Sums of Integer Cubes

by

Eric Pine

(Under the direction of Andrew Granville)

Abstract

Taxicab numbers, of Hardy and Ramanujan fame, are positive integers which can be represented as the sum of two positive integer cubes, in two distinct ways. The smallest such integer is $1729 = 1^3 + 12^3 = 9^3 + 10^3$. One question which naturally arises, is to ask how many numbers with this property there are, up to some bound N. This is usually denoted $\nu(N)$. The current best lower bound, $\nu(N) > CN^{1/3}\log(N)$, is due to Hooley. The best upper bound, $\nu(N) = O\left(N^{4/9+\epsilon}\right)$, is due to Heath-Brown.

A related question is to count the number of integer solutions to $w^3 + x^3 + y^3 + z^3 = 0$. A solution is considered trivial if it is some permutation of the form $w^3 + (-w)^3 + y^3 + (-y)^3 = 0$. Manin's conjecture states that the number of non-trivial solutions, with $|w|, |x|, |y|, |z| < N^{1/3}$ should be asymptotic to $cN^{1/3}(\log(N))^4$ for some positive constant c.

Using a parametrization found by Euler, we show that the number of such solutions is in fact bounded below as predicted by Manin's conjecture. Moreover, we show that by restricting ourselves to the case where two of w, x, y, z are non-negative and the other two are non-positive (that is, a solution which yields a taxicab number) we get the same lower bound $cN^{1/3}(\log(N))^4$, though not necessarily the same constant.

Index words: Diophantine Equations, Taxicab Numbers, Manin's Conjecture

Sums of Integer Cubes

by

Eric Pine

B.S., Lehigh University, 1995

M.S., Lehigh University, 1997

A Dissertation Submitted to the Graduate Faculty

of The University of Georgia in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2004

Sums of Integer Cubes

by

Eric Pine

Approved:

Major Professor: Andrew Granville

Committee: Matt Baker
E. Rodney Canfield
Akos Magyar
Robert Rumely

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2004

Acknowledgments

The work described in this dissertation could not have been completed if not for the help and support of so many people. I would like to thank my advisor Andrew Granville for his guidance throughout this process; especially for teaching me to ask the right questions. I would like to thank Carl Pomerance for inspiring me to study number theory by describing open problems in such a way that students can not help but direct their energy toward solving them. I would like to thank the members of my committee for all of their patience and helpful suggestions. I would also like to thank all of the graduate students in the department who have made what can be an arduous task, enjoyable. A special thanks to Mike Beck who helped critique my proofs and listened to talks about taxicab numbers more times than I (or he) care to count. To my parents, between their genes and their parenting, anything I am able to accomplish is directly attributable to them. And to my wife for supporting me in every way imaginable, particularly during what can only be described as the longest "two more years." Finally, I would like to thank God for making all things possible.

Table of Contents

Chapter 1

Introduction

Taxicab numbers are so named after a story about mathematicians Hardy and Ramanujan. As the story goes, Hardy went to visit Ramanujan at the hospital as he had fallen ill. Not sure exactly what to say, Hardy mentioned that the number of the taxicab he rode in to get to the hospital was 1729, which he claimed seemed to be a rather uninteresting number. Ramanujan is said to have immediately replied that in fact 1729 was quite interesting, as it is the smallest positive integer which can be written as the sum of two positive integer cubes, in two different ways. Indeed:

$$1729 = 1^3 + 12^3 = 9^3 + 10^3$$

In order to study the positive integers which can be represented as the sum of two cubes in at least two distinct ways, we begin with the following definitions:

$$\begin{aligned} \nu(N) &= \#\{k \leq N : k = x_1^3 + y_1^3 = x_2^3 + y_2^3;\ x_i, y_i \geq 0;\ x_1 \neq x_2, y_2\} \\ r(k) &= \#\{(x,y) : x^3 + y^3 = k \text{ and } x \geq y\} \\ r^+(k) &= \#\{(x,y) : x^3 + y^3 = k \text{ and } x \geq y \geq 0\} \end{aligned} \tag{1.1}$$

The count $\nu(N)$ has been widely studied. In 1963, Hooley [7] showed:

$$\nu(N) = O\left(N^{2/3} \log\log(N)(\log(N))^{-1/2}\right)$$

In 1980, Hooley [8] improved this result to $\nu(N) = O_\epsilon(N^{5/9+\epsilon})$, using the large sieve. In 1995, Trevor Wooley [24] gave an elementary proof of Hooley's second bound using binary quadratic forms.

In 1997, Heath-Brown [6] proved a general theorem about non-singular cubic forms with three rational coplanar lines. Applying the result to this problem gives the current best upper bound for $\nu(N)$:

$$\nu(N) = O_\epsilon(N^{4/9+\epsilon})$$

The current best lower bound for $\nu(N)$ also appeared in Hooley's 1980 paper [8]. He uses a partial parametrization of taxicab solutions given by Ramanujan, which we discuss in chapter eight, to show:

$$\nu(N) > CN^{1/3}\log(N)$$

Note that the count $\nu(N)$ can be expressed as:

$$\nu(N) = \sum_{\substack{n \le N \\ r^+(n) \ge 2}} 1$$

In contrast, the count we consider in this paper is slightly different:

$$\sum_{\substack{n \le N \\ r^+(n) \ge 2}} \binom{r^+(n)}{2} \tag{1.2}$$

This count can be considered counting taxicab numbers with multiplicity where the multiplicity is the number of ways that an integer n can be expressed as the sum of two cubes in two distinct ways. From these expressions we see that if every integer had at most two such representations, these two counts would be equal. But in fact:

$$\begin{aligned}
87539319 &= 167^3 + 436^3 = 228^3 + 423^3 = 255^3 + 414^3 \\
6963472309248 &= 2421^3 + 19083^3 = 5436^3 + 18948^3 \\
&= 10200^3 + 18072^3 = 13322^3 + 16630^3 \\
48988659276962496 &= 38787^3 + 365757^3 = 107839^3 + 362753^3 \\
&= 205292^3 + 342952^3 = 221424^3 + 336588^3 \\
&= 231518^3 + 331954^3
\end{aligned}$$

$$\begin{aligned} 24153319581254312065344 &= 28906206^3 + 582162^3 = 28894803^3 + 3064173^3 \\ &= 28657487^3 + 8519281^3 = 27093208^3 + 16218068^3 \\ &= 26590452^3 + 17492496^3 = 26224366^3 + 18289922^3 \end{aligned}$$

These results were found by Leech [12] in 1957, Rosenstiel et. al. [18] in 1991, Wilson [23] in 1997, and Rathbun [17] in 2002 respectively. The first three of these examples are in fact the smallest such integers with their respective number of representations. The last is conjectured to be the smallest positive integer which can be written as the sum of two positive integer cubes in six different ways, but this is not yet known. More generally, Silverman and Tate [19] show that for any given positive integer N there exists some positive integer which can be written as the sum of two positive integer cubes in N different ways. Their technique uses elliptic curves to find rational solutions, and then by clearing denominators leads to an integer solution. This result may seem a bit unsatisfying as it induces large cube factors. We may then be inclined to modify the question to require that the cubes involved be pairwise coprime. That is, if $w^3 + z^3 = x^3 + y^3 = k$, then $\gcd(w, z) = \gcd(x, y) = 1$. Surprisingly, there are no known integers with at least 4 positive coprime solutions! For the rest of the paper, we will not require this additional pairwise coprimality condition.

An alternative way of looking at this new count of taxicab numbers is to instead consider the equation:

$$w^3 + x^3 + y^3 + z^3 = 0 \tag{1.3}$$

Note that each taxicab number corresponds to a solution to this equation. Moreover if we remove the condition that all of the integers involved in a taxicab number be positive, then the count with multiplicities (1.2) would be the same (up to a constant factor to account for permutations) as counting integer solutions to (1.3) where say $w^3 + z^3 < N$.

In general, suppose $F(w, x, y, z)$ is a non-singular cubic form with integer coefficients. Then Manin's conjecture implies that if there is at least one non-zero solution to $F(w, x, y, z) = 0$, then the number of non-trivial solutions such that $|w|, |x|, |y|, |z| < B$ will be asymptotically $cB(\log B)^r$ where r is the rank of the Picard group of the surface

$F = 0$. Peyre and Tschinkel [14] calculated the rank of the Picard group for the surface (1.3), as $r = 4$.

Now if we are considering solutions to (1.3) which correspond to our original taxicab definition, we need for exactly two of w, x, y, z to be non-negative, say w and z, and the other two to be non-positive, say x and y. Moreover in this case, if we want $w^3 + z^3 = -x^3 - y^3 < N$ then indeed we must have $w, -x, -y, z < N^{1/3}$. Hence Manin's conjecture gives an expected upper bound on (1.2) of $cN^{1/3}(\log N)^4$ by setting $B = N^{1/3}$. In chapter six we show that in fact, (1.2) is bounded *below* by $cN^{1/3}(\log N)^4$.

Chapters two, three, and four discuss the parametrization to (1.3) that Euler found which we will use to bound the number of solutions. In chapter five we discuss the ideas of using this parametrization by giving an upper bound on a special case. In chapter seven we apply the same techniques used for the lower bound to a proof of an upper bound for solutions of a particular type. Chapters eight and nine give and extend a partial parametrization given by Ramanujan which give solutions to (1.3) of a useful type.

Finally, any work involved in adding like powers of integers would not be complete without mentioning Waring's Problem. In 1770, Waring wrote that every positive integer is the sum of at most nine cubes, and the sum of at most 19 fourth powers (for a survey of results and current research on Waring's Problem see [21]). Wieferich in 1909 [22] with Kempner in 1912 [10] finally proved the statement for cubes. Also in 1909, Landau [11] showed that at most a finite number of integers actually required nine cubes. This leads to the more difficult question of how many cubes are required to realize all except a finite number of integers. Framed in this way Landau's result is that at most eight are required for all but a finite number. Dickson in 1939 [3] in fact showed that 23 and 239 are the only two integers for which nine cubes are required. Linnik in 1942 [13] proved that at most seven are required for all except a finite number. As mentioned above, for $k \equiv 4, 5 \pmod 9$ at least four cubes are required, thus we know that the correct answer is one of 4,5,6,7; and it is expected that 4 or 5 is most likely. Finally, we can relax the condition again to ask how many cubes are required in order to realize almost all integers. Davenport in 1939 [2] proved that almost all integers can in fact be written as the sum of at most 4 cubes.

Chapter 2

Rational Parametrization

As discussed in the introduction, we will bound a count of taxicab numbers by looking at non-trivial solutions to (1.3), which we'll restate here:

$$w^3 + x^3 + y^3 + z^3 = 0$$

To study solutions to this equation, we'll use the following complete rational parametrization discovered by Euler [9]. To define the parametrization, we let:

$$F(a,b,c) = 9a^3 + 9a^2b + 3a^2c + 3ab^2 - 6abc + 3ac^2 + 3b^3 + 3b^2c + bc^2 + c^3$$

For each (w,x,y,z) solution to (1.3), there exists $r \in \mathbf{Q}$ and $a,b,c \in \mathbf{Z}$ so that:

$$\begin{aligned} w &= r \cdot F(a,b,c) \\ x &= r \cdot F(-a,b,-c) \\ y &= r \cdot F(-a,-b,c) \\ z &= r \cdot F(a,-b,-c) \end{aligned}$$

Moreover, given a solution to (1.3) with $w+y$ and $x+z$ not both zero, we can find such a,b,c by letting

$$\begin{aligned} A(w,x,y,z) &= yz - wx \\ B(w,x,y,z) &= w^2 - wz + z^2 - x^2 + xy - y^2 \\ C(w,x,y,z) &= w^2 - wz + z^2 + x^2 - xy + y^2 - yz - wx + 2wy + 2xz \end{aligned} \tag{2.1}$$

and then choosing any $s \in \mathbf{Q}$ so that

$$\begin{aligned} a &= s \cdot A \\ b &= s \cdot B \\ c &= s \cdot C \end{aligned}$$

are all integers.

If $w + y = x + z = 0$ (which we consider as "trivial" solutions later) then let

$$\begin{aligned} A(w, x, y, z) &= x + y \\ B(w, x, y, z) &= y - x \\ C(w, x, y, z) &= 0 \end{aligned}$$

We will most often consider $s = 1$ and $s = \frac{1}{\gcd(A,B,C)}$.

To realize a taxicab number from a solution to (1.3) we need only place the variables w, x, y, z into pairs. While we could choose any of the three possible pairings, by denoting our taxicab number k, the following appears to possess the most symmetry when used with the parametrization:

$$k = w^3 + z^3 = (-x)^3 + (-y)^3 \tag{2.2}$$

In order to simplify the use of this parametrization, we will define the map

$$\phi(a, b, c) \mapsto (W, X, Y, Z) \tag{2.3}$$

where:

$$\begin{aligned} W &= W(a, b, c) = F(a, b, c) && (2.4) \\ X &= X(a, b, c) = F(-a, b, -c) \\ Y &= Y(a, b, c) = F(-a, -b, c) \\ Z &= Z(a, b, c) = F(a, -b, -c) \end{aligned}$$

Thus for any $a, b, c \in \mathbf{Z}$, $\phi(a, b, c) = (W, X, Y, Z)$ satisfies (1.3), e.g. $W^3 + X^3 + Y^3 + Z^3 = 0$.

Substituting these expressions for the variables w, x, y, z in (2.2), allow us to better understand the form of a taxicab number. By letting

$$\begin{aligned} U &= U(a,b,c) = 3a^2 + (b+c)^2 \\ V &= V(a,b,c) = 3a^2 + (b-c)^2 \end{aligned} \tag{2.5}$$

we have an expression for $K = W^3 + Z^3$ as:

$$K = K(a,b,c) = 18aUV[UV + 4b^2(U+V)] \tag{2.6}$$

We call a solution to (1.3) or (2.2), a *primitive* solution if $\gcd(w, x, y, z) = 1$. The following proposition, shows that every primitive solution to (2.2), up to permutation, corresponds to a positive integer triple (a, b, c) via the map ϕ. This will allow us to bound the number of taxicab numbers by bounding the number of triples (a, b, c). Except for the added condition that the integers a, b, c can be made positive, this result is also given in [4].

Proposition 2.1: *For any primitive solution to (2.2) with $k > 0$ (up to re-ordering of the variables combined with possibly multiplying through by -1 to ensure $k > 0$), there exists an integer g, and integers a, b, c with $\gcd(a, b, c) = 1$ and $a, b, c \geq 0$ with $\phi(a, b, c) = (W, X, Y, Z)$, such that*

$$W = gw \quad X = gx \quad Y = gy \quad Z = gz$$

and so:

$$K(a,b,c) = g^3 k$$

Proof. Using the A, B, C from (2.1), and $h = \gcd(A, B, C)$ we let $a = A/h$, $b = B/h$, $c = C/h$. Then let:

$$\phi(a,b,c) = (W, X, Y, Z)$$

By choosing $g = W/w$ we have found a, b, c, g so that $\gcd(a, b, c) = 1$ and W, X, Y, Z are as required by the proposition. We now must show we can choose $a, b, c \geq 0$.

Since U, V of (2.5) are positive semi-definite quadratic forms, we have $U, V \geq 0$. By (2.6) we can see that $K(a, b, c) > 0$ if and only if $a > 0$. Notice that swapping the pairs,

$k = (-x)^3 + (-y)^3 = w^3 + z^3$, or changing the order within a pair, for example $k = z^3 + w^3 = (-y)^3 + (-x)^3$, only permutes the order of the variables and does not change the basic solution to (2.2). To see that we can also choose $b, c \geq 0$, we examine how b and c change with respect to such permutations. The following maps define three other permutations:

$$\begin{aligned} \phi(a, -b, -c) &= (Z, Y, X, W) \\ \phi(a, b, -c) &= (-Y, -Z, -W, -X) \\ \phi(a, -b, c) &= (-X, -W, -Z, -Y) \end{aligned}$$

We can see from these maps that we can indeed choose $b \geq 0$ and $c \geq 0$ as well. ∎

We could prove a similar proposition for non-primitive solutions to (2.2). In this case, we would have to allow for $g \in \mathbf{Q}$. But since for our technique, we will need only to count primitive solutions and will handle non-primitive solutions by scaling primitive solutions, we won't require such a result.

Note that there are eight permutations (allowing multiplying by -1 to keep $k > 0$) of the variables which preserve a particular solution to (2.2):

w,x,y,z	z,y,x,w	-y,-z,-w,-x	-x,-w,-z,-y
w,y,x,z	z,x,y,w	-y,-w,-z,-x	-x,-z,-w,-y

The maps given in the above proposition, along with the identity map, describe the relationship between the permutations in each row. We were able to show in the above proposition that by restricting ourselves to $a > 0$, $b, c \geq 0$ we will count each row exactly once. But since all eight of these permutations represent the same solution, there are therefore two different triples a, b, c with $\gcd(a, b, c) = 1$ and $a > 0$, $b, c \geq 0$ associated with each solution.

We can also give the map which takes a solution above to the other in the same column. This map, composed with the identity and the three maps given in the previous proposition, generate the other four permutations which preserve a solution to (2.2),

$$\begin{aligned} (a, b, c) &\longrightarrow (ah_1(a^2, b^2, c^2), ch_2(a^2, b^2, c^2), bh_3(a^2, b^2, c^2)) \\ (W, X, Y, Z) &\longmapsto (W \cdot H, Y \cdot H, X \cdot H, Z \cdot H) \end{aligned}$$

where

$$\begin{aligned} h_1(t,u,v) &= (27t^2 + 18tu + 3u^2 + 18tv + 10uv + 3v^2) \\ h_2(t,u,v) &= (9t^2 + 30tu + 9u^2 + 6tv + 6uv + v^2) \\ h_3(t,u,v) &= (81t^2 + 54tu + 9u^2 + 30tv + 6uv + v^2) \end{aligned}$$

and:

$$H = H(a^2, b^2, c^2) = h_1(a^2, b^2, c^2) \cdot h_2(a^2, b^2, c^2) \cdot h_3(a^2, b^2, c^2)$$

Notice that $a, b, c \geq 0$ if and only if each of $ah_1(a^2, b^2, c^2)$, $ch_2(a^2, b^2, c^2)$, and $bh_3(a^2, b^2, c^2)$ are non-negative as well. Hence as described, for each primitive solution to (2.2) there are exactly two triples, a, b, c associated to it as described in Proposition 2.1. We will discuss the relationship between these two triples more extensively in chapter four.

Since taxicab numbers require two *distinct* representations as the sum of two cubes, we next provide a characterization of trivial solutions. A solution to (2.2) is clearly trivial, and hence does not represent a taxicab number, if as sets $\{w, z\} = \{-x, -y\}$, or equivalently if $w + x = 0$ or $w + y = 0$. We also consider trivial the case where $w + z = 0$ which corresponds to $k = 0$.

Lemma 2.2: *The trivial solutions to (2.2), $W + Z = 0$, $W + X = 0$, and $W + Y = 0$, arise exactly when a, b, or c is 0, respectively.*

Proof.

