1(x_1) + f_2(x_2) + \cdots + f_s(x_s) = 0 \), and so \( R(0) \ll B^{s-1} \).

Recall from Chapter 3 that

\[ S(1, D) = B^s \text{Vol}(\mathfrak{B}) \sum_{d=1}^{\infty} \frac{\mu(d) \rho(d^2)}{d^{2s}} \]

\[ + O \left( \sum_{d \leq D} \frac{\mu(d)^2 \rho(d^2)}{d^{2s}} + 1 \right) + B^s \sum_{d > D} \frac{\mu(d)^2 \rho(d^2)}{d^{2s}} + DR(0) \].
From Lemma 4.5 and the beginning of this section, this is

\[ B^s \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + \left( \sum_{d \leq D} (B^{s-1} d^\varepsilon + d^{2s-2+\varepsilon}) + B^s \sum_{d > D} d^{-2+\varepsilon} + DB^{s-1} \right) \]

\[ = B^s \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{s-1} D^{1+\varepsilon} + D^{2s-1+\varepsilon} + B^s D^{-1+\varepsilon}). \]

We also showed in Chapter 3 that

\[ S(D, B^{3/2}) \ll \frac{B^{3/2+\varepsilon}}{D^{1/2}} \left( \sum_{n \ll B^3} R(n)^2 \right)^{1/2}. \]

When \( n = 3 \), this is

\[ \ll B^{3+1/4+\varepsilon} D^{-1/2} \]

and for \( n \geq 4 \) this is

\[ \ll B^{s+\varepsilon} D^{-1/2}. \]

Putting both of these estimates together gives

\[ N_g(B) = B^3 \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^6} \right) + O(B^2 D^{1+\varepsilon} + D^{5+\varepsilon} + B^3 D^{-1+\varepsilon} + B^{3+1/4+\varepsilon} D^{-1/2}) \]

for \( s = 3 \). Setting \( D = B^\gamma \), the error term becomes

\[ B^{2+\gamma+\varepsilon} + B^{5\gamma+\varepsilon} + B^{13/4-\gamma/2+\varepsilon} \]

which is minimized when \( \gamma = 13/22 \) resulting in

\[ N_g(B) = B^3 \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{3-1/22+\varepsilon}) \]

completing the proof. When \( s \geq 4 \), we have

\[ N_g(B) = B^s \text{Vol}(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{s-1} D^{1+\varepsilon} + D^{2s-1+\varepsilon} + B^s D^{-1+\varepsilon} + B^{s+\varepsilon} D^{-1/2}). \]
Again, setting $D = B^\gamma$ the error term is

$$B^{s-1+\gamma+\varepsilon} + B^{2s\gamma-\gamma+\varepsilon} + B^{3s-\gamma+\varepsilon} + B^{s-\gamma/2+\varepsilon}.$$ 

Setting $\gamma = \frac{2s}{4s-1}$ gives

$$N_g(B) = B^s \text{Vol}(\mathcal{B}) \prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right) + O(B^{s-\frac{2s}{4s-1}+\varepsilon})$$

which was the desired result.

### 4.3 Proofs of the Corollaries

To prove the first corollary, we note that the infinite product cannot diverge to zero, as a consequence of Lemma 4.5, and so the only for it to be equal to zero is if one of the factors were zero. In this case, there would be a $p_1$ so that $\rho(p_1^2) = p_1^{2s}$. In the proof of the lemma, we saw that

$$\rho(p^2) = \frac{1}{p^2} \sum_{a=1}^{p^2} \sum_{y_1=1}^{p^2} \cdots \sum_{y_s=1}^{p^2} e((f_1(y_1) + f_2(y_2) + \cdots + f_s(y_s))a/p^2).$$

To maximize this, we would need to have

$$\sum_{a=1}^{p^2} e((f_1(y_1) + f_2(y_2) + \cdots + f_s(y_s))a/p^2) = p^2$$

for each choice of $(y_1, \ldots, y_s)$. This can only happen if $p^2$ divides $f_1(y_1) + \cdots + f_s(y_s)$ for all choices of $(y_1, \ldots, y_s)$.

Setting $y_1 = y_2 = \cdots = y_s = p_1^2$ shows that $f_1(0) + \cdots + f_s(0)$ must be divisible by $p_1^2$. Then, fixing a $j \leq s$ and setting $x_i = p_1^2$ for all $i \neq j$, we see that we must have $f_j(x) \equiv f_j(0) \pmod{p^2}$ for all $x$.

To prove the second corollary, suppose $g(x_1, \ldots, x_s) = x_1^3 + \cdots + x_s^3$. Similarly to the first corollary, since

$$\{(x_1, \ldots, x_s) : 1 \leq x_i \leq p^2\} = p^{2s}$$

so the only way for the infinite product to be zero is for there to be a prime $p_1$ where
$p_1^2$ divides $x_1^3 + \cdots + x_s^3$ for all choices of $x_i$. However, if $x_1 = 1$ and $x_2 = \cdots = x_s = p_1^2$, we see that $g(x_1, \ldots, x_s) \equiv 1 \pmod{p_1^2}$. Therefore, $\rho(p^2) < p^{2s}$ and so the infinite product must be positive.
Chapter 5  
Sums of Two Cubes

In the previous chapter, we were able to prove our formula for sums of 3 or more cubic polynomials. Unfortunately, our method will not work for a sum of two polynomials, because of a conflict between two of our bounds. For any $s$, we must have

$$\sum_n R(n)^2 \gg B^s$$

since the sum represents the number of solutions to $g(x) = g(y)$, and for any choice of $x$, setting $x = y$ gives a solution. For the case when $s = 2$, the best we could hope for, then, is $B^2$. But this gives us the estimate

$$S(D, B^{3/2}) \ll B^{5/2+\varepsilon} D^{-1/2}$$

which is only $o(B^2)$ if $D$ is larger than $B$. But in this case the error term for $S(1, D)$, which contains the term $B D^{1+\varepsilon}$ would not be $o(B^2)$.

This case was already established by Greaves [15], as it is a binary cubic form, but in this chapter we show how our method can be altered to deal with cases with this kind of obstruction.

**Theorem 5.1.** If $g(x, y) = x^3 + y^3$, then

$$N_g(B) = B^2 Vol(\mathcal{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^4} \right) + O(B^2 (\log B)^{-1}).$$
5.1 Proof of the Theorem

Let $P = (\log B)/2$ and set $D$ to be the product of all primes bounded by $P$,

$$D = \prod_{p \leq P} p.$$ 

Then we can write the number of pairs $(x, y) \in B\mathbb{N}$ where $x^3 + y^3$ is squarefree as

$$N_g(B) \geq N_1 - N_2$$

$$= \# \{(x, y) \in B\mathbb{N} : p^2|x^3 + y^3 \implies p > P\}$$

$$- \# \{(x, y) \in B\mathbb{N} : \text{there exists a prime } p > P \text{ where } p^2|x^3 + y^3\}.$$ 

Note, then, that $N_1 - N_g(B) \leq N_2$ and so $N_g(B) = N_1 + O(N_2)$. The cardinality of the second set above, $N_1$, can be expressed as

$$N_2 = \sum_{P < p \leq B^{3/2}} \sum_{(x, y) \in B\mathbb{N}} \sum_{p^2|x^3 + y^3} 1.$$ 

Since $x^3 + y^3$ factors into $(x + y)(x^2 - xy + y^2)$ we can consider the following cases where $p^2|x^3 + y^3$. 

First, we could have $p^2|x + y$. Such a $p$ must be $\ll B^{1/2}$ as $x$ and $y$ are bounded. For a given $p$, there are $\ll \left(\frac{B}{p^2} + 1\right) B$ choices for $x$ and $y$. Then, we must have

$$N_2 \ll \sum_{P < p \leq B^{1/2}} \left(\frac{B}{p^2} + 1\right) B \ll B^2(\log B)^{-1}.$$ 

Next, we could have $p|x + y$ but $p^2 \nmid x + y$ and so $p|x^2 - xy + y^2$. These conditions together imply that either $p = 3$, or $p|x$ and $p|y$, and so there are at most $\left(\frac{B}{p} + 1\right)^2$ choices for $x$ and $y$. In this case we then have

$$N_2 \ll \sum_{P < p \leq B} \left(\frac{B}{p} + 1\right)^2 \ll B^2(\log B)^{-1}.$$ 

Finally, in the case where $p \nmid x + y$ and $p^2|x^2 - xy + y^2$, given $p$ and $x$, there are at most two choices for $y \pmod{p^2}$. This is because we must have $p \nmid x$ or else we would have $p|y$ and so $p|x + y$. Therefore, given $p$, there are $\ll \left(\frac{B}{p^2} + 1\right) B$ choices for $x$ and
y. Since \( p \ll B^2 \), we have

\[
N_2 \ll \sum_{P < p \ll B^2} \left( \frac{B}{p^2} + 1 \right) B \ll B^2 (\log B)^{-1}
\]

and so \( N_2 \ll B^2 (\log B)^{-1} \) in each case.

For \( N_1 \), we proceed essentially as in the usual method,

\[
N_1 = \sum_{(x,y) \in \mathbb{Z}^2} \sum_{d \mid (x^3 + y^3, D^2)} \mu(d) = \sum_{d \mid D} \mu(d) \sum_{\substack{u,v \leq d^2 \equiv u \pmod{d^2} \equiv v \pmod{d^2} \mid u^3 + v^3}} 1,
\]

which is equivalent to

\[
\sum_{d \mid D} \mu(d) \rho(d^2) \frac{B^2 \text{Vol}(\mathfrak{B})}{d^4} + O(BD^{1+\varepsilon} + D^{3+\varepsilon}).
\]

We can write the sum as a product, giving us

\[
B^2 \text{Vol}(\mathfrak{B}) \prod_{p \leq P} \left( 1 - \frac{\rho(p^2)}{p^4} \right) + O(BD^{1+\varepsilon} + D^{3+\varepsilon}).
\]

Using the result from Lemma 4.5, we can bound the product

\[
\prod_{p > P} \left( 1 - \frac{\rho(p^2)}{p^4} \right)^{-1} \ll \frac{1}{P \log P},
\]

and so we can extend to an infinite product

\[
N_1 = B^2 \text{Vol}(\mathfrak{B}) \prod_{p} \left( 1 - \frac{\rho(p^2)}{p^4} \right) + O \left( \frac{B^2}{P \log P} + BD^{1+\varepsilon} + D^{3+\varepsilon} \right).
\]

Since we set \( P = (\log B)/2 \) we have \( D = O(B^{1/2+\varepsilon}) \) giving the desired estimate

\[
N_g(B) = B^2 \text{Vol}(\mathfrak{B}) \prod_{p} \left( 1 - \frac{\rho(p^2)}{p^4} \right) + O \left( \frac{B^2}{\log B} \right).
\]

25
A Special Case for Cubic Forms

In this chapter, we will consider the special case where $g(x)$ is a cubic form with an isolated variable. We follow the method described in Chapter 3 to prove the following theorem.

**Theorem 6.1.** Let $g(x)$ be a cubic form with $g(x) = x_1^3 + F(x_2, \ldots, x_s)$ where $F$ is a cubic form in $s - 1$ variables, and $F$ is not of the form $AL(x)^3$ where $L(x)$ is a linear form. Then

$$N_g(B) = B^s \text{Vol}(\mathfrak{B}) \prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right) + O(B^{s-\frac{2}{s-2}+\varepsilon}).$$

If $F$ is a linear form cubed, one would expect a similar result to follow from the work of Greaves [15].

As we saw before, we require estimates for $\rho(d^2)$ and $\sum_n R(n)^2$, which we will now establish.

**6.1 Estimating $\rho(d^2)$**

We will use an elementary argument to bound $\rho(p^2)$, which will require the following two theorems from Hardy and Wright [16].

**Lemma 6.2** (Theorem 107). If $f(x)$ is a polynomial of degree $n$ and has more than $n$ roots (mod $p$) then $f(x) \equiv 0$ (mod $p$).

Here by $f(x) \equiv 0$ (mod $p$) we mean each that each coefficient of $f$ is divisible by $p$. 

26
Lemma 6.3 (Theorem 123). The number of solutions to \( f(x) \equiv 0 \pmod{p^a} \) corresponding to a solution \( \xi \) of \( f(x) \equiv 0 \pmod{p^{a-1}} \) is

- zero, if \( f'(\xi) \equiv 0 \pmod{p} \) and \( \xi \) is not a solution to \( f(x) \equiv 0 \pmod{p^a} \),
- one, if \( f'(\xi) \not\equiv 0 \pmod{p} \),
- \( p \), if \( f'(\xi) \equiv 0 \pmod{p} \) and \( \xi \) is a solution to \( f(x) \equiv 0 \pmod{p^a} \).

Lemma 6.3 is commonly referred to as a version of Hensel's Lemma (see [30] for a general statement). We will assume that \( p > 3 \) and is large enough that it does not divide any of the coefficients of \( F(y) \). For a fixed choice of \( (y_1, \ldots, y_{s-1}) \), we have the polynomial congruence in \( x \)

\[
x^3 + F(y_1, \ldots, y_{s-1}) \equiv 0 \pmod{p^2}.
\]

First, if we consider the above congruence modulo \( p \), we see that there can be at most 3 solutions for \( x \) by Lemma 6.2 since the coefficient of \( x^3, 1 \), is not divisible by \( p \).

If \( F(y_1, \ldots, y_{s-1}) \not\equiv 0 \pmod{p} \) then \( \xi \not\equiv 0 \pmod{p} \) for any solution \( \xi \) and so \( f'(\xi) = 3\xi^2 \not\equiv 0 \pmod{p} \) provided \( p > 3 \). Therefore, in this case each solution modulo \( p \) lifts to at most one solution modulo \( p^2 \) by Lemma 6.3 and hence \( \rho(p^2) \ll p^{2s-2} \) as there are \( O((p^2)^{s-1}) \) choices for the \( y_i \).

If \( F(y_1, \ldots, y_{s-1}) \equiv 0 \pmod{p} \), however, then we must have \( x \equiv 0 \pmod{p} \) and so there are \( p \) solutions for \( x \) modulo \( p^2 \). We then want to find a bound for the number of \( (y_1, \ldots, y_{s-1}) \) where this occurs.

Assume that \( y_2, \ldots, y_{s-1} \) have already been chosen, and write \( F(y_1, \ldots, y_{s-1}) \) as a polynomial in \( y_1 \), so

\[
C_0y_1^3 + C_1(y_2, \ldots, y_{s-1})y_1^2 + C_2(y_2, \ldots, y_{s-1})y_1 + C_2(y_2, \ldots, y_{s-1}) \equiv 0 \pmod{p}
\]

where \( C_0 \) is constant, \( C_1 \) is a linear form, \( C_2 \) is a quadratic form, and \( C_3 \) is a cubic form. Again appealing to Lemma 6.2, this congruence either has at most 3 solutions for \( y_1 \) or each coefficient is divisible by \( p \). In the first case, the solutions will lift to at most \( 3p \) choices for \( y_1 \) modulo \( p^2 \) and so \( \rho(p^2) \ll p \cdot p 
\cdot (p^2)^{s-2} = p^{2s-2} \) where each factor represents the number of choices for \( x, y_1 \), and \( (y_2, \ldots, y_{s-1}) \) respectively.

In the alternative case, we must have

\[
C_0 \equiv C_1(y_2, \ldots, y_{s-1}) \equiv C_2(y_2, \ldots, y_{s-1}) \equiv C_3(y_2, \ldots, y_{s-1}) \equiv 0 \pmod{p}.
\]
Since $C_0$ is constant and $p$ was chosen not to divide any coefficient of $F$, we must have $C_0 = 0$. Write $C_1(y_2, \ldots, y_{s-1}) = d_2y_2 + \cdots + d_{s-1}y_{s-1}$. If $d_j \neq 0$ for some $j$ then we have the congruence

$$d_jy_j \equiv -\sum_{i \neq j} d_iy_i \pmod{p}.$$  

If $(y_2, \ldots, y_{j-1}, y_{j+1}, \ldots, y_{s-1})$ are chosen in advance, there is only one $y_j$ that will satisfy this congruence, which corresponds to $p$ choices for $y_j$ modulo $p^2$. In this case, $\rho(p^2) \ll p \cdot p^2 \cdot p \cdot (p^2)^{s-3} = p^{2s-2}$, where each factor represents the number of choices for $x$, $y_1$, $y_j$, and $(y_2, \ldots, y_{j-1}, y_{j+1}, \ldots, y_{s-1})$ respectively.