Case 1: $W + Z = 0$

We have $W + Z = 6a(3a^2 + (b - c)^2)$ so $W + Z = 0$ if and only if $a = 0$.

Case 2: $W + X = 0$

We have $W + X = 2b(3b^2 + (3a - c)^2)$ so $W + X = 0$ if and only if $b = 0$.

Case 3: $W + Y = 0$

We have $W + Y = 2c(c^2 + 3(a - b)^2)$ so $W + Y = 0$ if and only if $c = 0$. ∎

As noted in the introduction, much of the previous work on this problem has been concerned with the solutions to (2.2) with $w, z, -x, -y$ all non-negative. To that end, we may be interested in which integer triples a, b, c lead to such a solution under the parametrization. The following two propositions give necessary and sufficient conditions. The first is a necessary condition which may aid in calculating an upper bound on the count of taxicab numbers.

Proposition 2.3: *Given integers $a, b, c > 0$, and using the parametrization given above in (2.4), if $W(a,b,c), Z(a,b,c), -X(a,b,c), -Y(a,b,c)$ are all positive, then $b + c < 3a$.*

Proof. We begin with the expression for $Z(a,b,c)$ via the parametrization:

$$\begin{aligned} Z &= 9a^3 - 9a^2b - 3a^2c + 3ab^2 - 6abc + 3ac^2 - 3b^3 - 3b^2c - bc^2 - c^3 \\ &= (3a - b - c)(3a^2 + b^2 + c^2) - (6a^2b + 2b^3 + 2b^2c + 6abc) \end{aligned}$$

From this we can see that if $Z > 0$ then $3a - b - c$ must be positive since $a, b, c > 0$ and hence $b + c < 3a$. ∎

The next proposition is a sufficient condition for a relation on a, b, c for which each of $W(a,b,c), -X(a,b,c), -Y(a,b,c), Z(a,b,c)$ are positive. This will be useful while calculating our lower bound on the count of taxicab numbers.

Proposition 2.4: *Given integers $a, b, c > 0$, with $b+c < a$, then using the parametrization given above in (2.4), $W(a,b,c), Z(a,b,c), -X(a,b,c), -Y(a,b,c)$ are all positive.*

Proof. We'll show that each of $W, -X, -Y, Z$ are positive under the condition $b + c < a$, beginning with the parametrization of each:

$$\begin{aligned} W &= 9a^3 + 9a^2b + 3a^2c + 3ab^2 - 6abc + 3ac^2 + 3b^3 + 3b^2c + bc^2 + c^3 \\ &> 9a^3 + 9abc + 3a^2c + 3ab^2 - 6abc + 3ac^2 + 3b^3 + 3b^2c + bc^2 + c^3 \\ &= 9a^3 + 3abc + 3a^2c + 3ab^2 + 3ac^2 + 3b^3 + 3b^2c + bc^2 + c^3 \\ &> 0 \end{aligned}$$

$$\begin{aligned} -X &= 9a^3 - 9a^2b + 3a^2c + 3ab^2 + 6abc + 3ac^2 - 3b^3 + 3b^2c - bc^2 + c^3 \\ &> 9a^2b - 9a^2b + 3a^2c + 3b^3 + 6abc + 3bc^2 - 3b^3 + 3b^2c - bc^2 + c^3 \end{aligned}$$

$$
\begin{aligned}
&= 3a^2c + 6abc + 2bc^2 + 3b^2c + c^3 \\
&> 0
\end{aligned}
$$

$$
\begin{aligned}
-Y &= 9a^3 + 9a^2b - 3a^2c + 3ab^2 + 6abc + 3ac^2 + 3b^3 - 3b^2c + bc^2 - c^3 \\
&> 9a^2c + 9a^2b - 3a^2c + 3b^2c + 6abc + 3c^3 + 3b^3 - 3b^2c + bc^2 - c^3 \\
&= 6a^2c + 9a^2b + 6abc + 2c^3 + 3b^3 + bc^2 \\
&> 0
\end{aligned}
$$

$$
\begin{aligned}
Z &= 9a^3 - 9a^2b - 3a^2c + 3ab^2 - 6abc + 3ac^2 - 3b^3 - 3b^2c - bc^2 - c^3 \\
&= 3(a-b-c)(3a^2 + b^2 + c^2) + 2c(3a^2 + bc + c^2 - 3ab) \\
&> 3a^2 + bc + c^2 - 3ab \\
&> 3ab + bc + c^2 - 3ab \\
&= bc + c^2 \\
&> 0 \quad \blacksquare
\end{aligned}
$$

Chapter 3

Describing the gcd's

In this chapter we will describe the gcd's which arise from an arbitrary but fixed a, b, c triple. In the next chapter explore the relationship between the two different gcds coming from the two distinct a, b, c triples which yield the same solution to (2.2). Let $\phi(a, b, c) = (W, X, Y, Z)$ from (2.3), and let $g = \gcd(W, X, Y, Z)$. Although we will have to prove several lemmas before beginning the proof of the main result in this chapter, we will state it first here. Simply stated, Theorem 3.1 shows that $g \asymp \alpha\beta\gamma$, where $\alpha = \gcd(a, c^2 + 3b^2)$, $\beta = \gcd(b, c^2 + 3a^2)$, and $\gamma = \gcd(c, b^2 + 3a^2)$; and the implied constant is a product of small powers of 2 and 3. This result was proven independently in [4].

Theorem 3.1: *Suppose* $\gcd(a, b, c) = 1$. *Then we can write* $g = 2^{e_2}3^{e_3}\alpha\beta\gamma$, *where* $\alpha = \gcd(a, c^2 + 3b^2)$, $\beta = \gcd(b, c^2 + 3a^2)$, *and* $\gamma = \gcd(c, b^2 + 3a^2)$. *Further, if 2 exactly divides* abc *then* $e_2 = 2$, *if 4 divides one of* a, b *or* c *and the other two are odd then* $e_2 = 1$, *otherwise* $e_2 = 0$. *If* $3 \mid c$ *but* $3 \nmid ab$ *then* $e_3 = 1$, *otherwise* $e_3 = 0$. *Moreover, if a prime* p *divides* $\gcd(\alpha, \beta) \cdot \gcd(\alpha, \gamma) \cdot \gcd(\beta, \gamma)$, *then* $p = 2, 3$.

In order to prove this result, we'll begin with some preliminary lemmas.

Lemma 3.2: *If a prime* $p \neq 2, 3$ *divides* $\gcd(W, X, Y, Z)$, *and* p *divides* $\gcd(a, b) \cdot \gcd(a, c) \cdot \gcd(b, c)$, *then* p *divides* $\gcd(a, b, c)$.

Proof. Suppose $p \mid \gcd(a, b)$. Since $p \mid \gcd(W, X, Y, Z)$, we must have $p \mid W + Y$. But:

$$W + Y \equiv 2c^3 \pmod p$$

Hence $p \mid \gcd(a, b, c)$. A similar argument works for the other two gcd's: if $p \mid \gcd(a, c)$ we notice that $W + X \equiv 6b^3 \pmod p$, and if $p \mid \gcd(b, c)$ we notice that $W + Z \equiv 18a^3 \pmod p$. ∎

Next note for a prime $p \neq 3$ that $p^e \mid (W+Z)$ and $p^{2e} \mid (W^2 - WZ + Z^2)$ if and only if $p^e \mid W$ and $p^e \mid Z$. Using the parametrization from chapter two, we also have that:

$$\begin{aligned} W + Z &= 6a(3a^2 + (b-c)^2) \\ X + Y &= 6a(3a^2 + (b+c)^2) \end{aligned}$$

This next lemma proves that the primes that we are interested in (i.e. those dividing $\gcd(W, X, Y, Z)$), can not divide both of the non-trivial factors in either $W + Z$ or $X + Y$ given above.

Lemma 3.3: *Let $p \neq 2, 3$ be a prime dividing $\gcd(W, X, Y, Z)$. If $\gcd(a, b, c) = 1$ then p does not divide either $\gcd(a, 3a^2 + (b-c)^2)$ or $\gcd(a, 3a^2 + (b+c)^2)$.*

Proof. Suppose $p \mid \gcd(a, 3a^2 + (b-c)^2)$. By hypothesis, p must divide $W^2 - WZ + Z^2$, but:

$$W^2 - WZ + Z^2 \equiv 12b^2(3a^2 + (b+c)^2)^2 \pmod p$$

Since by Lemma 3.2, p can not divide both a and b, we must have that p divides $3a^2+(b+c)^2$. But we assumed p divides $3a^2 + (b-c)^2$, hence it must divide their difference $(3a^2 + (b + c)^2) - (3a^2 + (b-c)^2) = 4bc$, which also yields a contradiction to Lemma 3.2.

To get the second gcd condition, use the pair X, Y rather than W, Z with the same argument. ∎

Proposition 3.4: *Suppose that a, b, c are integers such that $\gcd(a, b, c) = 1$. Let $p \neq 2, 3$ be a prime. If $p^e \mid \gcd(W, X, Y, Z)$, then p^e divides one of:*

$$\begin{aligned} &i) && \gcd(a, c^2 + 3b^2) \\ &ii) && \gcd(b, c^2 + 3a^2) \\ &iii) && \gcd(c, b^2 + 3a^2) \end{aligned}$$

Proof. Since $p^e \mid \gcd(W, X, Y, Z)$, then p^e divides both:

$$\begin{aligned} W + Z &= 6a(3a^2 + (b-c)^2) \\ X + Y &= 6a(3a^2 + (b+c)^2) \end{aligned}$$

By Lemma 3.3 p can not divide both a and $3a^2+(b-c)^2$ nor can p divide both a and $3a^2+(b+c)^2$. So, if p^e does not divide a, then p^e must divide both $3a^2+(b+c)^2$ and $3a^2+(b-c)^2$ and hence their difference, namely $4bc$. Since p does not divide $\gcd(b,c)$ by Lemma 3.2, either $p^e \mid b$ or $p^e \mid c$.

Case 1: $p^e \mid a$.

Note that p^{2e} divides both W^2-WZ+Z^2 and X^2-XY+Y^2. Examining these modulo p^{2e} we have:

$$\begin{aligned} W^2-WZ+Z^2 &\equiv 3(b+c)^2(c^2+3b^2)^2 \pmod{p^{2e}} \\ X^2-XY+Y^2 &\equiv 3(b-c)^2(c^2+3b^2)^2 \pmod{p^{2e}} \end{aligned}$$

Hence p^e divides (c^2+3b^2), since if it does not, p must divide both $(b+c)$ and $(b-c)$, hence both b and c, which contradicts Lemma 3.2. So this gives condition i).

Case 2: $p^e \mid b$.

We'll use the same argument here noticing that this time:

$$\begin{aligned} W^2-WZ+Z^2 &\equiv 3(c^2+3a^2)^3 \pmod{p^{2e}} \\ X^2-XY+Y^2 &\equiv 3(c^2+3a^2)^3 \pmod{p^{2e}} \end{aligned}$$

Hence p^{2e} divides $(3a^2+c^2)$, giving condition ii).

Case 3: $p^e \mid c$. Again the same argument applies, noticing this time

$$\begin{aligned} W^2-WZ+Z^2 &\equiv 6a(b^2+3a^2)^3 \pmod{p^{2e}} \\ X^2-XY+Y^2 &\equiv 9(a^2+3b^2)(b^2+3a^2)^3 \pmod{p^{2e}} \end{aligned}$$

Hence p^e divides $(3a^2+b^2)$, since if it does not, we would have p dividing a which is a contradiction to Lemma 3.2. So this gives condition iii). ∎

At this point, we have characterized the gcd's up to some powers of 2 and 3. These powers are described by the following lemmas.

Lemma 3.5: *Let* $g=\gcd(W,X,Y,Z)$. *If* $\gcd(a,b,c)=1$ *then the only powers of 2 which can divide* g *are* $2^0=1$ *and* $2^3=8$. *Moreover 8 divides* g *if and only if 2 divides* $a+b+c$.

Proof. If we consider a, b, c modulo 16 we see that under the map ϕ (modulo 16), when $2 \nmid \gcd(a,b,c)$ then either $g \equiv 1 \pmod 2$ or $g \equiv 8 \pmod{16}$. Looking modulo 2 we have:

$$W \equiv X \equiv Y \equiv Z \equiv (a+b+c) \pmod 2 \quad \blacksquare$$

Lemma 3.6: *Let* $g = \gcd(W, X, Y, Z)$. *If* $\gcd(a,b,c) = 1$ *then the only powers of 3 which can divide* g *are* $3^0 = 1$, $3^1 = 3$, *and* $3^2 = 9$. *Moreover, 3 divides* g *if and only if 3 divides* c, *and 9 divides* g *if and only if 3 divides both* c *and* b.

Proof. If we consider a, b, c modulo 27 we see that under the map ϕ (modulo 27), that if $3 \nmid \gcd(a,b,c)$ then $g \not\equiv 0 \pmod{27}$. Next we look modulo 3:

$$\begin{aligned}
W &\equiv c^2(b+c) \pmod 3 \\
X &\equiv c^2(b+2c) \pmod 3 \\
Y &\equiv c^2(2b+c) \pmod 3 \\
Z &\equiv 2c^2(b+c) \pmod 3
\end{aligned}$$

So, 3 divides g if and only if 3 divides c, since if 3 doesn't divide c it must divide both $b+c$ and $2b+c$ and hence their sum, which would imply that 3 does divide c. So, to understand when higher powers of 3 divide g, we'll suppose that 3 divides c and look modulo 9:

$$\begin{aligned}
W &\equiv 3b^2(a+b) \pmod 9 \\
X &\equiv 3b^2(2a+b) \pmod 9 \\
Y &\equiv 6b^2(a+b) \pmod 9 \\
Z &\equiv 3b^2(a+2b) \pmod 9
\end{aligned}$$

Like the case for modulo 3, we have that 9 divides g if and only if 3 divides $\gcd(b,c)$. $\blacksquare$

We now can prove the result mentioned at the start of this chapter, namely:

Theorem 3.1: *Suppose* $\gcd(a,b,c) = 1$. *Then we can write* $g = 2^{e_2}3^{e_3}\alpha\beta\gamma$, *where* $\alpha = \gcd(a, c^2+3b^2)$, $\beta = \gcd(b, c^2+3a^2)$, *and* $\gamma = \gcd(c, b^2+3a^2)$. *Further, if 2 exactly divides* abc *then* $e_2 = 2$, *if 4 divides one of* a, b *or* c *and the other two are odd then* $e_2 = 1$, *otherwise*

$e_2 = 0$. *If* $3 \mid c$ *but* $3 \nmid ab$ *then* $e_3 = 1$, *otherwise* $e_3 = 0$. *Moreover, if a prime* p *divides* $\gcd(\alpha, \beta) \cdot \gcd(\alpha, \gamma) \cdot \gcd(\beta, \gamma)$, *then* $p = 2, 3$.

Proof. Let $p > 5$ be a prime. Then if p divides two of the factors α, β, γ then it divides two of a, b, c. But by the form of α, β, and γ, p must therefore divide all three of a, b, c. Since $\gcd(a, b, c) = 1$ indeed the last statement of the theorem is satisfied. The rest of the proof follows directly from Lemma 3.2 and Proposition 3.4, except for the values of e_2 and e_3.

For e_2, notice that since $\gcd(a, b, c) = 1$:

$$2 \mid \alpha \quad \text{iff} \quad 2 \mid a \text{ and } 2 \nmid bc$$

$$2 \mid \beta \quad \text{iff} \quad 2 \mid b \text{ and } 2 \nmid ac$$

$$2 \mid \gamma \quad \text{iff} \quad 2 \mid c \text{ and } 2 \nmid ab$$

Therefore if 2 divides two of a, b, c or none of a, b, c, then 2 does not divide $\alpha\beta\gamma$ and in this case by Lemma 3.5, 2 does not divide g, so $e_2 = 0$. So suppose now that 2 divides only one of a, b, c. Without loss of generality, suppose 2 divides a but $2 \nmid bc$. If 2 exactly divides a, then 2 exactly divides $\alpha\beta\gamma$ but 8 exactly divides g by Lemma 3.5, hence $e_2 = 2$. Finally, if 4 divides a, then 4 exactly divides $\alpha\beta\gamma$ (since 4 also exactly divides $c^2 + 3b^2$ and hence α), and by Lemma 3.5, 8 exactly divides g, so $e_2 = 1$.

For e_3, notice that since $\gcd(a, b, c) = 1$

$$3 \parallel \alpha \quad \text{iff} \quad 3 \mid \gcd(a, c)$$

$$3 \parallel \beta \quad \text{iff} \quad 3 \mid \gcd(b, c)$$

$$3 \parallel \gamma \quad \text{iff} \quad 3 \mid \gcd(b, c)$$

since no higher powers of 3 can divide any one of α, β, or γ. So, if

$3 \nmid abc$, or

$3 \mid a$ but $3 \nmid bc$, or

$3 \mid b$ but $3 \nmid ac$, or

$3 \mid \gcd(a, b)$ but $3 \nmid c$

then 3 does not divide $\alpha\beta\gamma$. By Lemma 3.6, 3 does not divide g hence $e_3 = 0$.

If 3 does not divide b, but 3 divides both a and c then 3 exactly divides $\alpha\beta\gamma$ and by Lemma 3.6, 3 exactly divides g, so again $e_3 = 0$.

If 3 does not divide a, but 3 divides both b and c, then 3 exactly divides both β and γ, and hence 9 exactly divides $\alpha\beta\gamma$. By Lemma 3.6, 9 exactly divides g, so again $e_3 = 0$.

Finally, if 3 divides c but 3 does not divide ab, then 3 does not divide $\alpha\beta\gamma$, but by Lemma 3.6, 3 exactly divides g, so we must have $e_3 = 1$. ∎

We can deduce the following Corollary also given in [4].

Corollary 3.7: *Let* $p > 3$ *be a prime dividing* $\gcd(W, X, Y, Z)$*, then* $p \equiv 1, 7 \pmod{12}$.

Proof. From Proposition 3.4 we have that p divides one of $\gcd(a, c^2+3b^2)$, $\gcd(b^2, c^2+3a^2)$, and $\gcd(c^2, b^2+3a^2)$, and by Lemma 3.2, p does not divide $\gcd(a, b)\gcd(b, c)\gcd(a, c)$. Hence -3 must be a quadratic residue modulo p. So indeed $p \equiv 1, 7 \pmod{12}$. ∎

Chapter 4

Comparing gcd's From The Two (a,b,c)

In chapter two, after the proof of Proposition 2.1 we showed that for each primitive solution to (2.2) there there are exactly two (a, b, c) integer triples associated to this solution with $a, b, c > 0$ and $\gcd(a, b, c) = 1$, which account for all permutations of w, x, y, z in (2.2) preserving k. In this chapter, we will compare the gcds which arise from these two (a, b, c) triples. We recall some definitions from chapter two and add a few more.

We begin with the following map, which has most of the features we would like; and then show how to modify it slightly to preserve the coprimality of the a, b, c triples.