If each coefficient of $C_1$ is zero, we must turn to $C_2$. Note that $C_0$, $C_1$, and $C_2$ cannot all be identically zero, as we insisted that $y_1$ appear explicitly in $F$. We write

$$2C_2(y_2, \ldots, y_{s-1}) = \sum_{i, j} d_{ij}y_iy_j$$

where $d_{ij} = d_{ji}$. There must be some indices $m$ and $n$, not necessarily distinct, where $d_{mn} \neq 0$. Suppose all of the variables except $x$, $y_1$, and $y_m$ are chosen in advance, and write

$$d_{mm}y_m^2 + 2y_m \sum_{j \neq m} d_{mj}y_j + \sum_{i, j \neq m} d_{ij}y_iy_j \equiv 0 \pmod{p}.$$

Once again, using Lemma 6.2, this congruence either has at most two solutions in $y_m$ modulo $p$, which would lead to at most $2p$ solutions modulo $p^2$, or we must have

$$d_{mm} \equiv 0 \pmod{p}$$

and

$$\sum_{j \neq m} f_{mj}y_j \equiv 0 \pmod{p}.$$  

In the first case, we see that $\rho(p^2) \ll p^{2s-2}$, counting as in the prior cases. In the second case, it is necessary that $m \neq n$, since $d_{mm}$ is the coefficient of the $y_1y_m^2$ term of $F$, and so could not be both nonzero and divisible by $p$. Then, we write the second congruence as

$$d_{mn}y_n \equiv -\sum_{j \neq m \atop j \neq n} d_{mj}y_j \pmod{p}.$$  

For a given choice of $y_j$ for each $j \neq n$, there is only one solution to this congruence in $y_n$ modulo $p$, which lifts to $p$ solutions modulo $p^2$. In this case, $y_1$ and $y_m$ can be
any value, and again we have $\rho(p^2) \ll p^{2s-2}$. Since we’ve accounted for every possible case, we have $\rho(p^2) \ll p^{2s-2}$, as desired

As we showed in Chapter 4, if $d$ is squarefree, it follows that $\rho(d^2) \ll d^{2s-2+\epsilon}$.

### 6.2 A Bound on the Number of Solutions to $F(x) = F(y)$

In order to find an upper bound for

$$\sum_n R(n)^2 = \# \{x_1, x_2, x, y : x_1^3 + F(x) = x_2^3 + F(y)\}$$

we will first find an upper bound for

$$\# \{x, y : F(x) = F(y)\}.$$

We aim to prove the following.

**Theorem 6.4.** If $F(x)$ is a cubic form in $t \geq 2$ variables, satisfying the above conditions, and is not of the form $A\mathcal{L}(x)^3$ where $\mathcal{L}(x)$ is a linear form, then the number $N(P)$ of solutions of

$$F(x) = F(X)$$

with $x, X \in P^B^*$ satisfies

$$N(P) \ll P^{2t-2+\epsilon}.$$  

Here $t$ is $s - 1$, and $P^B^*$ is $[Pa_2, Pb_2] \times \cdots \times [Pa_s, Pb_s]$. We will suppose, for simplicity, that $P^B^* = [-P, P]^t$. In the end, the only difference will be in the implicit constants, so there is no harm in this.

We will begin with two results from Estermann [8].

**Lemma 6.5.** Suppose that $a, b,$ and $n$ are positive integers and let $Q(n; a, b)$ denote the number of solutions of $ax^2 + by^2 = n$ in positive integers $x$ and $y$. Then

$$Q(n; a, b) \leq 2d(n).$$

**Lemma 6.6.** Suppose that $a, b, m,$ and $n$ are positive integers and let $R(n; a, b)$ denote the number of solutions of $ax^2 - by^2 = n$ in positive integers $x$ and $y$ with
ax^2 \leq m. Then

\[ R(n; a, b) \leq 2d(n)(1 + \log m). \]

Another minor lemma we will need is as follows.

**Lemma 6.7.** Suppose that \( n \) is a positive integer, \( b \) is any integer, and \( S(P; n, b) \) denotes the number of integers \( y \in [-P, P] \) such that \( ny + b \) is a perfect square. Let \( k^2 \) be the largest square dividing \( (n, b) \). Then

\[ S(P; n, b) \ll n^\varepsilon \left( 1 + k\sqrt{\frac{P}{n}} \right). \]

Note that setting \( n = 1 \) and \( b = 0 \) shows that this lemma is best possible.

**Proof.** Write \((n, b) = k^2l, n_1 = n/(n, b), \) and \( b_1 = b/(n, b) \) so that \( l \) is squarefree and \((n_1, b_1) = 1\). If \( x \) satisfies \( x^2 = ny + b \), then \( kl|x \). We wish to bound the number of pairs \( z, y \) with \( z \geq 0, y \in [-P, P] \) and \( lz^2 = n_1y + b_1 \). Since \((n_1, b_1) = 1\), we have \((l, n_1) = 1\). Let \( R \) denote the set of residue classes \( r \mod n_1 \) such that \( lr^2 \equiv b_1 \mod n_1 \). Since \((lb_1, n_1) = 1\) we have \#\(R \ll n_1^\varepsilon\). Let \( r \in R \). Then it suffices to bound the number of solutions with \( z \equiv r \mod n_1 \). Let \( z_0 \) be the least such solution and \( y_0 \) the corresponding value of \( y \). Thus for any other solution \( z \), we have \( z = z_0 + n_1v \) where \( v \geq 0 \). Hence

\[ n_1(y - y_0) = (lz^2 - b_1) - (lz_0^2 - b_1) = lz^2 - lz_0^2 = l(z_0 + n_1v)^2 - lz_0^2 = 2lz_0n_1v + ln_1^2v^2 = ln_1v(2z_0 + n_1v) \]

and so \( ln_1v^2 = (y - y_0) - 2lvz_0 \leq 2P \). Therefore, the number of possible \( v \) is

\[ \ll 1 + \sqrt{\frac{P}{ln_1}}, \]

from which the desired result follows. \( \square \)

Next is the main lemma necessary for the theorem.
Lemma 6.8. Let \( P \geq 2 \) and \( Q \geq 2 \), and suppose that \( a, b, c, d, e, \) and \( f \) are integers in \([-Q, Q]\) and let \( \Delta = 4ac - b^2 \) and

\[
\Theta = 4acf + ebd - ae^2 - cd^2 - fb^2.
\]

Let \( N(P, Q) \) denote the number of solutions of

\[
a x^2 + bxy + cy^2 + dx + ey + f = 0
\]

in integers \( x \) and \( y \) with \( x, y \in [-P, P] \). Then we have the following cases:

(i) if \( (a^2 + c^2)\Delta\Theta \neq 0 \), then

\[
N(P, Q) \ll (PQ)^\varepsilon
\]

(ii) if \( (a^2 + c^2)\Delta \neq 0, \Theta = 0 \), and \(-\Delta\) is not a perfect square, then

\[
N(P, Q) \ll 1
\]

(iii) if \( a = c = 0 \) and \( \Delta\Theta \neq 0 \), then

\[
N(P, Q) \ll (PQ)^\varepsilon
\]

(iv) if \( (a^2 + c^2)\Delta \neq 0, \Theta = 0 \), and \(-\Delta\) is a perfect square, then

\[
N(P, Q) \ll P
\]

(v) if \( a \neq 0, 2ae - bd = \Delta = 0 \), and \( d^2 - 4af \) is not a perfect square, then

\[
N(P, Q) = 0
\]

(vi) if \( a \neq 0, 2ae - bd \neq 0, \Delta = 0 \), and \( k^2 \) is the largest square dividing \(|2ae - bd|\), then

\[
N(P, Q) \ll Q^\varepsilon \left(1 + k\sqrt{\frac{P}{|2ae - bd|}}\right)
\]

(vii) if \( a \neq 0, 2ae - bd = \Delta = 0 \) and \( d^2 - 4af \) is a perfect square, then

\[
N(P, Q) \ll P
\]
(viii) if \(a = c = \Theta = 0\) and \(\Delta \neq 0\), then

\[ N(P, Q) \ll P \]

and for completeness, we also state

(ix) if \(a = c = \Delta = \Theta = 0\), then

\[ N(P, Q) \ll P^2. \]

Proof. If \(a = c = 0\), then \(\Delta = -b^2\) and \(\Theta = b(ed - fb)\). Hence if \(\Delta \neq 0\), so that \(b \neq 0\), multiplication by \(b\) gives

\[(bx + e)(by + d) + bf - ed = 0\]

and this has \(\ll (PQ)^\varepsilon\) solutions when \(\Theta \neq 0\) and \(\ll P\) solutions when \(\Theta = 0\). This deals with cases (iii) and (viii) and so, apart from the trivial case (xi), we can suppose that \(a^2 + c^2 \neq 0\), and thus, without loss of generality, that \(a \neq 0\). Completing the square gives the equation

\[(2ax + by + d)^2 + \Delta y^2 + 2(2ae - bd)y + 4af - d^2 = 0.\]

Suppose \(\Delta = 0\). Then we want \(2(bd - 2ae)y + d^2 - 4af\) to be a perfect square. If \(2ae - bd = 0\) and \(d^2 - 4af\) is not a perfect square, then we have no solutions and are in case (v). If \(bd \neq 2ae\), then we are in case (vi) and this follows from Lemma 6.7. If \(bd = 2ae\) and \(d^2 - 4af\) is a perfect square, then \(x\) is determined by \(y\) and we get case (vii). Thus, we may assume that \(\Delta \neq 0\). Completing the square once more gives

\[ \Delta(2ax + by + d)^2 + (\Delta y + 2ae - bd)^2 + 4a\Theta = 0. \]  \hspace{1cm} (6.1) \]

If \(\Theta = 0\) and \(-\Delta\) is not a perfect square, the solutions are only possible with

\[ 2ax + by + d = 0 \]

\[ \Delta y + 2ae - bd = 0 \]

and so \(y\) is determined by the second equation above and then \(x\) is determined by the
first. This gives case (ii).