Given a triple (a, b, c) where $\gcd(a, b, c) = 1$, we have the following map to the other triple (A, B, C) which yields the same primitive solution:

$$\psi'(a, b, c) = (A, B, C) \tag{4.1}$$

so that

$$A = a \cdot h_1(a^2, b^2, c^2)$$

$$B = c \cdot h_2(a^2, b^2, c^2)$$

$$C = b \cdot h_3(a^2, b^2, c^2)$$

where:

$$\begin{aligned}
h_1(t, u, v) &= 27t^2 + 18tu + 3u^2 + 18tv + 10uv + 3v^2 \\
h_2(t, u, v) &= 9t^2 + 30tu + 9u^2 + 6tv + 6uv + v^2 \\
h_3(t, u, v) &= 81t^2 + 54tu + 9u^2 + 30tv + 6uv + v^2
\end{aligned}$$

Using the map ϕ from (2.3) let:

$$\phi(a,b,c) = (w,x,y,z)$$

Then

$$\phi(A,B,C) = (W,X,Y,Z) = (wH, yH, xH, zH)$$

where:

$$H = H(a^2,b^2,c^2) = h_1(a^2,b^2,c^2)h_2(a^2,b^2,c^2)h_3(a^2,b^2,c^2) \tag{4.2}$$

Since a major concern is with the gcd's of our solutions, we note that if we let $g = \gcd(w,x,y,z)$ then:

$$G = \gcd(W,X,Y,Z) = gH \tag{4.3}$$

Notice that the (A,B,C) from this map are not necessarily coprime even if the original (a,b,c) were. It turns out in fact that $\gcd(A,B,C) = 2^{e_1}3^{e_2}g^2$, that is, except for some powers of the primes 2 and 3, which we will describe explicitly, the $\gcd(A,B,C)$ is just g^2. We will prove this beginning with the following proposition.

Proposition 4.1: *Given a,b,c with $\gcd(a,b,c) = 1$, using the map ψ' defined above by (4.1), and letting $D = \gcd(A,B,C)$ and $g = \gcd(w,x,y,z)$, then for any prime p not equal to 2 or 3, $p \mid D$ iff $p \mid g$. Moreover:*

$$p^{2e} \parallel D \quad \text{iff} \quad p^e \parallel g$$

Proof. Throughout this proof we let p denote a prime not equal to 2 or 3. First note that if $p \mid a$ and $p \mid b$ then $p \nmid c$, and further $p \nmid h_2(a^2,b^2,c^2)$. The first since $\gcd(a,b,c) = 1$, while the second follows by noting that $h_2(a^2,b^2,c^2) \equiv c^3 \pmod{p}$ for such a prime p. This then tells us that $p \nmid D$, since $B = c \cdot h_2(a^2,b^2,c^2)$. Recall from Theorem 3.1 that $g = 2^{e_2}3^{e_3}\alpha\beta\gamma$ where $\alpha = \gcd(a, c^2+3b^2)$, $\beta = \gcd(b, c^2+3a^2)$, and $\gamma = \gcd(c, b^2+3a^2)$. Therefore such a p also does not divide g.

We also can show that $p \nmid abc$ implies $p \nmid D$. We'll show this by contradiction, suppose that $p \nmid abc$ but $p \mid D$. Then p must divide each of $h_1(a^2,b^2,c^2)$, $h_2(a^2,b^2,c^2)$, and $h_3(a^2,b^2,c^2)$.

So then p must divide both:

$$\begin{aligned} 3h_1 - h_3 &= 8c^2(3a^2 + 3b^2 + c^2) \\ 3h_2 - h_1 &= 8b^2(9a^2 + 3b^2 + c^2) \end{aligned}$$

Since p does not divide b, c or 2, then p must divide both

$$3a^2 + 3b^2 + c^2$$
$$9a^2 + 3b^2 + c^2$$

and hence their difference $6a^2$. But since p does not divide 2,3 or a this is a contradiction. Moreover such a p also can not divide g which is a product of α, β, and γ as described above. Thus the only primes p which can divide D or g must divide exactly one of a, b, or c.

Suppose that $p \mid a$, $p \nmid bc$, and $p \mid D$, then p must divide both $h_2(a^2, b^2, c^2)$ and $h_3(a^2, b^2, c^2)$. But,

$$\begin{aligned} h_2(a^2, b^2, c^2) &\equiv (c^2 + 3b^2)^2 \pmod{p} \\ h_3(a^2, b^2, c^2) &\equiv (c^2 + 3b^2)^2 \pmod{p} \end{aligned}$$

so p must divide $c^2 + 3b^2$.

Note also that if $p \mid a$, $p \nmid bc$, and $p \mid g$, then p must divide $\alpha = \gcd(a, c^2 + 3b^2)$, and hence p must divide $3b^2 + c^2$. The cases for $p \mid b$ and $p \mid c$ work similarly, so we know that indeed $p \mid g$ if and only if $p \mid D$. We now must show that the exponents are as stated in the proposition.

We continue by describing the powers of p which divide each of A, B, and C. Let $p^{e_1} \parallel a$ and $p^{e_2} \parallel 3b^2 + c^2$, where $e_1, e_2 \geq 1$.

We begin with A. Since $A = a \cdot h_1(a^2, b^2, c^2)$ we need to know what power of p divides h_1. We can rewrite h_1 as:

$$h_1(a^2, b^2, c^2) = (c^2 + 3b^2)(b^2 + 3c^2) + 27a^4 + 18a^2(b^2 + c^2)$$

Since $p \mid c^2+3b^2$ but $p \nmid b$ and $p \nmid c$, then $p \nmid b^2+3c^2$ and $p \nmid b^2+c^2$. So:

$$\begin{aligned} p^{e_2} &\quad \| \quad (c^2+3b^2)(3c^2+b^2) \\ p^{2e_1} &\quad \| \quad 27a^4+18a^2(b^2+c^2) \end{aligned}$$

Therefore if $e_2 \neq 2e_1$ then $p^{\min(e_2,2e_1)} \parallel h_1(a^2,b^2,c^2)$.

If $e_2 = 2e_1$ then $p^{\min(e_2,2e_1)} \mid h_1(a^2,b^2,c^2)$, but it's possible that a higher power of p divides h_1.

Therefore, if $e_2 \neq 2e_1$ then $p^{e_1+\min(e_2,2e_1)} \parallel A$, and if $e_2 = 2e_1$ then $p^{e_1+\min(e_2,2e_1)} \mid A$.

We move on to B. Since $B = c \cdot h_2(a^2,b^2,c^2)$, and we know that $p \nmid c$, we need only be concerned with the power of p dividing h_2. We begin by rewriting h_2 as:

$$h_2(a^2,b^2,c^2) = (3b^2+c^2)^2 + 9a^4 + 6a^2(5b^2+c^2)$$

Since $p \mid 3b^2+c^2$ but $p \nmid b$ and $p \nmid c$, then $p \nmid 5b^2+c^2$. So:

$$\begin{aligned} p^{2e_2} &\quad \| \quad (3b^2+c^2)^2 \\ p^{2e_1} &\quad \| \quad 9a^4+6a^2(5b^2+c^2) \end{aligned}$$

Therefore if $e_1 \neq e_2$ then $p^{2\min(e_1,e_2)} \parallel B$, and if $e_2 = e_1$ then $p^{2\min(e_1,e_2)} \mid B$.

Now for C. The argument for C is just like the one above for B, noting that $B = c \cdot h_3(a^2,b^2,c^2)$, and rewriting h_3 as:

$$h_3(a^2,b^2,c^2) = (3b^2+c^2)^2 + 81a^4 + 6a^2(9b^2+5c^2)$$

It then follows that if $e_1 \neq e_2$ then $p^{2\min(e_1,e_2)} \parallel C$, and if $e_2 = e_1$ then $p^{2\min(e_1,e_2)} \mid C$.

To now calculate what power of p divides D and g we will split into three cases. Note that in calculating the power of p dividing g, recall that we are considering the case $p \mid a$, $p \nmid bc$, and so the power of p dividing g is exactly the power of p dividing $\alpha = \gcd(a, 3b^2+c^2)$. So in all of the cases below, $p^{\min(e_1,e_2)} \parallel g$.

<u>Case 1:</u> $e_2 < e_1$

In this case, we have, $p^{e_1+e_2} \parallel A$, $p^{2e_2} \parallel B, C$. So, $p^{2e_2} \parallel D$.

The power of p dividing g, is $p^{e_2} \parallel g$.

<u>Case 2:</u> $e_2 = e_1$

In this case, we have $p^{e_1+e_2} = p^{2e_1} \parallel A$, $p^{2e_1} \mid B, C$. So, $p^{2e_1} \parallel D$.

The power of p dividing g is $p^{e_1} \parallel g$.

<u>Case 3:</u> $e_1 < e_2$

In this case, $p^{2e_1} \parallel B, C$. There are three possible cases for the power of p dividing A. If $e_1 < e_2 < 2e_1$ then $p^{e_1+e_2} \parallel A$. If $e_2 = 2e_1$ then $p^{3e_1} \mid A$. If $e_2 > 2e_1$ then $p^{3e_1} \parallel A$. But in all three of these possibilities, the power of p dividing A is larger than the power dividing B and C, and hence $p^{2e_1} \parallel D$.

The power of p dividing g is $p^{e_1} \parallel g$.

In all three cases, we notice for a prime $p \neq 2, 3$, where $p \mid a$ that indeed $p^{2e} \parallel D$ if and only if $p^e \parallel g$. The cases for $p \neq 2, 3$ where $p \mid b$ or $p \mid c$ follow from a similar argument. ∎

We next describe how the primes 2 and 3 divide D, beginning with the prime 2.

Lemma 4.2: *Given a, b, c with $\gcd(a, b, c) = 1$, let $(A, B, C) = \psi'(a, b, c)$ and let $D = \gcd(A, B, C)$, then $2 \mid D$ if and only if $a + b + c \equiv 0 \pmod 2$. Moreover, if $a + b + c \equiv 0 \pmod 2$ then $2^4 \parallel D$.*

Proof. By looking at A, B, and C modulo 2 we see:

$$\begin{aligned} A &\equiv a(a^4 + b^4 + c^4) \pmod 2 \\ B &\equiv c(a^4 + b^4 + c^4) \pmod 2 \\ C &\equiv b(a^4 + b^4 + c^4) \pmod 2 \end{aligned}$$

Since $\gcd(a, b, c) = 1$, we then have that $2 \mid D$ if and only if $a + b + c \equiv 0 \pmod 2$.

Note that $a + b + c \equiv 0 \pmod 2$ implies that 2 divides exactly one of a, b, c since $\gcd(a, b, c) = 1$. We'll now show that if 2 divides exactly one of a, b, c then 2^4 exactly divides each of $h_1(a^2, b^2, c^2)$, $h_2(a^2, b^2, c^2)$, and $h_3(a^2, b^2, c^2)$.

We begin with h_1. First suppose that $2 \mid a$ and $2 \nmid bc$. We begin by rewriting h_1 as:

$$h_1(a^2, b^2, c^2) = (3b^2 + c^2)(3c^2 + b^2) + 27a^4 + 18a^2(b^2 + c^2)$$

<u>Case 1:</u> $2 \parallel a$

First note that $3b^2 + c^2 \equiv 4 \pmod 8$ and $3c^2 + b^2 \equiv 4 \pmod 8$, and that $b^2 + c^2 \equiv 2 \pmod 4$. Therefore,

$$\begin{aligned} 2^4 &\parallel (3b^2 + c^2)(3c^2 + b^2) \\ 2^4 &\parallel 27a^4 \\ 2^4 &\parallel 18a^2(b^2 + c^2) \end{aligned}$$

and so $2^4 \parallel h_1(a^2, b^2, c^2)$.

<u>Case 2:</u> $2^2 \mid a$

As in Case 1, we have $2^4 \parallel (3b^2 + c^2)(3c^2 + b^2)$, but now $2^5 \mid 27a^4 + 18a^2(b^2 + c^2)$, so $2^4 \parallel h_1(a^2, b^2, c^2)$.

Similarly, $2^4 \parallel h_1(a^2, b^2, c^2)$ in the cases $2 \mid b$, $2 \nmid ac$ and $2 \mid c$, $2 \nmid ab$ using the following two rearrangements of h_1 respectively:

$$\begin{aligned} h_1(a^2, b^2, c^2) &= 3(c^2 + 3a^2)^2 + 3b^4 + 2b^2(9a^2 + 5c^2) \\ h_1(a^2, b^2, c^2) &= 3(b^2 + 3a^2)^2 + 3c^4 + 2c^2(5b^2 + 9a^2) \end{aligned}$$

We use a similar argument for $h_2(a^2, b^2, c^2)$ and $h_3(a^2, b^2, c^2)$. ∎

Lemma 4.3: *Given* a, b, c *with* $\gcd(a, b, c) = 1$, *let* $(A, B, C) = \psi'(a, b, c)$ *and let* $D = \gcd(A, B, C)$, *then* $3 \mid D$ *if and only if* $3 \mid c$, $9 \parallel D$ *if and only if* $3 \mid \gcd(a, c)$, *and* $27 \parallel D$ *if and only if* $3 \mid \gcd(b, c)$.

Proof. We begin by looking at A, B, C modulo 3:

$$\begin{aligned} A &\equiv 10ab^2c^2 \pmod 3 \\ B &\equiv c^5 \pmod 3 \\ C &\equiv bc^4 \pmod 3 \end{aligned}$$

Hence $3 \mid D$ if and only if $3 \mid c$.

Now suppose that $3 \mid c$ and look modulo 9:

$$\begin{aligned} A &\equiv 3ab^4 \pmod 9 \\ B &\equiv 0 \pmod 9 \\ C &\equiv 0 \pmod 9 \end{aligned}$$

So we see that if $3 \mid c$ but $3 \nmid ab$ then $3 \parallel D$.

Now suppose that $3 \mid c$ and look modulo 27:

$$\begin{aligned} A &\equiv ab^2(3b^2 + 10c^2 + 18a^2) \pmod{27} \\ B &\equiv 3c(b^2 + 3a^2)(a^2 + 3b^2) \pmod{27} \\ C &\equiv 9b^5 \pmod{27} \end{aligned}$$

From this we can see that if $3 \mid \gcd(a, c)$ (and $3 \nmid b$), then $A \equiv 0, 9, 18 \pmod{27}$, $B \equiv 0 \pmod{27}$ and $C \equiv 9, 18 \pmod{27}$, so $9 \parallel D$.

Moreover, if $3 \mid \gcd(b, c)$ (and $3 \nmid a$), then $A, B, C \equiv 0 \pmod{27}$. By noting that if $3 \mid \gcd(b, c)$, then $A \equiv 27a^5 \pmod{81}$ we see that $27 \parallel D$. ∎

We can now describe the two coprime (a, b, c) triples corresponding to each non-trivial solution to (2.2). Let:

$$D = \gcd(ah_1(a^2, b^2, c^2), ch_2(a^2, b^2, c^2), bh_3(a^2, b^2, c^2))$$

Then we'll define a map ψ as

$$\psi(a, b, c) = (a', b', c') = \left(\frac{A}{D}, \frac{B}{D}, \frac{C}{D}\right) \tag{4.4}$$

where A, B, C come from (4.1). So if we let

$$\begin{aligned} \phi(a, b, c) &= (W, X, Y, Z) \\ \phi(a', b', c') &= (W', X', Y', Z') \end{aligned}$$

then

$$\begin{aligned} (W, X, Y, Z) &= (gw, gx, gy, gz) \\ (W', X', Y', Z') &= (g'w, g'y, g'x, g'z) \end{aligned}$$

where (w, x, y, z) is a primitive solution to (2.2), e.g. $\gcd(w, x, y, z) = 1$. Now we can compare the sizes of these two gcds, g and g'. Notice from (4.3) that

$$g' = \frac{gH}{D^3} \asymp \frac{gH}{g^6} = \frac{H}{g^5}$$

where H is from (4.2). By letting $m = \max(a, b, c)$ we use (4.2) to see that in fact:

$$g' \asymp \frac{m^{12}}{g^5} \tag{4.5}$$

What we prove next is a bound on the size of the minimum of these two gcds. First we'll recall from (2.5) and (2.6) that

$$\begin{aligned} U &= 3a^2 + (b+c)^2 \\ V &= 3a^2 + (b-c)^2 \end{aligned}$$

and:

$$K = 18aUV(UV + 4b^2(U+V))$$

Proposition 4.4: *Suppose a, b, c and a', b', c' are the two coprime triples associated with a primitive solution to (2.2). Suppose further that $w, -x, -y, z > 0$. Then using the map ϕ from (2.3) let:*

$$\begin{aligned} \phi(a, b, c) &= (W, X, Y, Z) \\ \phi(a', b', c') &= (W', X', Y', Z') \end{aligned}$$

Letting $g = \gcd(W, X, Y, Z)$ and $g' = \gcd(W', X', Y', Z')$, then

$$\begin{aligned} W^3 + Z^3 &= g^3 k \\ W'^3 + Z'^3 &= g'^3 k \end{aligned}$$

and $\min(g, g') \ll k^{2/3}$.

Proof. From Proposition 2.3 we know that if $W, -X, -Y, Z > 0$ then $b + c < 3a$, so certainly $b, c < 3a$. But if $b, c < 3a$ then $U \asymp a^2$ and $V \asymp a^2$ so $K \asymp a^9$. Therefore $K = g^3k$

implies $a \asymp g^{1/3}k^{1/9}$. As before, let $m = \max(a, b, c)$ and so $m \asymp g^{1/3}k^{1/9}$. Thus from (4.5):

$$g' \asymp \frac{g^4 k^{4/3}}{g^5} = \frac{k^{4/3}}{g}$$

So indeed if $g \gg k^{2/3}$ then $g' \ll k^{2/3}$. ∎

The general case allowing some of the integers $w, -x, -y, z$ to be negative remains as yet unproven.

Chapter 5

Counting Primitive Solutions

In order to bound the number of taxicab numbers, we'll bound the number of non-trivial solutions to (2.2). We begin by bounding the number of primitive solutions, those for which $\gcd(w, x, y, z) = 1$, and use this to bound the total number of solutions. In chapter two we showed that we can use the parametrization given by (2.3) and we need only to consider $a, b, c > 0$ where $\gcd(a, b, c) = 1$. Thus to bound the number of primitive solutions to (2.2), we'll count the following:

$$\frac{1}{2}\sum_{g\geq 1} \# \left\{ a, b, c \in \mathbf{Z}_{>0} : \begin{array}{c} \gcd(a,b,c) = 1; \quad K \leq g^3 N; \\ \gcd(W, X, Y, Z) = g \end{array} \right\}$$

where K is from (2.6) and W, X, Y, Z from (2.4). The 1/2 at the beginning of this expression is to account for the fact that there are two a, b, c triples for each solution to (2.2).

For the rest of this chapter, we'll bound the first term in this sum, that is the term $g = 1$. Note that in this case, the result of the parametrization is a primitive solution, i.e. letting $\phi(a, b, c) = (W, X, Y, Z)$, then $\gcd(W, X, Y, Z) = 1$. We hope to be able to use this as a model to generalize for the rest of the terms in the sum using what we have proven about the gcd's which arise from this parametrization in the previous chapters. While in this chapter we give an argument for the upper bound on this term, the ideas used are similar to those for the lower bound given in the next chapter. Note that by Proposition 2.3, if we are interested in solutions to (2.2) where $w, z, -x, -y$ are all non-negative, i.e. the taxicab numbers originally considered by Ramanujan, then we need to only consider case 1 in the proof that follows.