If \( \Theta = 0 \) and \(-\Delta \) is a nonzero square, say \( m^2 \), then equation 6.1 becomes

\[
(2amx + mby + md)^2 - (m^2y + 2ae - bd)^2 = 0.
\]

Any choice of \( y \) gives \( O(1) \) solutions for \( x \), which gives case (iv).

For the final case, case (i), we write equation 6.1 in the form

\[
\Delta X^2 + Y^2 = -4a\Theta.
\]

If \( \Delta > 0 \) and \(-4a\Theta \leq 0 \), then there is at most one solution in integers \( X \) and \( Y \). If \( \Delta > 0 \) and \(-4a\Theta > 0 \), then we can appeal to Lemma 6.5, and we see that the number of solutions in \( X \) and \( Y \) is \( O(Q^\varepsilon) \).

For each such pair \( X, Y \), there are \( O(1) \) pairs \( x, y \) with \( \Delta y + 2ae - bd = Y \) and \( 2ax + by + d = X \). If \( \Delta < 0 \) and \(-4a\Theta > 0 \), then we write the equation as

\[
Y^2 - (-\Delta)X^2 = -4a\Theta
\]

and use Lemma 6.6 instead. On the other hand, if \( 4a\Theta > 0 \), then we write

\[
(-\Delta)X^2 - Y^2 = 4a\Theta
\]

and proceed in the same way.

We will now give a proof of Theorem 6.4

**Proof.** Now suppose that \( t \geq 2 \). We will write \( F(x) \) as

\[
F(x) = \sum_{i=1}^{t} \sum_{j=1}^{t} \sum_{k=1}^{t} c_{ijk}x_i x_j x_k
\]

where the coefficients are symmetric, that is \( c_{ijk} = c_{\pi(ijk)} \) where \( \pi(ijk) \) is any permutation of \( i, j, \) and \( k \). We will first transform the form, if necessary, so that at least two of the variables, say \( x_1 \) and \( x_2 \), have nonzero \( x_1^3 \) and \( x_2^3 \) terms. If two variables already appear in this way, then we’re done. Otherwise, we have \( c_{111} = 0 \) (replace 1 with 2 if \( x_1^3 \) has a nonzero coefficient). If there is a \( j \) where \( c_{11j} \neq 0 \), then replace \( x_j \) with \( x_j + \lambda x_1 \) where \( \lambda \) is an integer at our disposal. Then \( x_1^3 \) will appear with coefficient
(3c_{11j}\lambda + 3c_{1jj}\lambda^2 + c_{jjj}\lambda^3), taking into account the different permutations of 11j and 1jj. We can choose \( \lambda \) so that this is nonzero.

If \( c_{11j} = 0 \) for every \( j \), we can do the same with \( c_{1jj} \). If one of these is nonzero, then replacing \( x_j \) with \( x_j + \lambda x_1 \) gives us \( x_3^3(3\lambda^2 c_{1jj} + \lambda^3 c_{jjj}) \) which we can make nonzero as well.

If we also have \( c_{1jj} = 0 \) for all \( j \), then since \( x_1 \) appears explicitly there must be \( j \neq k \) where \( c_{1jk} \neq 0 \). Now, replace \( x_j \) with \( x_j + \lambda x_1 \) and \( x_k \) with \( x_k + \mu x_1 \), where \( \lambda \) and \( \mu \) are integers at our disposal. Now we have

\[
(6c_{1jk}\lambda\mu + 3c_{jkk}\lambda^2\mu + 3c_{jjk}\lambda\mu^2 + c_{jjj}\lambda^3 + c_{kkk}\mu^3)x_1^3.
\]

Again, this can be made nonzero with a suitable choice for \( \lambda \) and \( \mu \). This process can be repeated, if necessary, for \( x_2 \). The transformations are invertible, and so this new form represents the same values as the old one, although our domain is now a parallelepiped. This new domain can be contained in \([-cP,cP]^t\) for some constant \( c \), however, so our results are unaffected.

We now will distinguish two variables \( x \) and \( y \) where \( x^3 \) and \( y^3 \) appear explicitly and denote the remaining variables by \( z \). Thus

\[
F(x) = Ax^3 + Bx^2y + Cxy^2 + Dy^3 \\
+ x^2\mathcal{L}_1(z) + xy\mathcal{L}_2(z) + y^2\mathcal{L}_3(x) + x\mathcal{Q}_1(z) + y\mathcal{Q}_2(z) + \mathcal{C}_1(z)
\]

where \( \mathcal{L}_i, \mathcal{Q}_j, \) and \( \mathcal{C}_1 \) are linear, quadratic, and cubic forms, respectively, which are not all identically zero, as the variables in \( z \) must appear explicitly. Additionally, \( AD \neq 0 \) per our choice of \( x \) and \( y \). In fact, we can assume that the \( \mathcal{L}_i \) and the \( \mathcal{Q}_j \) are not all identically zero, otherwise, we would have \( F(x) = \mathcal{C}_0(x,y) + \mathcal{C}_1(z) \) where \( \mathcal{C}_0 \) is a binary cubic form, and the number of solutions to \( F(x) - F(X) = 0 \) is the number of solutions to \( \mathcal{C}_0(x,y) - \mathcal{C}_0(X,Y) = m \) which is bounded by the number of solutions where \( m = 0 \) and so follows from the two variable case (which we establish first).

Let \( R(n) \) here denote the number of solutions of \( F(x) = n \) with \( x \in [-P,P]^t \). Then sorting by the choice of \( z \), we have

\[
R(n) = \sum_{z \in [-P,P]^{t-2}} R(n, z)
\]
where $R(n, z)$ is the number of solutions of

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + x^2L_1(z) + xyL_2(z) + y^2L_3(z) + xQ_1(z) + yQ_2(z) + C_1(z) = n$$

with $x, y, \in [-P, P]$. The object of our theorem, the number of solutions of $F(x) = F(X)$, can then be written as

$$N(P) = \sum_n R(n)^2 = \sum_n \left( \sum_{z \in [-P,P]^{t-2}} R(n, z) \right)^2.$$ 

Applying the Cauchy-Schwarz inequality, we have

$$N(P) \leq (2P + 1)^{t-2} \sum_{z \in [-P,P]^{t-2}} \sum_n R(n, z)^2.$$ 

The double sum represents the number of solutions to

$$Ax^3 + Bx^2y + Cxy^2 + Dy^3 + x^2L_1(z) + xyL_2(z) + y^2L_3(z) + xQ_1(z) + yQ_2(z) + C_1(z) = n$$

This equation has $t+2$ variables, and we want to show that there are $O(P^{t+\epsilon})$ solutions.

Setting $g = X - x$ and $h = Y - y$, the above equation becomes

$$Ag(3x^2 + 3gx + g^2) + B(x^2h + 2gxy + 2ghx + g^2y + g^2h) + C(2hxy + gy^2 + h^2x + 2ghy + gh^2) + Dh(3y^2 + 3hy + h^2) + L_1(z)(2xg + g^2) + L_2(z)(xh + yg + gh) + L_3(z)(2yh + h^2) + gQ_1(z) + hQ_2(z) = 0.$$ 

We will rewrite this as

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

where

$$a = 3Ag + Bh, \quad b = 2Bg + 2Ch, \quad c = Cg + 3Dh,$$
\[ d = 3Ag^2 + 2Bgh + Ch^2 + 2L_1(z)g + L_2(z)h, \]
\[ e = Bg^2 + 2Cgh + 3Dh^2 + L_2(z)g + 2L_3(z)h, \]

and

\[ f = Ag^3 + Bg^2h + Cgh^2 + Dh^3 + L_1(z)g^2 + L_2(z)gh + L_3(z)h^2 + Q_1(z)g + Q_2(z)h. \]

Note that these coefficients depend on \( g, h, \) and \( z, \) but not on \( x \) or \( y. \) We will apply Lemma 6.8 multiple times, for the cases (i) through (ix).

We start by specifically addressing the case when \( t = 2. \) In this case, each term involving \( z \) vanishes. If for a given choice of \( g \) and \( h \) any of cases (i), (ii), (iii), or (v) of Lemma 6.8 hold, we are done, as the number of solutions in \( x \) and \( y \) is \( O(P^\varepsilon). \) In case (iv), the equation \( \Theta = 0 \) is a polynomial in \( g \) where the coefficient of \( g^5 \) is \( A(3AC - B^2). \) If \( 3AC - B^2 \neq 0, \) then \( g \) is determined by \( h \) so we are done. If \( 3AC - B^2 = 0, \) then the \( g^4 \) term of \( \Theta = 0 \) is \( (9A^2D + 2ABC - B^2)g^4h \) which simplifies to \( A(9AD - BC)g^4h \) and so either \( h = 0, \) \( g \) is determined by \( h \) or \( 9AD - BC = 0. \) In the first two cases, we are done. In the third case, we look at the \( h^5 \) term of \( \Theta = 0. \) Either \( h \) depends on \( g \) or we have

\[ 3AC - B^2 = 9AD - BC = C^2 - 3BD = 0, \]

but this would give \( \Delta = 0, \) which is excluded in case (iv).

For cases (vi) and (vii), \( \Delta = 0 \) gives us

\[ (B^2 - 3AC)g^2 + (BC - 9AD)gh + (C^2 - 3BD)h^2 = 0. \]

If any of these coefficients are nonzero, then \( g \) or \( h \) must be zero, or \( g \) is determined by \( h, \) or vice versa. If all three are zero, then we have the case

\[ F(x, y) = \frac{1}{3BC}(Bx + Cy)^3 \]

which we have excluded.

For cases (vii) and (ix), \( a = c = 0 \) implies that

\[ g = -\frac{Bh}{3A}, \quad h = -\frac{Cg}{3D}. \]

36
In case (vii), $B$ and $C$ cannot both be zero as $\Delta \neq 0$, so we have $g$ determined by $h$ or both are zero, so we are done.

In case (ix), if either $B$ or $C$ were zero, then both $g$ and $h$ would be zero and we would be done, so we suppose $BC \neq 0$. Then $g$ is determined by $h$, so we write $g = \lambda h$ where

$$\lambda = -\frac{B}{3A} = -\frac{3D}{C} = -\frac{C}{B}.$$  

In this case we then have

$$F(x, y) = A(x - \lambda y)^3$$

which we’ve excluded.

Now consider $t > 2$. In the notation of the lemma, if for a given choice of $g$, $h$, and $z$ cases (i), (ii), (iii), or (v) hold, then we are done.

Now consider case (iv). Given that $\Theta = 0$, the coefficient of $g^5$ is $A(3AC - B^2)$. If $3AC - B^2 \neq 0$, then $g$ is determined by $z$ and $h$ so we are done. If $3AC - B^2 = 0$, then $\Theta = 0$ has a term $(9A^2D + 2ABC - B^2)g^4h = A(9AD - BC)g^4h$ and so $h = 0$ or $g$ is determined by $h$. Finally, by considering the $h^5$ term, either we are done or

$$3AC - B^2 = BC - 9AD = C^2 - 3BD = 0.$$  

In this case $a = \frac{B}{C}(Bg + Ch)$, $b = 2(Bg + Ch)$, and $c = \frac{C}{B}(Bg + Ch)$. But then $\Delta = 0$, which is contrary to the assumption in this case.

For the remaining cases, if it should happen that $a = 0$ and $c \neq 0$, we will interchange $x$ and $y$ so that $a \neq 0$ and $c = 0$.

For cases (vi) and (vii), $\Delta = 0$ gives us

$$(B^2 - 3AC)g^2 + (BC - 9AD)gh + (C^2 - 3BD)h^2 = 0.$$  

If any of the coefficients are nonzero, then $g$ or $h$ must be zero, or $g$ is determined by $h$, or vice versa. Otherwise, we have

$$B^2 - 3AC = BC - 9AD = C^2 - 3BD = 0.$$  

Since $AD \neq 0$, we also have $BC \neq 0$ and so

$$A = \frac{B^2}{3C}, \quad D = \frac{C^2}{3B}.$$  

37
and so

\[ a = \frac{B}{C}(Bg + Ch), \quad c = \frac{C}{B}(Bg + Ch) \]

and hence

\[ ax^2 + bxy + cy^2 = \frac{1}{BC}(Bg + Ch)(Bx + Cy)^2. \]

The above immediately implies that \(3C\) divides \(B^2\) and \(3B\) divides \(C^2\), and so all of the following expressions are integer valued. Since \(a \neq 0\), we have \(Bg + Ch \neq 0\). We also have

\[ d = \frac{1}{C}(Bg + Ch)^2 + 2L_1(z)g + L_2(z)h, \]

\[ e = \frac{1}{B}(Bg + Ch)^2 + L_2(z)g + 2L_3(z)h, \]

and

\[ f = \frac{1}{3BC}(Bg + Ch)^3 + L_1(z)g^2 + L_2(z)gh + L_3(z)h^2 + Q_1(z)g + Q_2(z)h. \]

Recall that in case (vi) \(a \neq 0\), \(2ae - bd \neq 0\), \(\Delta = 0\), and in case (vii) \(a \neq 0\), \(2ae - bd = \Delta = 0\), \(d^2 - 4af = m^2\) for some \(m\). Moreover,

\[ 2ae - bd = \frac{2B}{c}(Bg + Ch)\left(\frac{1}{B}(Bg + Ch)^2 + L_2(z)g + 2L_3(z)h\right) - 2(Bg + Ch)\left(\frac{1}{C}(Bg + Ch)^2 + 2L_1(z)g + L_2(z)h\right) \]

so that

\[ 2ae - bd = (Bg + Ch)\left(\frac{2B}{C}L_3(z)h + \left(\frac{Bg}{C} - h\right)L_2(z) - 2L_1(z)g\right). \]

In case (vi), let \(j = |2ae - bd|\) that \(0 < j \ll P^3\). Then \(g, h, \) and \(z\) satisfy

\[ (Bg + Ch)(2BL_3(z)h + (Bg - Ch)L_2(z) - 2CL_1(z)g) = \pm Cj. \]

Then in this case, given \(g, h, \) and \(z\), the number of choices for \(x\) and \(y\) is

\[ \ll P^\varepsilon\left(1 + k\sqrt{\frac{P}{j}}\right) \]

where \(k^2\) divides \(j\). The total contribution from the \(P^\varepsilon\) term is \(O(P^\varepsilon + \varepsilon)\), which is
acceptable. We need to determine the contribution from the $P^\varepsilon k \sqrt{P/j}$ term. We can presume that there is a $j \in \mathbb{N}$ and a $\delta \in \mathbb{Z} \setminus \{0\}$ such that

$$Bg + Ch = \delta$$

and

$$(BL_2(z) - 2CL_1(z))g + (2BL_3(z) - CL_2(z))h = \pm Cj/\delta.$$ Given $g$, the first of these equations determines $h$. Since in the second equation we have $Cj/\delta \neq 0$ and the left side is a linear form in $z$, at least one of the $z_j$ appears explicitly and so is determined by the other variables. Thus, given $j$, the total number of possible $\delta, g, h$ and $z$ is $O(P^{t-2+\varepsilon}).$ Thus the total contribution is

$$\ll P^{t-2+\varepsilon} \sum_{j \ll P^3} \sum_{k \ll P^3/j} k \sqrt{P/j} \ll P^{t-2+\varepsilon} \sum_{k \ll P^{3/2}} P^{1/2} \sum_{l \ll P^3/k^2} l^{-1/2} \ll P^{t+2\varepsilon}$$

and so we are done in this case.