Proposition 5.1: *Using the notation in (2.3):*

$$\# \left\{ (a, b, c) : \begin{array}{c} a, b, c > 0, \quad \gcd(a,b,c) = 1, \quad (W, X, Y, Z) = \phi(a, b, c) \\ \gcd(W, X, Y, Z) = 1, \quad 0 < W^3 + Z^3 = K \leq N \end{array} \right\} \ll N^{1/3}$$

Proof. Recall from (2.6) that letting

$$\begin{aligned} U &= 3a^2 + (b+c)^2 \\ V &= 3a^2 + (b-c)^2 \end{aligned}$$

we have:

$$K = 18aUV(UV + 4b^2(U+V))$$

<u>**Case 1:**</u> $b, c < a$.

In this case, $U \asymp a^2$ and $V \asymp a^2$, so $K \asymp a^9$. Since for each choice of a there are at most a choices for each of b and c, we have:

$$\#\{(a,b,c)\ \ b,c < a : \gcd(W,X,Y,Z) = 1 \text{ and } 0 < W^3 + Z^3 = K \leq N\}$$

$$\ll \sum_{a<N^{1/9}} a^2 \ll N^{1/3}$$

<u>**Case 2:**</u> $b \leq a \leq c$ (and $c \leq a \leq b$).

If $c < 2a$ say, then $U \asymp c^2$ and $V \asymp a^2$, but since $a \asymp c$ we also have $V \asymp c^2$. and if $c > 2a$, then $U \asymp c^2$ and $V \asymp c^2$ so no matter the size of c we have $K \asymp ac^8$. Since for a fixed a there are at most a choices for b, we have:

$$\#\{(a,b,c)\ \ b < a < c : \gcd(W,X,Y,Z) = 1 \text{ and } 0 < W^3 + Z^3 = K \leq N\}$$

$$\begin{aligned} &\ll \sum_{a<N^{1/9}} \sum_{c<\left(\frac{N}{a}\right)^{1/8}} a \\ &\ll N^{1/8} \sum_{a<N^{1/9}} a^{7/8} \ll N^{1/3} \end{aligned}$$

Note that for the other situation, in parenthesis, we can use the same argument but then $V \asymp b^2$ and $U \asymp b^2$ and hence $k \asymp ab^8$, which gives us the same count.

Case 3: $a < b < c$ where $c - b < a$ (and $a < c < b$ where $b - c < a$).

Here we have $V \asymp a^2$ and $U \asymp c^2$, so $K \asymp a^3c^4b^2 \asymp a^3b^6 \gg a^9$. Since $c - b < a$, for each choice of a and b we have at most a choices for c; so:

$$\#\{(a, b, c) \text{ in Case 3 } : \gcd(W, X, Y, Z) = 1 \text{ and } 0 < W^3 + Z^3 = K \leq N\}$$

$$\begin{aligned} &\ll \sum_{a<N^{1/9}} \sum_{b<\left(\frac{N}{a^3}\right)^{1/6}} a \\ &\ll N^{1/6} \sum_{a<N^{1/9}} a^{1/2} \ll N^{1/3} \end{aligned}$$

For the other situation, in parenthesis, we repeat the argument noting that we get $U \asymp b^2$ and $V \asymp a^2$, and so $K \asymp a^3b^6$, from which we get the same count.

Case 4: $a < b < c$ where $c - b \geq a$ (and $a < c < b$ where $b - c \geq a$).

In this case, $V \asymp (c - b)^2$ and $U \asymp c^2$, and so:

$$\begin{aligned} K &\asymp ac^2(c-b)^2[c^2(c-b)^2 + 4b^2c^2] \\ &\asymp ac^4(c-b)^2[(c-b)^2 + 4b^2] \\ &\asymp ac^6(c-b)^2 \gg a(c-b)^8 \gg a^9 \end{aligned}$$

We can then bound a by $N^{1/9}$ as usual, and since $(c - b) > a$, we can then bound c by $\left(\frac{N}{a^3}\right)^{1/6}$, i.e. so $K \asymp ac^6(c - b)^2 \gg a^3c^6$. after choosing an a and c, we then have restricted b to the range $c - \left(\frac{N}{ac^6}\right)^{1/2} < b < c - a$. Note that for small c, namely $c < \left(\frac{N}{a}\right)^{1/8}$, this lower bound for b is negative, while we have restricted b to positive numbers. So we must count as follows:

$$\#\{(a, b, c) \text{ in Case 4 } : \gcd(W, X, Y, Z) = 1 \text{ and } 0 < W^3 + Z^3 = K \leq N\}$$

$$\begin{aligned} &\ll \sum_{a<N^{1/9}} \left(\sum_{c<\left(\frac{N}{a}\right)^{1/8}} \sum_{b<c} 1 + \sum_{c=\left(\frac{N}{a}\right)^{1/8}}^{\left(\frac{N}{a^3}\right)^{1/6}} \sum_{b=c-\left(\frac{N}{ac^6}\right)^{1/2}}^{c} 1 \right) \\ &\ll \sum_{a<N^{1/9}} \left(\sum_{c<\left(\frac{N}{a}\right)^{1/8}} c + \sum_{c=\left(\frac{N}{a}\right)^{1/8}}^{\left(\frac{N}{a^3}\right)^{1/6}} \left(\frac{N}{ac^6}\right)^{1/2} \right) \end{aligned}$$

$$\ll \sum_{a<N^{1/9}} \left(\frac{N}{a}\right)^{1/4}$$
$$\ll N^{1/3}$$

Again, to handle the other situation, in the parenthesis, we have that $U \asymp b^2$ and $V \asymp (b-c)^2$; and thus, $K \asymp ab^6(b-c)^2 \gg a(b-c)^8$, which gives us the same count. ∎

Chapter 6

A Lower Bound

The main result of this chapter is the following corollary which will be proven at the very end of this chapter. We will first state it here

Corollary 6.7: *Let $r^+(n)$ be as given in (1.1). Then:*

$$\sum_{n<N} \binom{r^+(n)}{2} \gg N^{1/3} \log^4 N$$

Notice that this is indeed the same order as the upper bound predicted by Manin's conjecture which was discussed in the introduction. In order to prove this lower bound, we begin with a few preliminary lemmas.

Lemma 6.1: *Fix $\delta > 0$ small, then:*

$$\prod_{p|N} \left(1 - \frac{1}{p}\right) = \left\{1 + O\left(\frac{1}{\log\log N}\right)\right\} \prod_{\substack{p|N \\ p<\delta \log N}} \left(1 - \frac{1}{p}\right)$$

Proof. First we see that:

$$\prod_{p|N} \left(1 - \frac{1}{p}\right) \leq \prod_{\substack{p|N \\ p<\delta \log N}} \left(1 - \frac{1}{p}\right)$$

Next, split the product, and note that the number of prime factors p of N for which $p > \delta \log N$ is less than $\frac{\log N}{\log\log(N^\delta)}$. So:

$$\begin{aligned} \prod_{p|N} \left(1 - \frac{1}{p}\right) &= \prod_{\substack{p|N \\ p\geq\delta \log N}} \left(1 - \frac{1}{p}\right) \cdot \prod_{\substack{p|N \\ p<\delta \log N}} \left(1 - \frac{1}{p}\right) \\ &\geq \left(1 - \frac{1}{\delta \log N}\right)^{\frac{\log N}{\log\log(N^\delta)}} \prod_{\substack{p|N \\ p<\delta \log N}} \left(1 - \frac{1}{p}\right) \\ &= \left\{1 + O\left(\frac{1}{\log\log N}\right)\right\} \prod_{\substack{p|N \\ p<\delta \log N}} \left(1 - \frac{1}{p}\right) \end{aligned}$$ ∎

The next two lemmas bound $L(s,\chi)$ in different regions of the complex plane. For the region $0 < Re(s) < 1$, Rademacher [15] gives a bound which is better for most of the region, but Lemma 6.2 suffices as a bound for the entire region for our purposes.

Lemma 6.2: *Let $s = \sigma + it$, and let χ be a non-trivial character modulo d, then for $0 < \sigma \leq 1$:*

$$|L(s,\chi)| \ll (d(|s|+1))^{1-\sigma}\left(\log(d(|s|+1)) + \frac{1}{\sigma}\right)$$

Proof: We begin by rearranging the definition for $L(s,\chi)$ which is defined for $\sigma > 1$

$$\begin{aligned}
L(s,\chi) &= \sum_{n\geq 1}\frac{\chi(n)}{n^s} \\
&= \sum_{n\leq d(|s|+1)}\frac{\chi(n)}{n^s} + \sum_{k\geq |s|+1}\sum_{1\leq a<d}\frac{\chi(kd+a)}{(kd+a)^s} \\
&= \sum_{n\leq d(|s|+1)}\frac{\chi(n)}{n^s} + \sum_{k\geq |s|+1}\sum_{1\leq a<d}\chi(a)\left(\frac{1}{(kd+a)^s} - \frac{1}{(kd)^s}\right) \\
&= \sum_{n\leq d(|s|+1)}\frac{\chi(n)}{n^s} + \sum_{k\geq |s|+1}\frac{1}{(kd)^s}\sum_{1\leq a<d}\chi(a)\left(\left(1+\frac{a}{kd}\right)^{-s} - 1\right)
\end{aligned}$$

arriving an expression which is valid for $\sigma > 0$.

We now bound this for $0 < \sigma \leq 1$, first we note that:

$$|L(s,\chi)| \ll \sum_{n\leq d(|s|+1)}\frac{1}{n^\sigma} + \sum_{k\geq |s|+1}\frac{1}{(kd)^\sigma}\sum_{1\leq a<d}\frac{a|s|}{kd}$$

We can continue by bounding each of the sums above. For the first sum, if $\sigma = 1$ then:

$$\sum_{n\leq d(|s|+1)}\frac{1}{n^\sigma} \ll \log(d(|s|+1)) \tag{6.1}$$

While for $0 < \sigma < 1$:

$$\begin{aligned}
\sum_{n\leq d(|s|+1)}\frac{1}{n^\sigma} &\ll \left(\frac{(d(|s|+1))^{1-\sigma}}{1-\sigma} - \frac{1}{1-\sigma}\right) + 1 \\
&\ll (d(|s|+1))^{1-\sigma}\log(d(|s|+1)) \qquad (6.2)
\end{aligned}$$

The last line comes from using the mean value theorem on the function $f(x) = (d(|s|+1))^{1-x}$ to bound the expression inside the parentheses.

For the second sum, since $a < d$ we have:

$$\begin{aligned}\sum_{k\geq|s|+1}\frac{1}{(kd)^\sigma}\sum_{1\leq a<d}\frac{a|s|}{kd} &\leq |s|d^{-\sigma}\sum_{k\geq|s|+1}\frac{1}{k^{1+\sigma}}\sum_{1\leq a<d}1\\ &< |s|d^{1-\sigma}\sum_{k\geq|s|+1}\frac{1}{k^{1+\sigma}}\\ &\ll \frac{|s|^{1-\sigma}d^{1-\sigma}}{\sigma} \qquad (6.3)\end{aligned}$$

Gathering (6.1), (6.2) and (6.3) finishes the lemma. ∎

Lemma 6.3: *Let $s = \sigma + it$, and let χ be a non-trivial character modulo d, then for $1 \leq \sigma < 2$:*

$$|L(s,\chi)| \ll \log(d(|s|+1))$$

Proof: We'll begin as in Lemma 6.2, with the following rearrangement of $L(s,\chi)$:

$$L(s,\chi) = \sum_{n\leq d(|s|+1)}\frac{\chi(n)}{n^s} + \sum_{k\geq|s|+1}\frac{1}{(kd)^s}\sum_{1\leq a<d}\chi(a)\left(\left(1+\frac{a}{kd}\right)^{-s}-1\right)$$

Again proceeding as in Lemma 6.2 we continue with:

$$|L(s,\chi)| \ll \sum_{n\leq d(|s|+1)}\frac{1}{n^\sigma} + \sum_{k\geq|s|+1}\frac{1}{(kd)^\sigma}\sum_{1\leq a<d}\frac{a|s|}{kd}$$

We'll bound each of these two sums separately beginning with the first sum:

$$\sum_{n\leq d(|s|+1)}\frac{1}{n^\sigma} \leq \sum_{n\leq d(|s|+1)}\frac{1}{n} \ll \log(d(|s|+1)) \qquad (6.4)$$

Continuing by bounding the second sum:

$$\begin{aligned}\sum_{k\geq|s|+1}\frac{1}{(kd)^\sigma}\sum_{1\leq a<d}\frac{a|s|}{kd} &\leq |s|d^{-\sigma}\sum_{k\geq|s|+1}\frac{1}{k^{1+\sigma}}\sum_{1\leq a<d}1\\ &< |s|d^{1-\sigma}\sum_{k\geq|s|+1}\frac{1}{k^{1+\sigma}}\\ &\ll \frac{(|s|d)^{1-\sigma}}{\sigma} \qquad (6.5)\end{aligned}$$

Since $\sigma \geq 1$, together (6.4) and (6.5) gives our result. ∎

From Davenport [1] we have the following result:

Lemma 6.4: *Let $\delta(y)$ denote the function (for $c > 0$):*

$$\delta(y) = \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty} y^s \frac{ds}{s} = \begin{cases} 0 & \text{if } 0 < y < 1 \\ 1/2 & \text{if } y = 1 \\ 1 & \text{if } y > 1 \end{cases}$$

and let:

$$I(y,T) = \frac{1}{2i\pi}\int_{c-iT}^{c+iT} \frac{y^s}{s} ds$$

Then for $y > 0$, $c > 0$, $T > 0$:

$$|I(y,T) - \delta(y)| < \begin{cases} y^c \min(1, T^{-1}|\log y|^{-1}) & \text{if } y \neq 1 \\ cT^{-1} & \text{if } y = 1 \end{cases}$$

With these we can prove the following proposition:

Proposition 6.5: *Let $\omega(n)$ be the number of distinct prime factors of n, and let*

$$\rho(n) = \#\{t \pmod{n} : t^2 \equiv -3 \pmod{n}\}$$

then for any M

$$\sum_{\substack{g<G \\ (g,6)=1}} \frac{3^{\omega(g)}\rho(g)}{g} \prod_{\substack{5<p<M \\ p|g}} \left(1 - \frac{6}{p}\right) = K \log^3 G + O(\log^2 G)$$

where:

$$\begin{aligned} K &= \frac{4^3}{6 \cdot 3^3 \cdot 5^3} \prod_{5<p<M} \left(1 + 3\left(1 - \frac{6}{p}\right)\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3 \\ &\quad \cdot \prod_{p \geq M} \left(1 + 3\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3 \end{aligned}$$

Proof.

$$\sum_{\substack{g<G\\(g,6)=1}} \frac{3^{\omega(g)}\rho(g)}{g} \prod_{\substack{5<p<M\\p|g}} \left(1-\frac{6}{p}\right)$$

$$= \sum_{\substack{g<G\\(g,30)=1}} \frac{1}{g} \prod_{\substack{p^a\|g\\5<p<M}} \left(3\rho(p^a)\left(1-\frac{6}{p}\right)\right) \prod_{\substack{p^a\|g\\p\geq M}} 3\rho(p^a)$$

$$= \sum_{\substack{g\geq 1\\(g,30)=1}} \frac{1}{g} \left(\prod_{\substack{p^a\|g\\5<p<M}} 3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}} 3\rho(p^a)\right) \frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\left(\frac{G}{g}\right)^s\frac{ds}{s}$$

by Lemma 6.4, for some $c > 0$. We'll want to approximate the infinite integral with the following integral with finite limits:

$$\int_{c-iT}^{c+iT}\left(\frac{G}{g}\right)^s\frac{ds}{s}$$

for some appropriate T. We'll show first that this integral with the finite limits gives the desired result, and then show that this approximation is valid. It turns out that using the following for c and T will allow us to more easily bound error terms:

$$\begin{aligned} c &= \frac{1}{\log G} \\ T &= G^{1/12} \end{aligned} \tag{6.6}$$

We begin by re-writing

$$\sum_{\substack{g\geq 1\\(g,30)=1}} \frac{1}{g} \left(\prod_{\substack{p^a\|g\\5<p<M}} 3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}} 3\rho(p^a)\right) \frac{1}{2i\pi}\int_{c-iT}^{c+iT}\left(\frac{G}{g}\right)^s\frac{ds}{s}$$

$$\begin{aligned} = \frac{1}{2i\pi}\int_{c-iT}^{c+iT} \prod_{5<p<M}&\left(1+3\left(1-\frac{6}{p}\right)\left(1+\left(\frac{-3}{p}\right)\right)\sum_{k\geq 1}\frac{1}{p^{k(1+s)}}\right) \\ &\cdot\prod_{p\geq M}\left(1+3\left(1+\left(\frac{-3}{p}\right)\right)\sum_{k\geq 1}\frac{1}{p^{k(s+1)}}\right)\left(\frac{G^s}{s}\right)ds \end{aligned} \tag{6.7}$$

since for $p > 3$ and $a \geq 1$, $\rho(p^a) = \rho(p) = 1 + \left(\frac{-3}{p}\right)$.

Now let,

$$\begin{aligned} A(s) &= \kappa(s) \prod_{5<p<M} \left(\left(1 + 3\left(1 - \frac{6}{p}\right)\left(1 + \left(\frac{-3}{p}\right)\right) \sum_{k\geq 1} \frac{1}{p^{ks}} \right) \right. \\ & \qquad \left. \cdot \left(1 - \frac{1}{p^s}\right)^3 \left(1 - \frac{\left(\frac{-3}{p}\right)}{p^s}\right)^3 \right) \\ & \quad \cdot \prod_{p\geq M} \left(\left(1 + 3\left(1 + \left(\frac{-3}{p}\right)\right) \sum_{k\geq 1} \frac{1}{p^{ks}} \right) \right. \\ & \qquad \left. \cdot \left(1 - \frac{1}{p^s}\right)^3 \left(1 - \frac{\left(\frac{-3}{p}\right)}{p^s}\right)^3 \right) \end{aligned} \tag{6.8}$$

where:

$$\kappa(s) = \left(1 - \frac{1}{4^s}\right)^3 \left(1 - \frac{1}{3^s}\right)^3 \left(1 - \frac{1}{25^s}\right)^3$$

By expanding the terms inside the product we see:

$$\begin{aligned} A(s) &= \kappa(s) \prod_{5<p<M} \left(1 - \frac{6}{p^{s+1}} + \left(-9 - 6\left(\frac{-3}{p}\right)\right) \frac{1}{p^{2s}} \right. \\ & \qquad \left. + \left(-126 - 126\left(\frac{-3}{p}\right)\right) \frac{1}{p^{2s+1}} + O\left(\frac{1}{p^{3s}}\right) \right) \\ & \quad \cdot \prod_{p\geq M} \left((1 + \left(-9 - 6\left(\frac{-3}{p}\right)\right) \frac{1}{p^{2s}} + O\left(\frac{1}{p^{3s}}\right) \right) \end{aligned}$$

So we then can bound

$$|A(s)| \leq \kappa'(\sigma) \prod_{p} \left(1 + \frac{6}{p^{\sigma+1}} + \frac{15}{p^{2\sigma}} + \frac{252}{p^{2\sigma+1}} + O\left(\frac{1}{p^{3\sigma}}\right) \right)$$

where:

$$\kappa'(s) = \left(1 + \frac{1}{4^s}\right)^3 \left(1 + \frac{1}{3^s}\right)^3 \left(1 + \frac{1}{25^s}\right)^3$$

Hence, not only is $A(s)$ is absolutely convergent for $\sigma > 1/2$, but we can bound $A(s)$ uniformly, irrespective to our choice of M, so long as we can fix a δ and consider only $\sigma \geq \delta > 1/2$.