In case (vii) we have

$$(Bg + Ch) \left( \frac{2B}{C} L_3(z)h + \left( \frac{Bg}{C} - h \right) L_2(z) - 2L_1(z)g \right) = 0.$$ Since $a \neq 0$ we have $Bg + Ch \neq 0.$ Thus

$$\frac{2B}{c} L_3(z)h + \left( \frac{Bg}{C} - h \right) L_2(z) - 2L_1(z)g = 0$$

so that

$$(BL_2(z) - 2CL_1(z))g + (2BL_3(z) - CL_2(z))h = 0.$$ If either $BL_2(z) - 2CL_1(z)$ or $2BL_3(z) - CL_2(z)$ is not identically zero, then either $g$ is determined by $h$ and $z$, or $h$ is determined by $g$ and $z$, or there are $O(P^{t-3})$ choices of $z$ for which $BL_2(z) - 2CL_1(z) = 0$ or $2BL_3(z) - CL_2(z) = 0.$ Then we are done by the case (vii) of the lemma. If both $BL_2(z) - 2CL_1(z)$ and $2BL_3(z) - CL_2(z)$ are identically zero, then we have

$$0 = ax^2 + bxy + cy^2 + dx + ey + f$$

$$= \frac{Bg + Ch}{3BC} (3(Bx + Cy)^2 + 3(Bx + Cy)(Bg + Ch) + (Bg + Ch)^2)$$

39
$$+ \mathcal{L}_1(z)g^2 + \mathcal{L}_2(z)gh + \mathcal{L}_3(z)h^2 + \mathcal{Q}_1(z)g + \mathcal{Q}_2(z)h. \quad (6.2)$$

Since both $BL_2(z) - 2CL_1(z)$ and $2BL_3(z) - CL_2(z)$ are identically zero, this becomes

$$G(3X^2 + 3XG + G^2) + \frac{G^2}{B^2}L_1(z) + \frac{G}{B}Q_1(z) + \frac{h}{B}(BQ_2(z) - CQ_1(z)) = 0$$

where $X = Bx + Cy$ and $G = Bg + Ch$. If $G = 0$ or $h = 0$, then $g$ is determined by $h$ and we are done, since we are in case (vii) of the lemma. If $G \neq 0$ but $BQ_2(z) - CQ_1(z) = 0$ identically, then

$$3X^2 + 3XG + G^2 + \frac{G}{B}L_1(z) + \frac{1}{B}Q_1(z) = 0.$$ 

Applying the lemma to this polynomial, since $3, 1$ and $4 \cdot 3 \cdot 1 - 3^2$ are nonzero and $4 \cdot 3 \cdot 1 - 3^2 = 3$ is not a square, we have $P(P^\varepsilon)$ choices for $X$ and $G$ given $z$, and so again we are done.

If $G \neq 0$, $h \neq 0$ and $BQ_2(z) - CQ_1(z)$ is not identically zero, then $G$ divides $h(BQ_2(z) - CQ_1(z))$ and so given $h$ and $z$ there are $O(P^{t-1+\varepsilon})$ choices for $g$. Then, applying the result of the lemma from case (vii), we are done.

For case (viii), note that $a = c = 0$ implies that

$$g = -\frac{Bh}{3A} \quad \text{and} \quad h = -\frac{Cg}{3D}.$$ 

Since $B$ and $C$ cannot both be zero, as $\Delta \neq 0$, we have $g$ determined by $h$. Therefore, there are $O(P^{t-1})$ choices for $g$, $h$, and $z$, and so appealing to the lemma gives $O(P^t)$ solutions.

Case (ix) is similar to case (vii), but now $a = b = c = 0$. Then

$$g = -\frac{Bh}{3A}, \quad h = -\frac{Cg}{3D}.$$ 

Thus $B = 0$ would imply that $g = 0$ and so $h = 0$ and so we are done. Likewise if $C = 0$, and so we can suppose that $BC \neq 0$. Then $g$ is determined by $h$ and vice versa. It follows that $g = \lambda h$ where

$$\lambda = -\frac{B}{3A} = -\frac{3D}{C} = -\frac{C}{B}$$

40
and

\[ 3Ag^2 + 2Bgh + Ch^2 = 0 \]
\[ Bg^2 + 2Cgh + 3Dh^2 = 0 \]
\[ Ag^3 + Bg^2h + Cgh^2 + Dh^3 = 0 \]

and so our equation reduces to

\[ dx + ey + f = 0 \]

where

\[ d = 2L_1(z)g + L_2(z)h, \]
\[ e = L_2(z)g + 2L_3(z)h \]

and

\[ f = L_1(z)g^2 + L_2(z)gh + L_3(z)h^2 + Q_1(z)g + Q_2(z)h. \]

If \( d \neq 0 \) or \( e \neq 0 \), the either \( x \) or \( y \) is fixed by the other variables and we are done. Thus we can suppose that \( d = e = 0 \). Then \( f = 0 \) and so

\[ 2L_1(z)\lambda + L_2(z) = L_2(z)\lambda + 2L_3(z) = 0 \] (6.3)

and

\[ L_1(z)\lambda^2 + L_2(z)\lambda + L_3(z) + Q_1(z)\lambda + Q_2(z) = 0. \] (6.4)

Substituting equations 6.3 into equation 6.4 gives

\[ Q_1(z)\lambda + Q_2(z) = 0. \] (6.5)

If any of the equations 6.3 or 6.5 does not hold identically, then they hold for at most \( O(P^{t-3}) \) choices for \( z \) and we are done. If they all hold identically, then substituting this into the original equation \( F(X, Y, z) = F(x, y, z) \) gives us \( F(x + \lambda h, y + h, z) = F(x, y, z) \) identically for all \( x, y, h \), and \( z \). Taking \( h = -y \), this becomes \( F(x, y, z) = F(x - \lambda y, 0, z) \), and we can appeal to induction on \( t \), unless \( F(x - \lambda y, 0, z) \) can be expressed as a linear form cubed, but then in that case the original \( F(x, y, z) \) could have been as well. \[ \square \]
6.3 Estimating $\sum R(n)^2$

The sum of interest in this case is the number of solutions to $x^3 + F(x) = y^3 + F(y)$ where $(x, x)$ and $(y, y)$ are elements of $B\mathcal{S}$. We can write this as

$$\int_0^1 \sum_{x, y, x, y} e(\alpha(x^3 + F(x) - y^3 - F(y)))d\alpha = \int_0^1 \left| \sum_x e(\alpha x^3) \right|^2 \left| \sum_y e(\alpha F(x)) \right|^2 d\alpha.$$ 

Applying the Cauchy-Schwarz inequality, this is

$$\ll \left( \int_0^1 \left| \sum_x e(\alpha F(x)) \right|^2 d\alpha \right)^{1/2} \left( \int_0^1 \left| \sum_y e(\alpha y^3) \right|^4 \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha \right)^{1/2}.$$ 

The first integral above is the number of solutions of $F(x) = F(y)$ and so by the result from the previous section it must be $O(B^{2s-4+\varepsilon})$. Therefore, the expression above is

$$\ll B^{s-2+\varepsilon} \left( \int_0^1 \left| \sum_y e(\alpha y^3) \right|^4 \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha \right)^{1/2}.$$ 

For the remaining integral, we will modify the proof of Lemma 2.1. We consider

$$\left| \sum_y e(\alpha y^3) \right|^2 = \sum_h \sum_y e(\alpha((y + h)^3 - y^3))$$

where the values of $h$ are $O(B)$ (since $h = y_1 - y_2$ for some $y_1, y_2 \in [Ba_1, Bb_1]$) and each sum in $y$ runs over some subset of $[Ba_1, Bb_1]$ depending on $h$. Simplifying and isolating the term with $h = 0$ shows that the above is

$$\ll B + \sum_{h \neq 0} \sum_y e(\alpha(3y^2 h + 3yh^2 + h^3)).$$

Squaring, we get

$$\left| \sum_y e(\alpha y^3) \right|^4 \ll B^2 + \left| \sum_{h \neq 0} \sum_y e(\alpha(3y^2 h + 3yh^2 + h^3)) \right|^2,$$

which, if we set $j = y_2 - y_1$ so that $y_2 = y_1 + j$, becomes, after applying the Cauchy-
Schwarz inequality,

\[ \ll B^2 + B \sum_{h \neq 0} \sum_j \sum_y e(\alpha(3((y + j)^2 h + 3(y + j)h^2 + h^3) - 3(y^2 h + 3yh^3 + h^3))) \]

\[ = B^2 + B \sum_{h \neq 0} \sum_j \sum_y e(\alpha jh(6y + 3(j + h))). \]

Again, separating the term where \( j = 0 \), we have

\[ B^3 + B \sum_{h \neq 0} \sum_{j \neq 0} \sum_y e(\alpha jh(6y + 3(j + h))). \]