Using this notation, we can continue (6.7) from above:

$$\sum_{\substack{g\geq 1\\(g,30)=1}} \frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}} 3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}} 3\rho(p^a)\right)\frac{1}{2i\pi}\int_{c-iT}^{c+iT}\left(\frac{G}{g}\right)^s\frac{ds}{s}$$

$$= \frac{1}{2i\pi}\int_{c-iT}^{c+iT}\zeta(1+s)^3L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds$$

We can evaluate this integral by extending the integral from a line integral to a closed rectangle R with corners, $c-iT, c+iT, \frac{-1}{6}+iT, \frac{-1}{6}-iT$. Around this closed curve R we have:

$$2i\pi\sum\{\text{residues inside } R\} = \int_R = \int_{c-iT}^{c+iT} + \int_{c+iT}^{\frac{-1}{6}+iT} + \int_{\frac{-1}{6}+iT}^{\frac{-1}{6}-iT} + \int_{\frac{-1}{6}-iT}^{c-iT} \tag{6.9}$$

We continue by showing that we can bound the last three integrals on the right hand side of this equality. First we'll bound the two two horizontal integrals, by splitting the integral into two pieces. First integrating with respect to s along the line $c+iT$ to iT. Along this integral, $1+s$ will run from $(1+c)+iT$ to $1+iT$. Since T is large and $c>0$, then for large G in this region we can bound:

$$\begin{aligned} |\zeta(1+s)| &\ll \log(T) \\ \left|L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)\right| &\ll \log(T) \end{aligned}$$

The bound for the $L-$function comes from Lemma 6.3 above and the bound for ζ from Titchmarsh [20].

With this we can bound this integral as:

$$\left|\int_{c+iT}^{iT}\zeta(1+s)^3L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right|$$

$$\begin{aligned} &\ll \frac{\log^6 T}{T}\int_{c+iT}^{iT}|G^s|\,ds \\ &\ll \frac{\log^6 T}{T}\frac{G^c}{\log G} \end{aligned} \tag{6.10}$$

Next we bound the integral for s along the line iT to $\frac{-1}{6}+iT$. Along this integral, $1+s$ will run from $1+iT$ to $\frac{5}{6}+iT$. Since T is large, in this region we can bound:

$$\begin{aligned} |\zeta(1+s)| &\ll T^{1/12+o(1)} \\ \left|L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)\right| &\ll T^{1/6+o(1)} \end{aligned} \tag{6.11}$$

This bound for the $L-$function comes from Lemma 6.2 above, and the bound for ζ from Titchmarsh [20].

With this we can bound this integral as:

$$\left|\int_{iT}^{-1/6+iT} \zeta(1+s)^3 L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right|$$

$$\begin{aligned} &\ll \frac{T^{1/4+o(1)}T^{1/2+o(1)}}{T} \int_{iT}^{-1/6+iT} |G^s|\, ds \\ &\ll T^{-1/4+o(1)} \end{aligned} \tag{6.12}$$

Putting together (6.10) and (6.12) with our choices for c and T we have:

$$\left|\int_{c+iT}^{-1/6+iT} \zeta(1+s)^3 L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right| \ll G^{-1/48+o(1)} \tag{6.13}$$

In the same way, we can bound:

$$\left|\int_{c-iT}^{\frac{-1}{6}-iT} \zeta(1+s)^3 L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right| \ll G^{-1/48+o(1)} \tag{6.14}$$

For the final integral, along the line with s taking values $\frac{-1}{6}+iT$ to $\frac{-1}{6}-iT$ we can use the same bounds for ζ and L given in (6.11), hence:

$$\left|\int_{\frac{-1}{6}+iT}^{\frac{-1}{6}-iT} \zeta(1+s)^3 L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right|$$

$$\ll T^{3/4+o(1)} \int_{\frac{-1}{6}+iT}^{\frac{-1}{6}-iT} \left|\frac{G^s}{s}\right| ds$$

$$\ll \frac{T^{7/4+o(1)}}{G^{1/6}} \tag{6.15}$$

So putting together (6.9) with (6.13), (6.14), and (6.15) and our choices for c and T, we have:

$$\frac{1}{2i\pi} \int_{c-iT}^{c+iT} \zeta(1+s)^3 L\left(1+s, \left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s} ds$$

$$= \sum \{\text{residues inside } R\} + O\left(G^{-1/48+o(1)}\right) \tag{6.16}$$

We must now calculate the residues inside the rectangle R. Inside the rectangle, both $L\left(1+s, \left(\frac{-3}{\cdot}\right)\right)$ and $A(1+s)$ are analytic and their value at $s = 0$ is independent of the choice of G. The rest of the integrand has only the pole at $s = 0$ inside the rectangle. Since $\zeta(s+1)$ has a simple pole at $s = 0$ with residue 1, $\zeta(s+1)^3$ has a pole of order three. By expanding G^s we have:

$$G^s = e^{s \log G} = 1 + s \log G + \frac{(s \log G)^2}{2} + \frac{(s \log G)^3}{3!} + \cdots$$

Therefore:

$$\{\text{residue at } s = 0\} = L\left(1, \left(\frac{-3}{\cdot}\right)\right)^3 A(1)\frac{\log^3 G}{3!} + O\left(\log^2 G\right)$$

$$= \frac{\log^3 G}{3!} \prod_p \left(1 - \frac{\left(\frac{-3}{p}\right)}{p}\right)^{-3}$$

$$\cdot \kappa(1) \prod_{5<p<M} \left(\left(1 + 3\left(1 - \frac{6}{p}\right)\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\right.$$

$$\left.\cdot \left(1 - \frac{1}{p}\right)^3 \left(1 - \frac{\left(\frac{-3}{p}\right)}{p}\right)^3\right)$$

$$
\begin{aligned}
&\cdot \prod_{p \geq M} \left(\left(1 + 3\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right) \right. \\
&\qquad\qquad\qquad \left. \cdot \left(1 - \frac{1}{p}\right)^3 \left(1 - \frac{\left(\frac{-3}{p}\right)}{p}\right)^3 \right) \\
&+ O\left(\log^2 G\right) \\
= \; & \log^3 G \frac{4^3}{3! \cdot 3^3 \cdot 5^3} \\
&\cdot \prod_{5<p<M} \left(\left(1 + 3\left(1 - \frac{6}{p}\right)\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3 \right) \\
&\cdot \prod_{p \geq M} \left(1 + 3\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3 \\
&+ O(\log^2 G)
\end{aligned}
$$

So, by letting

$$
\begin{aligned}
K \; = \; & \frac{4^3}{3! \cdot 3^3 \cdot 5^3} \prod_{5<p<M} \left(\left(1 + 3\left(1 - \frac{6}{p}\right)\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3 \right) \\
& \cdot \prod_{p \geq M} \left(1 + 3\left(1 + \left(\frac{-3}{p}\right)\right)\left(\frac{1}{p-1}\right)\right)\left(1 - \frac{1}{p}\right)^3
\end{aligned}
$$

we have:

$$
\{\text{residue at } s = 0\} = K \log^3 G + O\left(\log^2 G\right)
$$

Using this with (6.16) we then have:

$$
\frac{1}{2i\pi} \int_{c-iT}^{c+iT} \zeta(1+s)^3 L\left(1+s, \left(\frac{-3}{\cdot}\right)\right)^3 A(1+s) \frac{G^s}{s} ds = K \log^3 G + O\left(\log^2 G\right) \tag{6.17}
$$

We now will bound the error induced by approximating the integral having infinite limits of integration, with the integral with the appropriate finite limits. Using Lemma 6.4:

$$
\left| \sum_{g<G} \frac{3^{\omega(g)}\rho(g)}{g} \prod_{\substack{5<p<L \\ p|g}} \left(1 - \frac{6}{p}\right) - \frac{1}{2i\pi} \int_{c-iT}^{c+iT} \zeta(1+s)^3 L\left(1+s, \left(\frac{-3}{\cdot}\right)\right)^3 A(1+s) \frac{G^s}{s} ds \right|
$$

$$
= \sum_{\substack{g \geq 1 \\ (g,30)=1}} \frac{1}{g} \left(\prod_{\substack{p^a \| g \\ 5<p<M}} 3\rho(p^a)\left(1 - \frac{6}{p}\right) \right) \left(\prod_{\substack{p^a \| g \\ p \geq M}} 3\rho(p^a) \right)
$$

$$
\begin{aligned}
&\cdot\left|\frac{1}{2i\pi}\int_{c-i\infty}^{c+i\infty}\left(\frac{G}{g}\right)^s\frac{ds}{s}-\frac{1}{2i\pi}\int_{c-iT}^{c+iT}\left(\frac{G}{g}\right)^s\frac{ds}{s}\right| \\
<\ &\sum_{\substack{|g-G|<G^{17/18}\\(g,30)=1}}\frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}}3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}}3\rho(p^a)\right)\left(\frac{G}{g}\right)^c \qquad (6.18)\\
+\ &\sum_{\substack{|g-G|>G^{17/18}\\(g,30)=1}}\frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}}3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}}3\rho(p^a)\right)\frac{\left(\frac{G}{g}\right)^c}{T|\log(G/g)|}
\end{aligned}
$$

We'll bound each of these sums separately beginning with the first sum. Since

$$\omega(g)\ll\frac{\log G}{\log\log G}$$

we can bound:

$$
\begin{aligned}
&\sum_{\substack{|g-G|<G^{17/18}\\(g,30)=1}}\frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}}3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}}3\rho(p^a)\right)\left(\frac{G}{g}\right)^c \\
&\qquad\ll\ \frac{1}{G}\sum_{|g-G|<G^{17/18}}6^{\omega(g)} \\
&\qquad\ll\ G^{-1/18+o(1)} \qquad (6.19)
\end{aligned}
$$

We bound the second summation next:

$$
\begin{aligned}
&\sum_{\substack{|g-G|>G^{17/18}\\(g,30)=1}}\frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}}3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}}3\rho(p^a)\right)\left(\frac{G}{g}\right)^c\frac{1}{T|\log(G/g)|} \\
\ll\ &\frac{G^{1/18+c}}{T}\sum_{\substack{g\geq1\\(g,30)=1}}\frac{1}{g^{1+c}}\left(\prod_{\substack{p^a\|g\\5<p<M}}3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}}3\rho(p^a)\right) \\
=\ &\frac{G^{1/18+c}}{T}\prod_{5<p<M}\left(1+3\rho(p)\left(1-\frac{6}{p}\right)\left(\sum_{k\geq1}\frac{1}{p^{k(1+c)}}\right)\right) \\
&\cdot\prod_{p\geq M}\left(1+3\rho(p)\left(\sum_{k\geq1}\frac{1}{p^{k(1+c)}}\right)\right) \\
=\ &\frac{G^{1/18+c}}{T}\zeta(1+c)^3L\left(1+c,\left(\frac{-3}{\cdot}\right)\right)^3A(1+c) \qquad (6.20)
\end{aligned}
$$

Recall our choice for $c = 1/\log G$, and so for large values of G we have $1 < 1 + c < 2$. In this region, we can bound both $L\left(1+c, \left(\frac{-3}{\cdot}\right)\right)^3$ and $A(1+c)$ by a constant. Moreover, as $c \to 0$ along the real axis, we have $\zeta(1+c) = \frac{1}{c} + O(1)$; and so:

$$\zeta(1+c)^3 = \frac{1}{c^3} + O\left(\frac{1}{c^2}\right)$$

Using these and recalling our choices for c and T, we continue (6.20):

$$\sum_{\substack{|g-G|>G^{17/18}\\(g,30)=1}} \frac{1}{g}\left(\prod_{\substack{p^a\|g\\5<p<M}} 3\rho(p^a)\left(1-\frac{6}{p}\right)\right)\left(\prod_{\substack{p^a\|g\\p\geq M}} 3\rho(p^a)\right)\left(\frac{G}{g}\right)^c \frac{1}{T|\log(G/g)|}$$

$$\begin{aligned} &\ll \frac{G^{1/18+c}}{Tc^3} \\ &\ll \frac{\log^3 G}{G^{1/36}} \end{aligned} \qquad (6.21)$$

Putting together (6.19) and (6.21) we continue (6.18) to get:

$$\left|\sum_{g<G}\frac{3^{\omega(g)}\rho(g)}{g}\prod_{\substack{5<p<M\\p|g}}\left(1-\frac{6}{p}\right) - \frac{1}{2i\pi}\int_{c-iT}^{c+iT}\zeta(1+s)^3 L\left(1+s,\left(\frac{-3}{\cdot}\right)\right)^3 A(1+s)\frac{G^s}{s}ds\right| \ll \frac{\log^3 G}{G^{1/36}} \qquad (6.22)$$

Finally, by combining (6.17) with (6.22) we complete the proof of Proposition 6.5. ∎

We can now prove the following result concerning primitive solutions. We'll use this to then prove a result concerning non-primitive solutions which relates this work back to the function $r^+(n)$ defined at the beginning of the first chapter.

Theorem 6.6:

$$\#\left\{a,b,c:\ {}^{a,b,c>0,\ \gcd(a,b,c)=1,}_{\substack{\phi(a,b,c)=(W,X,Y,Z)\\ g=\gcd(W,X,Y,Z),\ W^3+Z^3<g^3N,\\ W,Z,-X,-Y\geq 0}}\right\} \gg N^{1/3}\log^3 N$$

Proof. First, let $L = g^{1/3}N^{1/9}$, and we'll consider only the solutions for which $L/2 < a < L$. From Proposition 2.3, we can insure that we are only considering solutions for which $W, Z, -X, -Y$ are all positive if we consider only a, b, c triples with $a, b, c > 0$, $\gcd(a, b, c) = 1$, and $b + c < a$. Therefore, we'll count the number of triples arising as $b < L/4$, and $c < L/4$.

The idea is to count as follows:

$$\#\left\{a,b,c:\ \substack{a,b,c>0,\ \gcd(a,b,c)=1,\\ \phi(a,b,c)=(W,X,Y,Z)\\ g=\gcd(W,X,Y,Z),\ W^3+Z^3<g^3N,\\ W,Z,-X,-Y\geq 0}\right\}$$

$$\begin{aligned} &\geq \sum_{\substack{g<N^{1/9}\\ (g,6)=1}} \#\left\{a,b,c:\ \substack{a,b,c>0,\ \gcd(a,b,c)=1,\\ \phi(a,b,c)=(W,X,Y,Z)\\ g=\gcd(W,X,Y,Z),\ W^3+Z^3<g^3N,\\ W,Z,-X,-Y\geq 0}\right\} \\ &\geq \sum_{\substack{g<N^{1/9}\\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g\\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \mathsf{N}(\alpha,\beta,\gamma) \end{aligned} \tag{6.23}$$

where:

$$\mathsf{N}(\alpha,\beta,\gamma) = \#\left\{a,b,c:\ \substack{(a,b,c)=1,\ \phi(a,b,c)=(W,X,Y,Z),\\ W,Z,-X,-Y\geq 0,\ \gcd(W,X,Y,Z)=g=\alpha\beta\gamma\\ \alpha=(a,c^2+3b^2),\ \beta=(b,c^2+3a^2),\\ \gamma=(c,b^2+3a^2)}\right\}$$

Note that by Theorem 3.1, we know that if 2 doesn't divide $\alpha\beta\gamma$ then 2 can not divide g, similarly for 3.

Using (2.5) and (2.6) we see that if $b, c < a$, then $U, V \asymp a^2$ and $K \asymp a^9$. Let $M = \frac{1}{100}\log N$, and $\rho(n) = \#\{t \pmod n : t^2 \equiv -3 \pmod n\}$. By applying Lemma 6.1 we have:

$$\begin{aligned}
\mathsf{N}(\alpha,\beta,\gamma) &\geq \sum_{\substack{a=\frac{1}{2}L \\ \alpha|a}}^{L} \sum_{\substack{b<\frac{1}{4}L \\ \beta|b \\ \gamma|b^2+3a^2}} \sum_{\substack{c<\frac{1}{4}L \\ \gamma|c \\ \alpha|c^2+3b^2 \\ \beta|c^2+3a^2 \\ (a,b,c)=1 \\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1 \\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1 \\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1 \\
&\gg \sum_{\substack{a=\frac{1}{2}L \\ \alpha|a}}^{L} \sum_{\substack{b<\frac{1}{4}L \\ \beta|b \\ \gamma|b^2+3a^2}} \rho(\alpha\beta)\frac{L}{g} \prod_{\substack{p|b \\ p>3}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{b^2+3a^2}{\gamma} \\ p>3}} \left(1-\frac{1}{p}\right) \\
&\qquad \cdot \prod_{\substack{p|\frac{a}{\alpha} \\ p>3}} \left(1-\frac{2}{p}\right) \prod_{\substack{p|\frac{b}{\beta} \\ p>3}} \left(1-\frac{2}{p}\right) \\
&\gg \frac{\rho(\alpha\beta)L}{g} \sum_{\substack{a=\frac{1}{2}L \\ \alpha|a}}^{L} \prod_{\substack{p|\frac{a}{\alpha} \\ 3<p<M}} \left(1-\frac{2}{p}\right) \sum_{\substack{b<\frac{1}{4}L \\ \beta|b \\ \gamma|b^2+3a^2}} \prod_{\substack{p|b \\ 3<p<M}} \left(1-\frac{1}{p}\right) \\
&\qquad \cdot \prod_{\substack{p|\frac{b^2+3a^2}{\gamma} \\ 3<p<M}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{b}{\beta} \\ 3<p<M}} \left(1-\frac{2}{p}\right) \qquad (6.24)
\end{aligned}$$

We continue by bounding the inner most sum:

$$\begin{aligned}
&\sum_{\substack{b<\frac{1}{4}L \\ \beta|b \\ \gamma|b^2+3a^2}} \prod_{\substack{p|b, \\ 3<p<M}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{b^2+3a^2}{\gamma} \\ 3<p<M}} \left(1-\frac{1}{p}\right) \prod_{\substack{p|\frac{b}{\beta} \\ 3<p<M}} \left(1-\frac{2}{p}\right) \\
&\gg \sum_{\substack{0\leq r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{b<\frac{1}{4}L \quad b\equiv r \pmod{\beta\gamma}} \prod_{\substack{p|b \\ 3<p<M}} \left(1-\frac{3}{p}\right) \prod_{\substack{p|b^2+3a^2 \\ 3<p<M}} \left(1-\frac{1}{p}\right) \\
&= \sum_{\substack{0\leq r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{b<\frac{1}{4}L \quad b\equiv r \pmod{\beta\gamma}} \sum_{\substack{d|b \\ p|d\Rightarrow 3<p<M}} \frac{\mu(d)3^{\omega(d)}}{d} \sum_{\substack{e|b^2+3a^2 \\ p|e\Rightarrow 3<p<M}} \frac{\mu(e)}{e} \\
&= \sum_{\substack{0\leq r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ p|d\Rightarrow 3<p<M}} \frac{\mu(d)3^{\omega(d)}}{d} \sum_{\substack{e<\frac{49}{16}L^2 \\ p|e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1}} \frac{\mu(e)}{e} \sum_{\substack{b<\frac{1}{4}L \\ b\equiv r \pmod{\beta\gamma} \\ b\equiv 0 \pmod{d} \\ b^2\equiv -3a^2 \pmod{e}}} 1
\end{aligned}$$

$$= \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ p|d\Rightarrow 3<p<M \\ p|(d,\gamma)\Rightarrow p|a}} \frac{\mu(d)3^{\omega(d)}}{d}$$

$$\sum_{\substack{e<\frac{49}{16}L^2 \\ p|e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1 \\ p|(e,d)\Rightarrow p|a \\ p|(e,\beta)\Rightarrow p|a}} \frac{\mu(e)}{e} 2^{\omega'(e,a)} \left\{ \frac{\frac{1}{4}L}{\mathrm{LCM}(\beta\gamma,d,e)} + O(1) \right\}$$

$$= \frac{1}{4}\frac{L}{\beta\gamma} \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ p|d\Rightarrow 3<p<M \\ p|(d,\gamma)\Rightarrow p|a}} \frac{\mu(d)3^{\omega(d)}}{d} \prod_{\substack{p|d \\ p\nmid\beta\gamma}} \frac{1}{p}$$

$$\sum_{\substack{e<\frac{49}{16}L^2 \\ p|e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1 \\ p|(e,d)\Rightarrow p|a \\ p|(e,\beta)\Rightarrow p|a}} \frac{\mu(e)2^{\omega'(e,a)}}{e} \prod_{\substack{p|e \\ p\nmid d\beta\gamma}} \frac{1}{p}$$

$$+O\left(\sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ d-\text{square free} \\ p|d\Rightarrow 3<p<M \\ p|(d,\gamma)\Rightarrow p|a}} \frac{3^{\omega(d)}}{d} \sum_{\substack{e<\frac{49}{16}L^2 \\ e-\text{square free} \\ p|e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1 \\ p|(e,d)\Rightarrow p|a \\ p|(e,\beta)\Rightarrow p|a}} \frac{2^{\omega'(e,a)}}{e} \right) \tag{6.25}$$

where:

$$\omega(n) = \#\{\text{primes } p \mid n\}$$

$$\omega'(n,m) = \#\{\text{primes } p \mid n : p \nmid m\}$$

We can bound the error term as follows:

$$\sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ d-\text{square free} \\ p|d\Rightarrow 3<p<M \\ p|(d,\gamma)\Rightarrow p|a}} \frac{3^{\omega(d)}}{d} \sum_{\substack{e<\frac{49}{16}L^2 \\ e-\text{square free} \\ p|e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1 \\ p|(e,d)\Rightarrow p|a \\ p|(e,\beta)\Rightarrow p|a}} \frac{2^{\omega'(e,a)}}{e}$$

$$\ll \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ d-\text{square free} \\ p|d\Rightarrow 3<p<M \\ p|(d,\gamma)\Rightarrow p|a}} \frac{3^{\omega(d)}}{d} \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p|a}} \left(1+\frac{1}{p}\right) \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\nmid a}} \left(1+\frac{2}{p}\right)$$

$$
\begin{aligned}
&\ll (\log M)^2 \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d<\frac{1}{4}L \\ d-\text{square free} \\ p\mid d\Rightarrow 3<p<M \\ p\mid (d,\gamma)\Rightarrow p\mid a}} \frac{3^{\omega(d)}}{d} \\
&= (\log M)^2 \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \left(\prod_{\substack{3<p<M \\ p\mid (\gamma,a)}} \left(1+\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\nmid \gamma}} \left(1+\frac{3}{p}\right)\right) \\
&\ll (\log M)^5 \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} 1 \\
&= \rho(\gamma)(\log M)^5
\end{aligned}
$$

We will now bound the main term of (6.25). Note first that if d and e are square free and $p \mid de \Rightarrow 3 < p < M$ and by our choice of $M = \frac{1}{100}\log N$, that necessarily $e < \frac{49}{16}L^2$ and $d < L/4$. In fact the largest that d or e can be is:

$$
\prod_{p<M} p = \exp\left(\sum_{p<M} \log p\right) \le \exp((2\log 2)M) = \exp\left(\frac{\log 2}{50}\log N\right) < N^{1/50} = o(L)
$$

For a nice proof of the first inequality see [5].

So then:

$$
\frac{1}{4}\frac{L}{\beta\gamma} \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d\ge 1 \\ p\mid d\Rightarrow 3<p<M \\ p\mid (d,\gamma)\Rightarrow p\mid a}} \frac{\mu(d)3^{\omega(d)}}{d} \prod_{\substack{p\mid d \\ p\nmid \beta\gamma}} \frac{1}{p} \sum_{\substack{e\ge 1 \\ p\mid e\Rightarrow 3<p<M, \\ \left(\frac{-3}{p}\right)=1 \\ p\mid (e,d)\Rightarrow p\mid a \\ p\mid (e,\beta)\Rightarrow p\mid a}} \frac{\mu(e)2^{\omega'(e,a)}}{e} \prod_{\substack{p\mid e \\ p\nmid d\beta\gamma}} \frac{1}{p}
$$

$$
\begin{aligned}
= \frac{1}{4}\frac{L}{\beta\gamma} &\sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \sum_{\substack{d\ge 1 \\ p\mid d\Rightarrow 3<p<M \\ p\mid (d,\gamma)\Rightarrow p\mid a}} \frac{\mu(d)3^{\omega(d)}}{d} \prod_{\substack{p\mid d \\ p\nmid \beta\gamma}} \frac{1}{p} \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid (\beta,a)}} \left(1-\frac{1}{p}\right) \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid (d,a) \\ p\nmid \beta}} \left(1-\frac{1}{p}\right) \\
&\cdot \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid (a,\gamma) \\ p\nmid d\beta}} \left(1-\frac{1}{p}\right) \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid a \\ p\nmid d\beta\gamma}} \left(1-\frac{1}{p^2}\right) \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid \gamma \\ p\nmid ad\beta}} \left(1-\frac{2}{p}\right) \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\nmid ad\beta\gamma}} \left(1-\frac{2}{p^2}\right)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{1}{4}\frac{L}{\beta\gamma} \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid(\beta,a)}} \left(1-\frac{1}{p}\right) \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} \prod_{\substack{3<p<M \\ p\mid a \\ p\nmid \beta\gamma \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{4}{p^2}+\frac{3}{p^3}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{4}{p}+\frac{3}{p^2}\right) \\
&\qquad \cdot \prod_{\substack{3<p<M \\ p\mid a \\ p\nmid\beta\gamma \\ \left(\frac{-3}{p}\right)=-1}} \left(1-\frac{3}{p^2}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=-1}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid(a,\beta)}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid\beta \\ p\nmid a}} \left(1-\frac{3}{p}\right) \\
&\qquad \cdot \prod_{\substack{3<p<M \\ p\nmid a\beta\gamma \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{5}{p^2}\right) \prod_{\substack{3<p<M \\ p\mid\gamma \\ p\nmid a\beta \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{2}{p}\right) \prod_{\substack{3<p<M \\ p\nmid a\beta\gamma \\ \left(\frac{-3}{p}\right)=-1}} \left(1-\frac{3}{p^2}\right) \\
&\gg \frac{L}{\beta\gamma} \prod_{\substack{3<p<M \\ \left(\frac{-3}{p}\right)=1 \\ p\mid(a,\beta)}} \left(1-\frac{1}{p}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{4}{p}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=-1}} \left(1-\frac{3}{p}\right) \\
&\qquad \cdot \prod_{\substack{3<p<M \\ p\mid(a,\beta)}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid\beta \\ p\nmid a}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid\gamma \\ p\nmid a\beta \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{2}{p}\right) \sum_{\substack{0\le r<\beta\gamma \\ r\equiv 0 \pmod{\beta} \\ r^2\equiv -3a^2 \pmod{\gamma}}} 1 \\
&\gg \frac{L\rho(\gamma)}{\beta\gamma} \prod_{\substack{3<p<M \\ p\mid(a,\beta)}} \left(1-\frac{4}{p}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=1}} \left(1-\frac{4}{p}\right) \prod_{\substack{3<p<M \\ p\mid(a,\gamma) \\ p\nmid\beta \\ \left(\frac{-3}{p}\right)=-1}} \left(1-\frac{3}{p}\right)
\end{aligned}
$$

$$
\qquad \cdot \prod_{\substack{3<p<M \\ p\mid\beta \\ p\nmid a}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid\gamma \\ p\nmid a}} \left(1-\frac{2}{p}\right) \tag{6.26}
$$

$$
\gg \frac{L\rho(\gamma)}{\beta\gamma} \prod_{\substack{3<p<M \\ p\mid a}} \left(1-\frac{4}{p}\right) \prod_{\substack{3<p<M \\ p\mid\beta \\ p\nmid a}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p\mid\gamma \\ p\nmid a}} \left(1-\frac{2}{p}\right) \tag{6.27}
$$

$$
\gg \frac{L\rho(\gamma)}{\beta\gamma} \prod_{3<p<M} \left(1-\frac{4}{p}\right)
$$

To get the second equality, note that we have merely changed the sum over d into an Euler product, where the products inside the sum cause the Euler product to be split into various cases based upon the primes. For example, in the first case, $p \mid a,\ p \nmid \beta\gamma,\ \left(\frac{-3}{p}\right) = 1$, if p does not divide d we have the contribution from the fifth product of the summand $\left(1-\frac{1}{p^2}\right)$, while when p does divide d we have the usual factor $-\frac{3}{p}$ from the first term of the summand, multiplied by $\frac{1}{p}$ from the first product and $\left(1-\frac{1}{p}\right)$ from the second, giving us:

$$\left(\left(1-\frac{1}{p^2}\right)-\frac{3}{p}\frac{1}{p}\left(1-\frac{1}{p}\right)\right)=\left(1-\frac{4}{p^2}+\frac{3}{p^3}\right)$$

Also, we notice that by our choices for L and g that:

$$\frac{L}{\beta\gamma}\prod_{3<p<M}\left(1-\frac{4}{p}\right)\gg\frac{L}{\beta\gamma\log^4 M}\gg\frac{N^{1/27}}{\log^4 M}$$

So indeed, the main term is the dominant term.

We now return to (6.24) using these bounds and (6.27):

$$\begin{aligned}
\mathsf{N}(\alpha,\beta,\gamma) &\gg \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\sum_{\substack{a=\frac{1}{2}L\\ \alpha|a}}^{L}\prod_{\substack{3<p<M\\ p|a}}\left(1-\frac{2}{p}\right)\prod_{\substack{3<p<M\\ p|a}}\left(1-\frac{4}{p}\right)\\
&\gg \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\sum_{\substack{a=\frac{1}{2}L\\ \alpha|a}}^{L}\prod_{\substack{5<p<M\\ p|a}}\left(1-\frac{6}{p}\right)\\
&= \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\sum_{\substack{a=\frac{1}{2}L\\ \alpha|a}}^{L}\sum_{\substack{d|a\\ p|d\Rightarrow 5<p<M}}\frac{\mu(d)6^{\omega(d)}}{d}\\
&= \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\sum_{\substack{d<L\\ p|d\Rightarrow 5<p<M}}\frac{\mu(d)6^{\omega(d)}}{d}\sum_{\substack{a=\frac{1}{2}L\\ \alpha|a\\ d|a}}^{L}1\\
&= \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\sum_{\substack{d<L\\ p|d\Rightarrow 5<p<M}}\frac{\mu(d)6^{\omega(d)}}{d}\sum_{A=\left\lceil\frac{L}{2\mathrm{LCM}(\alpha,d)}\right\rceil}^{\left\lfloor\frac{L}{\mathrm{LCM}(\alpha,d)}\right\rfloor}1\\
&\gg \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\\
&\qquad\cdot\sum_{\substack{d<L\\ p|d\Rightarrow 5<p<M}}\frac{\mu(d)6^{\omega(d)}}{d}\left\{\frac{L}{\mathrm{LCM}(\alpha,d)}+O(1)\right\}\\
&= \frac{L^2\rho(g)}{\beta\gamma g}\prod_{\substack{3<p<M\\ p|\beta}}\left(1-\frac{3}{p}\right)\prod_{\substack{3<p<M\\ p|\gamma}}\left(1-\frac{2}{p}\right)\\
&\qquad\cdot\left\{L\sum_{\substack{d<L\\ p|d\Rightarrow 5<p<M}}\frac{\mu(d)6^{\omega(d)}}{d\,\mathrm{LCM}(\alpha,d)}+O\left(\sum_{\substack{d<L\\ d-\text{square free}\\ p|d\Rightarrow 5<p<M}}\frac{6^{\omega(d)}}{d}\right)\right\}
\end{aligned}$$

Note that as before, we can simply sum over all $d \geq 1$ instead of $d \leq L$ due to our choice of M, and the fact that d must be square free. We continue by showing that the error term indicated above is indeed smaller than the main term, by first bounding the main term:

$$\begin{aligned} L \sum_{\substack{d\geq 1 \\ p|d \Rightarrow 5<p<M}} \frac{\mu(d)6^{\omega(d)}}{d\,\mathrm{LCM}(\alpha,d)} &= \frac{L}{\alpha} \sum_{\substack{d\geq 1 \\ p|d \Rightarrow 5<p<M}} \frac{\mu(d)6^{\omega(d)}}{d} \prod_{\substack{5<p<M \\ p|d \\ p\nmid\alpha}} \frac{1}{p} \\ &= \frac{L}{\alpha} \prod_{\substack{5<p<M \\ p|\alpha}} \left(1-\frac{6}{p}\right) \prod_{\substack{5<p<M \\ p\nmid\alpha}} \left(1-\frac{6}{p^2}\right) \end{aligned}$$

While the error term becomes:

$$\ll \sum_{\substack{d\geq 1 \\ d-\text{squarefree} \\ p|d \Rightarrow 5<p<M}} \frac{6^{\omega(d)}}{d} = \prod_{5<p<M} \left(1+\frac{6}{p}\right)$$

Since $\alpha \log^n M = o(L)$ for any n, indeed the main term is larger than the error term. We can continue bounding $\mathsf{N}(\alpha,\beta,\gamma)$:

$$\begin{aligned} \mathsf{N}(\alpha,\beta,\gamma) &\gg \frac{L^3\rho(g)}{g^2} \prod_{\substack{5<p<M \\ p|\alpha}} \left(1-\frac{6}{p}\right) \prod_{\substack{3<p<M \\ p|\beta}} \left(1-\frac{3}{p}\right) \prod_{\substack{3<p<M \\ p|\gamma}} \left(1-\frac{2}{p}\right) \\ &\gg \frac{L^3\rho(g)}{g^2} \prod_{\substack{5<p<M \\ p|g}} \left(1-\frac{6}{p}\right) \end{aligned}$$

We now return to (6.23) using this bound:

$$\begin{aligned} &\#\left\{ a,b,c : \begin{smallmatrix} a,b,c>0,\ \gcd(a,b,c)=1, \\ \phi(a,b,c)=(W,X,Y,Z) \\ g=\gcd(W,X,Y,Z),\ W^3+Z^3<g^3N, \\ W,Z,-X,-Y\geq 0 \end{smallmatrix} \right\} \\ &\geq \sum_{\substack{g<N^{1/9} \\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g \\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \mathsf{N}(\alpha,\beta,\gamma) \\ &\gg \sum_{\substack{g<N^{1/9} \\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g \\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \frac{L^3\rho(g)}{g^2} \prod_{\substack{5<p<M \\ p|g}} \left(1-\frac{6}{p}\right) \\ &\gg \sum_{\substack{g<N^{1/9} \\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g \\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \frac{N^{1/3}\rho(g)}{g} \prod_{\substack{5<p<M \\ p|g}} \left(1-\frac{6}{p}\right) \\ &= N^{1/3} \sum_{\substack{g<N^{1/9} \\ (g,6)=1}} \frac{3^{\omega(g)}\rho(g)}{g} \prod_{\substack{5<p<M \\ p|g}} \left(1-\frac{6}{p}\right) \end{aligned}$$

Applying Proposition 6.5 completes the proof. ∎

We now prove the following corollary which gives us a lower bound on the count of the number of taxicab numbers.

Corollary 6.7: *Let $r^+(n)$ be as given in (1.1). Then:*

$$\sum_{n<N} \binom{r^+(n)}{2} \gg N^{1/3} \log^4 N$$

Proof.

We begin with the following equality where the 1/2 in front of the right hand sum corresponds to the fact that there are two a, b, c triples for each pair of solutions counted by $\binom{r^+(n)}{2}$:

$$\begin{aligned}
\sum_{n<N} \binom{r^+(n)}{2} &= \frac{1}{2} \sum_{m<N^{1/3}} \# \left\{ a, b, c : \substack{a,b,c>0,\ \gcd(a,b,c)=1, \\ \phi(a,b,c)=(W,X,Y,Z) \\ g=\gcd(W,X,Y,Z),\ W^3+Z^3<g^3\left(\frac{N}{m^3}\right), \\ W,Z,-X,-Y\geq 0} \right\} \\
&\gg \sum_{m\leq N^{1/6}} \left(\frac{N}{m^3}\right)^{1/3} \log^3\left(\frac{N}{m^3}\right) \\
&\gg N^{1/3} \log^3 N \sum_{m\leq N^{1/6}} \frac{1}{m} \\
&\gg N^{1/3} \log^4 N. \quad \blacksquare
\end{aligned}$$

Chapter 7

An Upper Bound

As we did with the theorems concerning the lower bounds, in the previous chapter, we'll first prove the theorem concerning primitive solutions. Note that this theorem only counts solutions for which the $\gcd(W, X, Y, Z)$ is small. In order to complete the upper bound, we would need to be able to handle larger values for the gcd. In fact, to account for all taxicab numbers where the integers involved are all positive we proved in chapter four that we would need to deal with gcd's of size $N^{2/3}$ rather than just up to $N^{1/6}$ as in this theorem.