Setting \( u = 6yjh + 3jh(j + h) \) we have

\[ B^3 + B \sum_u c(u)e(\alpha u), \]

where \( c(u) \) is the number of solutions to \( 6yjh + 3jh(h + j) = u \) in \( j, h, \) and \( y \). Since \( h \) and \( j \) must divide \( u \), and once \( h \) and \( j \) are chosen there at most one solution in \( y \), we have \( c(u) \ll |u|^\varepsilon \) for \( u \neq 0 \) and \( c(0) \ll B^2 \). Putting this back into the integral, we have

\[ \int_0^1 \left| \sum_y e(\alpha y^3) \right|^4 \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha \]

\[ \ll B^3 \int_0^1 \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha + B \int_0^1 \sum_u c(u)e(\alpha u) \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha. \]

In the second integral above, if we separate the term where \( u = 0 \), we get another copy of the first term, so the above is

\[ \ll B^3 \int_0^1 \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha + B \sum_{u \neq 0} c(u) \int_0^1 e(\alpha u) \left| \sum_y e(\alpha F(y)) \right|^2 d\alpha. \]

The first integral above is again the number of solutions to \( F(x) = F(y) \) and so is \( O(B^{2s-4+\varepsilon}) \) by Theorem 6.4. The second integral represents the number of solutions to the equation \( F(x) - F(y) = u \). If \( x \) and \( y \) are chosen, there is only one choice for \( u \), and so this integral is \( O(B^{2s-2}) \). Therefore, we have

\[ \sum_{n \ll B^3} R(n)^2 \ll B^{2s-5/2+\varepsilon}. \]
6.4 Proof of the Theorem

As in Chapter 4, if $x_2, \ldots, x_s$ are chosen in advance, there is now at most one possible choice for $x_1$ so that $x_1^2 + F(x_2, \ldots, x_s) = 0$, and so again $R(0) \ll B^{s-1}$. From the previous section, we have

$$S(D, B^{3/2}) \ll \left( \frac{B^{3/2+\varepsilon}}{D^{1/2}} \right) \left( B^{2s-5/2+\varepsilon} \right)^{1/2} = B^{s+1/4+\varepsilon} D^{-1/2}.$$

In Section 6.1, we showed that, for squarefree $d$, we have $\rho(d^2) \ll d^{2s-2+\varepsilon}$. Therefore

$$S(1, D) = B^s \text{Vol}(\mathfrak{B}) \sum_{d=1}^{\infty} \frac{\mu(d) \rho(d^2)}{d^{2s}} + O \left( \sum_{d \leq D} \mu(d)^2 \rho(d^2) \left( \frac{B^{s-1}}{d^{2s-2}} + 1 \right) + B^s \sum_{d > D} \frac{\mu(d)^2 \rho(d^2)}{d^{2s}} + DR(0) \right)$$

$$= B^s \text{Vol}(\mathfrak{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O \left( \sum_{d \leq D} d^{2s-2+\varepsilon} \left( \frac{B^{s-1}}{d^{2s-2}} + 1 \right) + B^s \sum_{d > D} \frac{d^{2s-2+\varepsilon}}{d^{2s}} + DB^{s-1} \right)$$

$$= B^s \text{Vol}(\mathfrak{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O \left( \sum_{d \leq D} B^{s-1} d^\varepsilon + \sum_{d \leq D} d^{2s-2+\varepsilon} + B^s \sum_{d > D} d^{-2+\varepsilon} + DB^{s-1} \right)$$

$$= B^s \text{Vol}(\mathfrak{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O \left( B^{s-1} D^{1+\varepsilon} + D^{2s-1+\varepsilon} + B^s D^{-1+\varepsilon} \right).$$

Combining these, we have

$$N_g(B) = B^s \text{Vol}(\mathfrak{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{s-1} D^{1+\varepsilon} + D^{2s-1+\varepsilon} + B^s D^{-1+\varepsilon} + B^{s+1/4+\varepsilon} D^{-1/2}).$$

Setting $D = B^\gamma$, this becomes

$$N_g(B) = B^s \text{Vol}(\mathfrak{B}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O(B^{s-1+\gamma+\varepsilon} + B^{2s\gamma-\gamma+\varepsilon} + B^{s-\gamma+\varepsilon} + B^{s+1/4-\gamma/2+\varepsilon}).$$
The optimal choice for $\gamma$ here is $\frac{4s+1}{8s-2}$, and with this choice we have

$$N_g(B) = B^s \text{Vol}(\mathfrak{B}) \prod_p \left(1 - \frac{\rho(p^2)}{p^{2s}}\right) + O(B^{s - \frac{1}{8s-2} + \varepsilon}).$$
Chapter 7  |  General Cubic Forms

In this chapter, we will establish the desired result for cubic forms with seven or more variables, satisfying a bound on an associated exponential sum.

For simplicity we will redefine $B\mathbb{B}$ to be the set of integer points in $[0,B]^s$. We suppose $g(\mathbf{x})$ is a cubic form in $s$ variables. We define

$$S(g,\alpha) = \sum_{\mathbf{x} \in B\mathbb{B}} e(\alpha g(\mathbf{x})),$$

and we define a new cubic form $F$ in $2s$ variables by

$$F(x_1,\ldots,x_{2s}) = g(x_1,\ldots,x_s) - g(x_{s+1},\ldots,x_{2s}). \quad (7.1)$$

We will require the following two hypotheses.

**Hypothesis 7.1.** Let $\theta$ be independent of $B$ and satisfy $0 < \theta < 1$. Let $\eta > 0$ be any fixed positive number. Then for every $\alpha$, either

$$|S(F,\alpha)| < B^{2s-\frac{1}{2}s^2+\eta}$$

or $\alpha$ has a rational approximation such that

$$(a,q) = 1, \quad 1 \leq q \ll B^{2\theta}, \quad |q\alpha - a| < B^{-3+2\theta}.$$  

This is alternative (B) from Lemma 13.4 in Davenport [6].

**Hypothesis 7.2.** Let $g_j(\mathbf{x}) = \frac{\partial g(x_1,\ldots,x_s)}{\partial x_j}$. Then for all but finitely many primes $p$, $g(\mathbf{x}), g_1(\mathbf{x}), \ldots, g_s(\mathbf{x})$ have no nontrivial factor in common modulo $p$. 

46
We define a new cubic form $F$ in $2s$ variables by

$$F(x_1, \ldots, x_{2s}) = g(x_1, \ldots, x_s) - g(x_{s+1}, \ldots, x_{2s}).$$

Then we have the following theorem.

**Theorem 7.3.** If $g(x)$ satisfies Hypothesis 7.2 and $F(x)$ satisfies Hypothesis 7.1, then for $s \geq 7$,

$$N_g(B) = B^s \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O\left( B^s - \frac{8s+3}{16s^2} + \delta \right)$$

where $\delta > 0$ is an arbitrary small real number.

### 7.1 Estimating $\rho(d^2)$

We start with the following lemma.

**Lemma 7.4.** For any form $f(x)$, we have $\rho(p) \ll p^{s-1}$ and $\rho(p^2) \ll p^{2s-1}$.

**Proof.** We will prove the first inequality by induction on the degree and the number of variables. For degree one, assume that $p$ is large enough that none of the coefficients of $f$ are divisible by $p$. Our form is then $c_1 x_1 + \cdots + c_s x_s$, and so for each choice of $x_1, \ldots, x_{s-1}$, the value of $x_s$ is determined uniquely.

Now suppose that the form $f(x)$ has degree $d$, and that

$$f(x) = g_0 x_s^d + g_1(y)x_s^{d-1} + \cdots + g_{d-1}(y)x_s + g_d(y)$$

where $y = (x_1, \ldots, x_{s-1})$ and $g_j$ is a form of degree $j$. Choose values for $y$. If there is a $j \leq d - 1$ such that $g_j(y) \not\equiv 0 \pmod{p}$ then there are at most $d$ choices for $x_s$. Otherwise, $g_j(y) \equiv 0 \pmod{p}$ for all $j \leq d - 1$, and so $f(x) \equiv 0 \pmod{p}$ only if $g_d(y) \equiv 0 \pmod{p}$ as well. Then, by induction on $d$ and $s$, the number of $y$ for which $g_d(y) \equiv 0 \pmod{p}$ is $O(p^{s-2})$.

The second inequality follows from the first as there at most $p^s$ solutions to $f(x) \equiv 0 \pmod{p^2}$ for each solution modulo $p$. \qed

Lemma 3.4 in Chapter 4 of [42] states

**Lemma 7.5.** Let $u_1(x), \ldots, u_t(x)$ be polynomials in $n$ variables over $F_q$, each of total degree at most $e$, and without common factor. Then the number of their common zeros is at most $q^{n-2}e^3$.
From this and the argument used to prove Lemma 7.4, we can deduce that if \( g(x) \) satisfies Hypothesis 7.2, then \( \rho(p) \ll p^{s-2} \) and \( \rho(p^2) \ll p^{2s-2} \). It follows, then, that for squarefree \( d \), we have \( \rho(d^2) \ll d^{2s-2+\epsilon} \).

### 7.2 Estimating \( \sum R(n)^2 \)

Given that

\[
S(F, \alpha) = \sum_{x \in (B \mathcal{B})^2} e(\alpha F(x))
\]

in this context, we have

\[
\sum_{n \leq B^3} R(n)^2 = \int_0^1 S(F, \alpha) d\alpha.
\]

Let \( 0 < \theta < 1 \) and call \( \xi(\theta) \) the set of numbers \( \alpha \in [0, 1] \) having a rational approximation satisfying

\[
(a, q) = 1, \quad 1 \leq q \ll B^{2\theta}, \quad |q\alpha - a| < B^{-3+2\theta}.
\]

Then, we call the set of \( \alpha \) belonging to \( \xi(\theta) \) the major arcs and label it \( \mathcal{M} \). We also call its complement relative to \( [0, 1] \) the minor arcs, labeled \( m \). Note that both \( \mathcal{M} \) and \( m \) depend on \( \theta \). The following is an adaptation of Lemma 15.1 in [6].

**Lemma 7.6.** Suppose \( F(x) \) is any cubic form in \( 2s \) variables that satisfies Hypothesis 7.1. Then given a number \( 0 < \Delta < 1 \), where \( 1 < \frac{s}{18} + \frac{\Delta}{3} \), we have

\[
\int_{m} |S(F, \alpha)| d\alpha \ll B^{2s-3+\Delta}.
\]

**Proof.** Choose a set of numbers

\[
\theta = \theta_0 < \theta_1 < \cdots < \theta_h = \frac{3}{4} + \delta
\]

for some small \( \delta > 0 \). Then every real \( \alpha \) lies in \( \xi(\theta_h) \), since one can always find \( a \) and \( q \) where

\[
q \leq B^{3/2}, \quad |q\alpha - a| < B^{-3/2}.
\]

Since \( \xi(\theta_0) \) is the major arcs, and the minor arcs are their complement, the set \( m \) can
be regarded as the union of

\[ \xi(\theta_h) \setminus \xi(\theta_{h-1}), \xi(\theta_{h-1}) \setminus \xi(\theta_{h-2}), \ldots, \xi(\theta_1) \setminus \xi(\theta_0). \]

In each set \( \xi(\theta_g) \setminus \xi(\theta_{g-1}) \) with \( 1 \leq g \leq h \), Hypothesis 7.1 holds with \( \theta = \theta_{g-1} \), so

\[ |S(F, \alpha)| \ll B^{2s - \frac{1}{2} s\theta_{g-1} + \eta}. \]

The measure of this set \( \xi(\theta_g) \setminus \xi(\theta_{g-1}) \) is bounded by the measure of \( \xi(\theta_g) \) which is

\[ \ll \sum_{q \leq B^{2\theta_g}} \sum_{a=1}^{q} q^{-1} B^{-3+2\theta_g}, \]

\[ \ll B^{-3+4\theta_g}, \]

and so the contribution over this set to the integral is

\[ \ll B^{2s - \frac{1}{2} s\theta_{g-1} - 3+4\theta_g + \eta}. \]

Since we require this to be \( O(B^{2s-3+\Delta}) \), we must have 7.2 and

\[ 2s - \frac{1}{2} s\theta_{g-1} - 3 + 4\theta_g + \eta < 2s - 3 + \Delta, \]

or equivalently

\[ \theta_{g-1} < \theta_g < \frac{s}{8} \theta_{g-1} + \frac{\Delta - \eta}{4}. \]

If \( s < 8 \), then we need

\[ \frac{8 - s}{8} \theta_{g-1} < \frac{\Delta - \eta}{4} \]

to hold for all \( g \leq h \) and then we require

\[ \theta_h < \frac{s}{8} \cdot \frac{8}{8 - s} \cdot \frac{\Delta - \eta}{4} + \frac{\Delta - \eta}{4} = \frac{8}{8 - s} \cdot \frac{\Delta - \eta}{4}. \]

By 7.2, this is

\[ \frac{8 - s}{8} \left( \frac{3}{4} + \delta \right) < \frac{\Delta - \eta}{4}. \]
Since $\delta$ and $\eta$ can be made arbitrarily small, we only need
\[
\frac{8 - s}{8} \cdot 3 < \Delta,
\]
or
\[
3 - \frac{3s}{8} < \Delta
\]
which is possible if
\[
1 < \frac{s}{8} + \frac{\Delta}{3}.
\]

**Lemma 7.7.** Under the same conditions as the previous lemma,
\[
\int_{\mathfrak{M}} |S(C, \alpha)| d\alpha \ll B^{s-3+4\theta}.
\]

**Proof.** For any $\alpha$, we have the simple estimate $|S(C, \alpha)| \ll B^s$. Then, as before, the measure of $\mathfrak{M} = \xi(\theta)$ is $O(B^{-3+4\theta})$, which gives the desired result. \qed

Combining the results of these two lemmas, when $\Delta$ is taken to be $4\theta$, we have
\[
\sum_{n \ll B^3} R(n)^2 = \int_0^1 S(F, \alpha) d\alpha \ll B^{2s-3+4\theta}
\]
since $F(x)$ has $2s$ variables.

### 7.3 Proof of the Theorem

If $g(x)$ is a cubic form in one variable, then $R(0) = 1$ and hence is $O(B^{s-1})$. In [17], Heath-Brown shows that $R(0) \ll B^{s-1 - \frac{1}{s} \log(B)^2}$ when $s > 1$, which is more than sufficient for our needs.

Using the previously obtained estimates, we have
\[
S(D, B^{3/2}) \ll \frac{B^{3/2+\varepsilon}}{D^{1/2}} \left( \sum_{n \ll B^3} R(n) \right)^{1/2} \ll B^{s+\varepsilon+2\theta} D^{-1/2}
\]
and

\[ S(1, D) = B^s \text{Vol}(\mathfrak{M}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O \left( B^{s-1} D^{1+\delta} + D^{2s-1-\delta} + B^s D^{-1+\delta} + DR(0) \right). \]

Combining these, we have

\[
N_g(B) = B^s \text{Vol}(\mathfrak{M}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) \\
+ O \left( B^{s-1} D^{1+\delta} + D^{2s-1+\delta} + B^s D^{-1+\delta} + B^{s+\varepsilon+2\theta} D^{-1/2} \right).
\]

Setting \( D = B^\gamma \), the error term becomes

\[
O \left( B^{s-1+\gamma+\gamma \delta} + B^{2s\gamma - \gamma + \gamma \delta} + B^{s-\gamma + \gamma \delta} + B^{s+\varepsilon+2\theta - \gamma/2} \right).
\]

Setting \( \theta = \frac{1}{8} \) (and hence \( \Delta = \frac{1}{2} \)) so that Lemma 7.6 holds with \( s \geq 14 \), then setting \( \gamma = \frac{4s+1}{8s-2} \) we have

\[
N_g(B) = B^s \text{Vol}(\mathfrak{M}) \prod_p \left( 1 - \frac{\rho(p^2)}{p^{2s}} \right) + O \left( B^{s-\frac{8s+1}{16s-4} + \delta} \right).
\]
Chapter 8 | Further Research

The results obtained in this dissertation are part of a quite large problem - determining the density of squarefree numbers amongst the values of an arbitrary polynomial of several variables - and as such there are numerous avenues for further work.

In Chapter 4, we gave an asymptotic formula for the number of squarefree values among sums of 3 or more cubic polynomials. As such a formula was established by Hooley [23, 24] for a single cubic polynomial, the sum of two cubic polynomials presents an obvious gap.

One would also suspect that sums of higher degree polynomials, or even sums of $k$-th powers, would be a reasonable first place to start on the higher degree cases.

In Chapter 6, we had to exclude the case where $g(x) = x_1^3 + A\mathcal{L}(x_2, \ldots, x_s)^3$. One would expect to be able to adapt the work of Greaves [15] - or even the method applied in Chapter 5 - to yield results in this case.

The result we obtained in Chapter 7 for general cubic forms is fairly weak. It should be possible to remove the dependence on the Hypotheses and to reduce the number of variables required.
Bibliography


54


Vita
James M. Kowalski

Education

Doctor of Philosophy  Mathematics, May 2020, Pennsylvania State University

Master of Arts  Mathematics, May 2014, Central Michigan University

Bachelor of Science  Mathematics, May 2011, Central Michigan University

Bachelor of Music Education  Instrumental Music, May 2011, Central Michigan University

Publications