Theorem 7.1:

$$\#\left\{ a,b,c : \begin{array}{c} a,b,c>0, \quad \gcd(a,b,c)=1, \\ \phi(a,b,c) = (W,X,Y,Z) \\ G = \gcd(W,X,Y,Z), \quad G < N^{1/6} \\ W^3 + Z^3 < G^3 N \end{array} \right\} \ll N^{1/3}\log^3 N$$

Proof. First consider a, b, c so that $G = \gcd(W, X, Y, Z) < N^{1/6}$. We will first re-write G as, $G = Mg$ where $M = 2^{e_1}3^{e_2}$ and $\gcd(g, 6) = 1$. Using Theorem 3.1, we have shown that the choices for M are 1,3,8,9,24,72. We will then split the count based on the size of a, b, c. Note that the values for m in the following expression are related to those arising as M and this relationship also comes from Theorem 3.1.

$$\#\left\{a,b,c: \begin{array}{c} a,b,c>0,\quad \gcd(a,b,c)=1, \\ \phi(a,b,c)=(W,X,Y,Z) \\ G=\gcd(W,X,Y,Z),\quad G<N^{1/6} \\ W^3+Z^3<G^3N \end{array}\right\}$$

$$\ll \sum_{\substack{g<N^{1/6}\\(g,6)=1}} \sum_{m\in\{1,2,3,4,6,9,12,18,36\}} \sum_{\substack{\alpha\beta\gamma=mg\\(\alpha,\beta)=(\alpha,\gamma)=1\\(\beta,\gamma)=1,3}} \mathsf{D}(\alpha,\beta,\gamma,g) \tag{7.1}$$

where:

$$D(\alpha,\beta,\gamma,g)=\#\left\{a,b,c>0: \begin{array}{c} (a,b,c)=1,\quad \alpha=(a,c^2+3b^2), \\ \beta=(b,c^2+3a^2),\ \gamma=(c,b^2+3a^2) \\ mg=\alpha\beta\gamma,\ W^3+Z^3<(72g)^3N, \\ \gcd(W,X,Y,Z)=g,3g,8g,9g,24g,72g \end{array}\right\}$$

Case 1: $b,c<a$

For this case, $K\asymp a^9$. So we can write:

$$\begin{aligned}
D(\alpha,\beta,\gamma,g) &\leq \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \sum_{\substack{c<a\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2\\ (a,b,c)=1\\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1\\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1\\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1 \\
&\leq \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \sum_{\substack{c<a\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2}} 1 \\
&= \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \left(\frac{a}{\alpha\beta\gamma}+O(1)\right)\rho(\alpha\beta) \\
&= \frac{\rho(\alpha\beta)}{g} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} 1 \quad + \quad O\left(\rho(\alpha\beta) \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} 1\right)
\end{aligned}$$

$$
\begin{aligned}
&= \frac{\rho(\alpha\beta)}{g} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a\left(\frac{a}{\beta\gamma} + O(1)\right)\rho(\gamma) \\
&\qquad\qquad + O\left(\rho(\alpha\beta) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} \left(\frac{a}{\beta\gamma}+1\right)\rho(\gamma)\right) \\
&= \frac{\rho(g)}{g\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a^2 + O\left(\frac{\rho(g)}{g} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a\right) + O\left(\frac{\rho(g)}{\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a\right) \\
&\qquad\qquad + O\left(\rho(g) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} 1\right) \\
&= \frac{\rho(g)}{g\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a^2 + O\left(\frac{\rho(g)}{\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} a\right) + O\left(\rho(g) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha | a}} 1\right) \\
&= \frac{\rho(g)\alpha^2}{g\beta\gamma} \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^2 + O\left(\frac{\rho(g)\alpha}{\beta\gamma} \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d\right) \\
&\qquad\qquad + O\left(\rho(g) \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} 1\right) \\
&= \frac{\rho(g)\alpha^2}{g\beta\gamma}\left(\frac{gN^{1/3}}{\alpha^3} + O\left(\frac{g^{2/3}N^{2/9}}{\alpha^2}\right)\right) + O\left(\frac{\rho(g)\alpha}{\beta\gamma}\frac{g^{2/3}N^{2/9}}{\alpha^2}\right) \\
&\qquad\qquad O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right) \\
&= \frac{N^{1/3}\rho(g)}{g} + O\left(\frac{N^{2/9}\rho(g)}{g^{1/3}}\right) + O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right)
\end{aligned}
$$

And so for $g < N^{1/6}$ we have:

$$D(\alpha,\beta,\gamma,g) \ll \frac{N^{1/3}\rho(g)}{g}$$

Case 2: $b \le a \le c$ (and similarly for $c \le a \le b$)

For this case, $K \asymp ac^8 \gg a^9$. So we can write:

$$
\begin{aligned}
D(\alpha,\beta,\gamma,g) &\le \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \sum_{\substack{a<c<\left(\frac{g^3N}{a}\right)^{1/8}\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2\\ (a,b,c)=1\\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1\\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1\\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1 \\
&\le \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \sum_{\substack{c<\left(\frac{g^3N}{a}\right)^{1/8}\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2}} 1 \\
&= \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} \left(\frac{g^{3/8}N^{1/8}}{\alpha\beta\gamma a^{1/8}} + O(1)\right)\rho(\alpha\beta) \\
&= \frac{N^{1/8}\rho(\alpha\beta)}{g^{5/8}} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{-1/8} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} 1 \\
&\qquad + O\left(\rho(\alpha\beta) \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<a\\ \beta|b\\ \gamma|b^2+3a^2}} 1\right) \\
&= \frac{N^{1/8}\rho(\alpha\beta)}{g^{5/8}} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{-1/8} \left(\frac{a}{\beta\gamma} + O(1)\right)\rho(\gamma) \\
&\qquad + O\left(\rho(\alpha\beta) \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \left(\frac{a}{\beta\gamma} + 1\right)\rho(\gamma)\right) \\
&= \frac{N^{1/8}\rho(g)}{g^{5/8}\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{7/8} + O\left(\frac{N^{1/8}\rho(g)}{g^{5/8}} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{-1/8}\right)
\end{aligned}
$$

$$+\ O\left(\frac{\rho(g)}{\beta\gamma}\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a\right)\ +\ O\left(\rho(g)\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} 1\right)$$

$$= \frac{N^{1/8}\rho(g)\alpha^{7/8}}{g^{5/8}\beta\gamma}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{7/8} + O\left(\frac{N^{1/8}\rho(g)}{g^{5/8}\alpha^{1/8}}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{-1/8}\right)$$

$$+\ O\left(\frac{\rho(g)\alpha}{\beta\gamma}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d\right)\ +\ O\left(\rho(g)\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} 1\right)$$

$$= \frac{N^{1/8}\rho(g)\alpha^{7/8}}{g^{5/8}\beta\gamma}\left(\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{15/8}\ +\ O\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{7/8}\right)$$

$$+O\left(\frac{N^{1/8}\rho(g)}{g^{5/8}\alpha^{1/8}}\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{7/8}\right)$$

$$+\ O\left(\frac{\rho(g)\alpha}{\beta\gamma}\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{2}\right)\ +\ O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right)$$

$$= \frac{N^{1/3}\rho(g)}{g}\ +\ O\left(\frac{N^{2/9}\rho(g)}{g^{1/3}}\right)\ +\ O\left(\frac{N^{1/9}g^{1/3}\rho(g)}{\alpha}\right)$$

Like in case 1, for $g < N^{1/6}$:

$$D(\alpha,\beta,\gamma,g) \ll \frac{N^{1/3}\rho(g)}{g}$$

Case 3: $a < b < c$ where $c - b < a$ (and similarly for $a < c < b$ where $b - c < a$)

For this case, $K \asymp a^3c^4b^2 \asymp a^3b^6 \gg a^9$. So we can write:

$$D(\alpha,\beta,\gamma,g) \leq \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}}\ \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \beta|b\\ \gamma|b^2+3a^2}}\ \sum_{\substack{b<c<b+a\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2\\ (a,b,c)=1\\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1\\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1\\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1$$

$$\leq \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}}\ \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \beta|b\\ \gamma|b^2+3a^2}}\ \sum_{\substack{b<c<b+a\\ \gamma|c\\ \alpha|c^2+3b^2\\ \beta|c^2+3a^2}} 1$$

$$
\begin{aligned}
&= \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \beta|b\\ \gamma|b^2+3a^2}} \left(\frac{a}{\alpha\beta\gamma}+O(1)\right)\rho(\alpha\beta)\\
&= \frac{\rho(\alpha\beta)}{g} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \beta|b\\ \gamma|b^2+3a^2}} 1 \;+\; O\left(\rho(\alpha\beta) \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \beta|b\\ \gamma|b^2+3a^2}} 1\right)\\
&= \frac{\rho(\alpha\beta)}{g} \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a\left(\left(\frac{g^3N}{a^3}\right)^{1/6}\frac{1}{\beta\gamma}+O(1)\right)\rho(\gamma)\\
&\qquad\qquad + O\left(\rho(\alpha\beta)\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}}\left(\left(\frac{g^3N}{a^3}\right)^{1/6}\frac{1}{\beta\gamma}+1\right)\rho(\gamma)\right)\\
&= \frac{N^{1/6}\rho(g)}{g^{1/2}\beta\gamma}\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{1/2} \;+\; O\left(\frac{\rho(g)}{g}\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a\right)\\
&\qquad\qquad + O\left(\frac{N^{1/6}g^{1/2}\rho(g)}{\beta\gamma}\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} a^{-1/2}\right)\\
&\qquad\qquad + O\left(\rho(g)\sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} 1\right)\\
&= \frac{N^{1/6}\rho(g)\alpha^{1/2}}{g^{1/2}\beta\gamma}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{1/2} \;+\; O\left(\frac{\rho(g)\alpha}{g}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d\right)\\
&\qquad\qquad + O\left(\frac{N^{1/6}g^{1/2}\rho(g)}{\beta\gamma\alpha^{1/2}}\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{-1/2}\right)\\
&\qquad\qquad + O\left(\rho(g)\sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} 1\right)
\end{aligned}
$$

$$\begin{aligned}
&= \frac{N^{1/6}\rho(g)\alpha^{1/2}}{g^{1/2}\beta\gamma}\left(\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{3/2} + O\left(\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{1/2}\right)\right) \\
&\qquad + O\left(\frac{\rho(g)\alpha}{g}\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{2}\right) \\
&\qquad + O\left(\frac{N^{1/6}g^{1/2}\rho(g)}{\beta\gamma\alpha^{1/2}}\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{1/2}\right) \\
&\qquad + O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right) \\
&= \frac{N^{1/3}\rho(g)}{g} + O\left(\frac{N^{2/9}\rho(g)}{g^{1/3}}\right) + O\left(\frac{N^{1/9}g^{1/3}\rho(g)}{\alpha}\right)
\end{aligned}$$

As in the first two cases, for $g < N^{1/6}$:

$$D(\alpha,\beta,\gamma,g) \ll \frac{N^{1/3}\rho(g)}{g}$$

Note that for the case in parenthesis, $a < c < b$ where $b - c < a$, we arrive at the same sequence of equations after the first two as we'll show below.

First note that $K \asymp a^3b^6 \gg a^9$, and so:

$$\begin{aligned}
D(\alpha,\beta,\gamma,g) &\le \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6} \\ \beta|b \\ \gamma|b^2+3a^2}} \sum_{\substack{\max(a,b-a)<c<b \\ \gamma|c \\ \alpha|c^2+3b^2 \\ \beta|c^2+3a^2 \\ (a,b,c)=1 \\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1 \\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1 \\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1 \\
&\le \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \sum_{\substack{b<\left(\frac{g^3N}{a^3}\right)^{1/6} \\ \beta|b \\ \gamma|b^2+3a^2}} \sum_{\substack{b-a<c<b \\ \gamma|c \\ \alpha|c^2+3b^2 \\ \beta|c^2+3a^2}} 1
\end{aligned}$$

We then continue the sequence as above to arrive at the same count.

<u>Case 4:</u> $a < b < c$ where $c - b \ge a$ (and similarly for $a < c < b$ where $b - c \ge a$)

For this case, $K \asymp ac^6(c-b)^2 \gg a(c-b)^8 \gg a^9$. As before we can bound a above by $g^{1/3}N^{1/9}$. Since $(c-b) > a$ we can bound c by $\left(\frac{g^3N}{a^3}\right)^{1/6}$, by noting that $K \asymp ac^6(c-b)^2 \gg a^3c^6$. Once a and c are chosen, we bound b as:

$$c - \left(\frac{g^3N}{ac^6}\right)^{1/2} < b < c - a$$

Note that for small c, namely $c < \left(\frac{g^3N}{a}\right)^{1/8}$, this lower bound for b is negative, while we have previously restricted b to positive numbers. We then must split our count and bound $D(\alpha,\beta,\gamma,g)$ as follows:

$$
\begin{aligned}
D(\alpha,\beta,\gamma,g) \;\le\; & \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{c<\left(\frac{g^3N}{a}\right)^{1/8}\\ \gamma|c\\ \beta|c^2+3a^2}} \; \sum_{\substack{b<c\\ \beta|b\\ \alpha|c^2+3b^2\\ \gamma|b^2+3a^2\\ (a,b,c)=1\\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1\\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1\\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1 \\
& + \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{\left(\frac{g^3N}{a}\right)^{1/8}\le c<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \gamma|c\\ \beta|c^2+3a^2}} \; \sum_{\substack{c-\left(\frac{g^3N}{ac^6}\right)^{1/2}<b<c\\ \beta|b\\ \alpha|c^2+3b^2\\ \gamma|b^2+3a^2\\ (a,b,c)=1\\ \left(\frac{c}{\gamma},\frac{b^2+3a^2}{\gamma}\right)=1\\ \left(\frac{a}{\alpha},\frac{c^2+3b^2}{\alpha}\right)=1\\ \left(\frac{b}{\beta},\frac{c^2+3a^2}{\beta}\right)=1}} 1
\end{aligned}
$$

$$
\begin{aligned}
\le\; & \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{c<\left(\frac{g^3N}{a}\right)^{1/8}\\ \gamma|c\\ \beta|c^2+3a^2}} \; \sum_{\substack{b<c\\ \beta|b\\ \alpha|c^2+3b^2\\ \gamma|b^2+3a^2}} 1 \\
& + \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{\left(\frac{g^3N}{a}\right)^{1/8}\le c<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \gamma|c\\ \beta|c^2+3a^2}} \; \sum_{\substack{c-\left(\frac{g^3N}{ac^6}\right)^{1/2}<b<c\\ \beta|b\\ \alpha|c^2+3b^2\\ \gamma|b^2+3a^2}} 1 \\
=\; & \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{c<\left(\frac{g^3N}{a}\right)^{1/8}\\ \gamma|c\\ \beta|c^2+3a^2}} \left(\frac{c}{\alpha\beta\gamma}+O(1)\right)\rho(\alpha\gamma) \\
& + \sum_{\substack{a<g^{1/3}N^{1/9}\\ \alpha|a}} \; \sum_{\substack{\left(\frac{g^3N}{a}\right)^{1/8}\le c<\left(\frac{g^3N}{a^3}\right)^{1/6}\\ \gamma|c\\ \beta|c^2+3a^2}} \left(\frac{1}{\alpha\beta\gamma}\left(\frac{g^3N}{ac^6}\right)^{1/2}+O(1)\right)\rho(\alpha\gamma)
\end{aligned}
$$

$$
\begin{aligned}
&= \frac{\rho(\alpha\gamma)}{g} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \sum_{\substack{c<\left(\frac{g^3N}{a}\right)^{1/8} \\ \gamma|c \\ \beta|c^2+3a^2}} c \\
&\qquad + \rho(\alpha\gamma)N^{1/2}g^{1/2} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/2} \sum_{\substack{\left(\frac{g^3N}{a}\right)^{1/8} \le c < \left(\frac{g^3N}{a^3}\right)^{1/6} \\ \gamma|c \\ \beta|c^2+3a^2}} c^{-3} \\
&\qquad + O\left(\rho(\alpha\gamma) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \sum_{\substack{c<\left(\frac{g^3N}{a^3}\right)^{1/6} \\ \gamma|c \\ \beta|c^2+3a^2}} 1\right) \\
&= \frac{\rho(\alpha\gamma)}{g} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \left(\frac{\rho(\beta)}{\beta\gamma}\left(\frac{g^3N}{a}\right)^{1/4} + O\left(\rho(\beta)\left(\frac{g^3N}{a}\right)^{1/8}\right)\right) \\
&\qquad + \rho(\alpha\gamma)N^{1/2}g^{1/2} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/2} \left(\frac{\rho(\beta)}{\beta\gamma}\left(\left(\frac{g^3N}{a}\right)^{-1/4} - \left(\frac{g^3N}{a^3}\right)^{-1/3}\right)\right. \\
&\qquad\qquad \left. + O\left(\rho(\beta)\left(\frac{g^3N}{a}\right)^{-3/8}\right)\right) \\
&\qquad + O\left(\rho(\alpha\gamma) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} \left(\frac{\rho(\beta)}{\beta\gamma}\left(\frac{g^3N}{a^3}\right)^{1/6} + \rho(\beta)\right)\right) \\
&\le \frac{\rho(g)N^{1/4}}{g^{1/4}\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/4} + O\left(\frac{\rho(g)N^{1/8}}{g^{5/8}} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/8}\right) \\
&\qquad + \frac{\rho(g)N^{1/4}}{g^{1/4}\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/4} + O\left(\frac{\rho(g)N^{1/8}}{g^{5/8}} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/8}\right) \\
&\qquad + O\left(\frac{\rho(g)N^{1/6}g^{1/2}}{\beta\gamma} \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} a^{-1/2}\right) + O\left(\rho(g) \sum_{\substack{a<g^{1/3}N^{1/9} \\ \alpha|a}} 1\right)
\end{aligned}
$$

$$
\begin{aligned}
= \; & \frac{2\rho(g)N^{1/4}}{g^{1/4}\beta\gamma\alpha^{1/4}} \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{-1/4} + O\left(\frac{\rho(g)N^{1/8}}{g^{5/8}\alpha^{1/8}} \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{-1/8}\right) \\
& + O\left(\frac{\rho(g)N^{1/6}g^{1/2}}{\beta\gamma\alpha^{1/2}} \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} d^{-1/2}\right) + \; O\left(\rho(g) \sum_{d<\frac{g^{1/3}N^{1/9}}{\alpha}} 1\right)
\end{aligned}
$$

$$
\begin{aligned}
= \; & \frac{2\rho(g)N^{1/4}}{g^{1/4}\beta\gamma\alpha^{1/4}} \left(\left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{3/4} + O(1)\right) + O\left(\frac{\rho(g)N^{1/8}}{g^{5/8}\alpha^{1/8}} \left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{7/8}\right) \\
& + O\left(\frac{\rho(g)N^{1/6}g^{1/2}}{\beta\gamma\alpha^{1/2}} \left(\frac{g^{1/3}N^{1/9}}{\alpha}\right)^{1/2}\right) + \; O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right) \\
= \; & \frac{2\rho(g)N^{1/3}}{g} + O\left(\frac{\rho(g)N^{1/4}}{g^{1/4}\beta\gamma\alpha^{1/4}}\right) + \; O\left(\frac{\rho(g)N^{2/9}}{g^{1/3}}\right) + \; O\left(\rho(g)\frac{g^{1/3}N^{1/9}}{\alpha}\right)
\end{aligned}
$$

As in the previous three cases, for $g < N^{1/6}$:

$$
D(\alpha,\beta,\gamma,g) \ll \frac{N^{1/3}\rho(g)}{g}
$$

Having handled all four cases, we return to (7.1) for $g < N^{1/6}$:

$$
\#\{a,b,c \text{ coprime } : k(a,b,c) < N\}
$$

$$
\begin{aligned}
& \ll \sum_{\substack{g<N^{1/6} \\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g \\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \mathsf{D}(\alpha,\beta,\gamma) \\
& \ll \sum_{\substack{g<N^{1/6} \\ (g,6)=1}} \sum_{\substack{\alpha\beta\gamma=g \\ \alpha,\beta,\gamma \text{ pairwise coprime}}} \frac{N^{1/3}\rho(g)}{g} \\
& \ll N^{1/3} \sum_{\substack{g<N^{1/6} \\ (g,6)=1}} \frac{3^{\omega(g)}\rho(g)}{g}
\end{aligned}
$$

Using Proposition 6.5, we can see that for the case $g < N^{1/6}$ we have finished the proof. ∎

Chapter 8

Ramanujan's Parametrization

Ramanujan [16] gave a different parametrization for solutions to (1.3) which is not a complete parametrization. The equations are as follows:

$$\begin{aligned} W_r &= W_r(m,n) = 6m^2 - 4mn + 4n^2 \\ X_r &= X_r(m,n) = -4m^2 + 4mn - 6n^2 \\ Y_r &= Y_r(m,n) = -5m^2 + 5mn + 3n^2 \\ Z_r &= Z_r(m,n) = -3m^2 - 5mn + 5n^2 \end{aligned}$$

In this chapter, we will discuss how this parametrization compares with the complete parametrization of Euler discussed in the previous chapters. The main result comparing these two parametrizations is Lemma 8.4 which shows that all of the solutions generated by Ramanujan's parametrization correspond to integer triples (a,b,c) in Euler's parametrization inducing large gcd's.

Since $\gcd(w,x,y,z)$ played such a substantial role in the complete rational parametrization discussed in previous chapters, we ought to describe the gcd's for this parametrization as well.

Lemma 8.1: *Using the parametrization of Ramanujan, with* $\gcd(m,n) = 1$*, then* $\gcd(w,x,y,z)$ *divides 21.*

Proof. Let $g = \gcd(W_r, X_r, Y_r, Z_r)$. We first show that:

$$\gcd(g,m) = \gcd(g,n) = 1$$

Suppose p is a prime dividing $\gcd(g,m)$. Since $p \mid \gcd(W_r, X_r, Y_r, Z_r)$ then we also have $p \mid \gcd(5n^2, 6n^2, 3n^2, 4n^2) = n^2$, hence p would divide n, which contradicts the hypothesis $\gcd(m,n) = 1$. Similarly, p can not divide n.

Certainly g must divide $9Z_r + Y_r + 8X_r = -8m(8m+n)$. From above, since $\gcd(g,m) = 1$, either $p = 2$ or p divides $8m+n$. Looking at the equations modulo 2 we see that:

$$Z_r \equiv m^2 + mn + n^2 \pmod 2$$

which has no solutions if $\gcd(m,n) = 1$. So 2 can not divide g. Hence g divides $8m+n$. Letting $n \equiv -8m \pmod g$, and substituting this into our equations we see that modulo g:

$$\begin{aligned} W_r &\equiv 294m^2 \\ X_r &\equiv -420m^2 \\ Y_r &\equiv 147m^2 \\ Z_r &\equiv 357m^2 \end{aligned}$$

From this we see $g \mid \gcd(357m^2, 147m^2, 420m^2, 294m^2) = 21m^2$, which with $\gcd(g,m) = 1$ completes the proof. ∎

We can now begin to describe the types of solutions that this parametrization gives with respect to the complete parametrization. The two sets of (a,b,c) which yield the parametrization of Ramanujan are:

$$\begin{aligned} (a_1, b_1, c_1) &= (13m^2 - 23mn + 13n^2, 14m^2 - 14n^2, 19m^2 - 11mn + 19n^2) \\ (a_2, b_2, c_2) &= (m^2 - mn + n^2, m^2 + mn + n^2, 2m^2 - 2n^2). \end{aligned}$$

Lemma 8.2: *Let* $(a_1, b_1, c_1) = (13m^2 - 23mn + 13n^2, 14m^2 - 14n^2, 19m^2 - 11mn + 19n^2)$*. If* $(m,n) = 1$*, then* $\gcd(a_1, b_1, c_1)$ *divides 147.*

Proof. Let $g = \gcd(a_1, b_1, c_1)$. We first show that $\gcd(g,m) = \gcd(g,n) = 1$. Suppose p divides $\gcd(g,m)$. Then

$$p \mid \gcd(13n^2, 14n^2, 19n^2) = n^2$$

and hence $p \mid n$, which contradicts $\gcd(m,n) = 1$. Similarly for $p \mid \gcd(g,n)$. Also note that $2 \nmid n$, since $2 \mid (13m^2 - 23mn + 13n^2)$ if and only if $2 \mid \gcd(m,n)$.

Certainly g must divide $13c_1 - 19a_1 = 294mn$. Since from above $\gcd(2,g) = \gcd(m,g) = \gcd(n,g) = 1$, we must have g dividing 147. ∎

Lemma 8.3: *Let* $(a_2, b_2, c_2) = (m^2 - mn + n^2, m^2 + mn + n^2, 2m^2 - 2n^2)$. *If* $\gcd(m,n) = 1$, *then* $\gcd(a_2, b_2, c_2) = 1$.

Proof. Let $g = \gcd(a_2, b_2, c_2)$. We first show that $\gcd(g,m) = \gcd(g,n) = 1$. Suppose p divides $\gcd(g,m)$. Then p must divide $\gcd(n^2, 2n^2) = n^2$, and hence $p \mid n$, which contradicts $\gcd(m,n) = 1$. Similarly for $p \mid \gcd(g,n)$. Also note that $2 \nmid g$, since $2 \mid (m^2 + mn + n^2)$ if and only if $2 \mid \gcd(m,n)$.

Certainly g must divide $b_2 - a_2 = 4mn$. But since $\gcd(2,g) = \gcd(m,g) = \gcd(n,g) = 1$, we must have $g = 1$. ∎

When working with the complete parametrization, we only considered a, b, c triples for which $\gcd(a,b,c) = 1$. So, to properly make comparisons we would have to divide out the gcd described in Lemma 8.2 to get the proper type of triples. But, since this gcd is bounded by a small constant, we can still use these expressions for a_i, b_i, c_i to prove the following lemma:

Lemma 8.4: *Using either* (a_1, b_1, c_1) *or* (a_2, b_2, c_2), *then the* w, x, y, z *which arise from the complete parametrization* ϕ *described in chapter two have*

$$\gcd(w, x, y, z) \asymp M^4$$

where $M = \max(m, n)$. *Further, the primitive* k *which is associated to these* (a_i, b_i, c_i) *has size* $\asymp M^6$.

Proof. By simply substituting the expressions for a_i, b_i, c_i into the expressions for W, X, Y, Z given by the parametrization (2.4) we have

$$\begin{aligned}
(a_1, b_1, c_1) &\rightarrow (g_1 W_r, g_1 X_r, g_1 Y_r, g_1 Z_r) \\
(a_2, b_2, c_2) &\rightarrow (g_2 W_r, g_2 Y_r, g_2 X_r, g_2 Z_r)
\end{aligned}$$

where:

$$\begin{aligned} g_1 &= 56(19m^2 - 11mn + 19n^2)(13m^2 - 23mn + 13n^2) \\ g_2 &= 8(m^2 - mn + n^2)(m^2 + mn + n^2) \end{aligned}$$

Note that the gcd factors, g_1, g_2 can be re-written as:

$$g_1 = 56a_1c_1 \;\; g_2 = 8a_2b_2$$

Since by Lemma 8.1, $\gcd(W_r, X_r, Y_r, Z_r)$ divides 147, letting $M = \max(m, n)$ we have that $\gcd(W, X, Y, Z) \asymp g_i \asymp M^4$.

Finally, factoring our expression for $W_r^3 + Z_r^3$ we see that $k \asymp M^6$:

$$k \asymp 63(m^2 + mn + n^2)(3m^2 - 3mn + n^2)(m^2 - 3mn + 3n^2) \quad \blacksquare$$

Note that re-arranging the parametrization given by Ramanujan, switching the expressions for y and z for example, leads to essentially the same sequence of lemmas. The only change is slightly modifying the constants the gcd's divide in Lemmas 8.2 and 8.3.

Another interesting property of this parametrization is shown in the following lemma.

Lemma 8.5: *Using the parametrization given above:*

$$\begin{aligned} W_r(m,n) &= W_r(m, m-n) \\ Z_r(m,n) &= Z_r(m, m-n) \end{aligned}$$

Moreover, unless $n = m - n$ or $m = 0$ we also have:

$$\begin{aligned} X_r(m,n) &\neq X_r(m, m-n) \\ Y_r(m,n) &\neq Y_r(m, m-n) \end{aligned}$$

Proof. By simply substituting in the given expressions:

$$\begin{aligned} W_r(m, m-n) &= 6m^2 - 4m(m-n) + 4(m-n)^2 \\ &= 6m^2 - 4m^2 + 4mn + 4m^2 - 8mn + 4n^2 \\ &= 6m^2 - 4mn + 4n^2 \\ &= W_r(m,n) \end{aligned}$$

Similarly for Z_r. This completes the first part of the lemma. To see the second part we calculate:

$$\begin{aligned} X_r(m,n) - X_r(m,m-n) &= -4m^2 + 4mn - 6n^2 - (-4m^2 + 4m(m-n) - 6(m-n)^2) \\ &= 4mn - (-2m^2 + 8mn) \\ &= 2m(m-2n) \end{aligned}$$

And indeed this expression equals 0 if and only if either $m = 0$ or $n = m - n$. The same argument follows for Y_r. ∎

Note that although this gives us a place to look for integers with at least ***three*** representations as the sum of two integer cubes, it does not guarantee this property. Although the $\gcd(W_r, X_r, Y_r, Z_r)$ is bounded by 21, the solution generated by (m, n) may have a different gcd from that generated by $(m, m-n)$.

Finally, we mentioned earlier that this parametrization gives us a family of examples which yields large gcd's, even for the case where $W, Z, -X, -Y$ are all positive. The following lemma gives a family of (m, n) pairs yielding such solutions.

Lemma 8.6: *Letting $n = -2m$ then $W_r, Z_r > 0$ and $X_r, Y_r < 0$.*

Proof. We can see that W_r is always positive as follows:

$$W_r = 6m^2 - 4mn + 4n^2 = (2n - m)^2 + 5m^2$$

Similarly, X_r is always negative.

By simply making the substitution described in the lemma we have

$$\begin{aligned} Z_r &= 27m^2 \\ Y_r &= -m^2 \end{aligned}$$

hence indeed $Z_r > 0$ and $Y_r < 0$. ∎

Chapter 9

Generalizing Ramanujan's Parametrization

In this chapter, we generalize Ramanujan's parametrization given in the previous chapter. We discuss some of the interesting properties this generalization shares with Ramanujan's original parametrization. One question which remains is whether or not the solutions given by this generalization also have the property that the associated (a, b, c) triples using Euler's parametrization induce large gcd's via Euler's parametrization.

First we recall Ramanujan's Parametrization from the previous chapter:

$$\begin{aligned} W_r &= 6m^2 - 4mn + 4n^2 \\ X_r &= -4m^2 + 4mn - 6n^2 \\ Y_r &= -5m^2 + 5mn + 3n^2 \\ Z_r &= -3m^2 - 5mn + 5n^2 \end{aligned}$$

Then for any m, n this is indeed a solution to:

$$W^3 + X^3 + Y^3 + Z^3 = 0 \tag{9.1}$$

We first note that the leading coefficients in these expressions given by the parametrization are themselves a solution to (9.1), that is:

$$6^3 - 4^3 - 5^3 - 3^3 = 0$$

So, to generalize our parametrization, we'll start with a primitive solution (A, B, C, D) to (9.1). Then our generalized parametrization might be expressed as:

$$\begin{aligned} W_g &= Am^2 + rmn - Bn^2 \\ X_g &= Bm^2 - rmn - An^2 \\ Y_g &= Cm^2 + smn - Dn^2 \\ Z_g &= Dm^2 - smn - Cn^2 \end{aligned}$$

With this as our form, we can prove the following proposition.

Proposition 9.1: *Given integers A, B, C, D satisfying (9.1), then*

$$(Am^2 + Rmn - Bn^2)^3 + (Bm^2 - Rmn - An^2)^3$$
$$+(Cm^2 + Smn - Dn^2)^3 + (Dm^2 - Smn - Cn^2)^3 = 0$$

for some rational numbers R, S if and only if

$$-(A + B)(C + D) = T^2 \in \mathbf{Z}^2$$

in which case $R = \frac{D^2-C^2}{T}$ and $S = \frac{A^2-B^2}{T}$.

Proof. We begin by deriving conditions for R and S. By substituting W_g, X_g, Y_g, Z_g into (9.1) and simplifying, we get the following two conditions:

$$R(A^2 - B^2) + S(C^2 - D^2) = 0 \tag{9.2}$$
$$R^2(A + B) + S^2(C + D) = AB(A + B) + CD(C + D) \tag{9.3}$$

While we might like for R and S to be integers, it suffices for them to be rationals at which point we can clear denominators. From (9.2) we see that we can write

$$R = -\frac{t_1}{t_2}(C^2 - D^2) \qquad S = \frac{t_1}{t_2}(A^2 - B^2)$$

for some integers t_1 and t_2.

Substituting these expressions for r and s into (9.3) we have:

$$\frac{t_1^2}{t_2^2}\left(C^2 - D^2\right)^2(A + B) + \frac{t_1^2}{t_2^2}\left(A^2 - B^2\right)(C + D) = AB(A + B) + CD(C + D)$$

Solving for $\frac{t_1^2}{t_2^2}$ we have:

$$\begin{aligned}
\frac{t_1^2}{t_2^2} &= \frac{AB(A+B)+CD(C+D)}{(A+B)(C+D)\left((C-D)\left(C^2-D^2\right)+(A-B)\left(A^2-B^2\right)\right)} \\
&= \frac{AB(A+B)+CD(C+D)}{(A+B)(C+D)\left(\left(A^3+B^3+C^3+D^3\right)-\left(AB(A+B)+CD(C+D)\right)\right)} \\
&= \frac{AB(A+B)+CD(C+D)}{(A+B)(C+D)\left(-\left(AB(A+B)+CD(C+D)\right)\right)} \\
&= \frac{1}{-(A+B)(C+D)}
\end{aligned}$$

So, in order for the parametrization to produce integer solutions to (9.1), we must have $-(A+B)(C+D)$ be a perfect integer square. In which case, by setting $t_1 = 1$ and $t_2 = \sqrt{-(A+B)(C+D)}$, we have R and S of the form required by the proposition. ∎

For the parametrization of Ramanujan given to start this chapter, we have:

$$A = 6, \quad B = -4, \quad C = -5, \quad D = -3$$

and so $-(6-4)(-5-3) = 16$ which is indeed a perfect integer square.

One interesting property of this generalization, is that the salient property $-(A+B)(C+D) \in \mathbf{Z}^2$ is preserved by the parametrization. That is, for any $m, n \in \mathbf{Z}$, we have:

$$\begin{aligned}
-(W_g+X_g)(Y_g+Z_g) &= -\big((A+B)(m^2-n^2)\big)\big((C+D)(m^2-n^2)\big) \\
&= -(A+B)(C+D)(m^2-n^2)^2 \\
&\in \mathbf{Z}^2
\end{aligned}$$

We might also like to characterize the a, b, c which yield such a parametrization. By substituting our complete parametrization, we have:

$$\begin{aligned}
W + X &= 2b(3b^2+(c-3a)^2) \\
Y + Z &= -2b(3b^2+(c+3a)^2)
\end{aligned}$$

So, in order for $-(W+X)(Y+Z)$ to be a perfect integer square, we can let:

$$\begin{aligned} 3b^2 + (c-3a)^2 &= mL_1^2 \\ 3b^2 + (c+3a)^2 &= mL_2^2 \end{aligned} \tag{9.4}$$

for some integers m, L_1, L_2.

We might like to use these equations to give complete conditions on a, b, c which give rise to such solutions, but as of yet, such complete conditions remain unproven. We can use a special case of these equations though to determine some a, b, c which satisfy this integer square conditions. Begin by rewriting these equations:

$$\begin{aligned} 3B^2 + N_1^2 &= mL_1^2 \\ 3B^2 + N_2^2 &= mL_2^2 \end{aligned} \tag{9.5}$$

There is then a one-to-one correspondence between integer solutions to (9.4) and integer solutions to (9.5) if we restrict $N_1 \equiv N_2 \pmod 6$. Note that the two equations in (9.5) are indeed the same, hence we can also say that in order to satisfy (9.5) we need two different solutions to

$$mL^2 = 3B^2 + N^2 \tag{9.6}$$

where the value of B is the same.

We will now begin with one such solution, and derive a second one. So suppose we have a solution to (9.6). Then, by cubing both sides of this expression and reorganizing terms, we have:

$$m\left(mL^3\right)^2 = 3\left(3BN^2 - 3B^3\right)^2 + \left(N^3 - 9NB^2\right)^2$$

This then is another solution to (9.6). In order to use these two equations for (9.5) we must multiply our original solution (9.6) by $(3N^2 - 2B^2)^2$, so that the B term in both equations agree. Thus we have:

$$\begin{aligned} m\left(3L\left(N^2 - B^2\right)\right)^2 &= 3\left(3B\left(N^2 - B^2\right)\right)^2 + \left(3N\left(N^2 - B^2\right)\right)^2 \\ m\left(mL^3\right)^2 &= 3\left(3B\left(N^2 - B^2\right)\right)^2 + \left(N\left(N^2 - 9B^2\right)\right)^2 \end{aligned}$$

We can then use these to find the corresponding values of a, b, c. So, let:

$$\begin{aligned} c + 3a = N_1 &= 3N(N^2 - B^2) \\ c - 3a = N_2 &= N(N^2 - 9B^2) \end{aligned}$$

Then we have:

$$\begin{aligned} a &= \frac{N_1 - N_2}{6} = \frac{N(N^2 + 3B^2)}{3} \\ b &= 3B(N^2 - B^2) \\ c &= \frac{N_1 + N_2}{2} = N(2N^2 - 6B^2) \end{aligned}$$

Thus, in order for a, b, c to be integers, we need to have $3 \mid N$.

Therefore, by choosing integers B, N with $3 \mid N$, we can generate a solution to (9.1) which yields a generalized Ramanujan parametrization.

Another question we might like to investigate, is whether or not this generalized version of Ramanujan's parametrization leads to solutions with large gcds as Ramanujan's original parametrization does. Such a general result also remains unproven.

Bibliography

[1] Harold Davenport, *Multiplicative Number Theory*, Third Edition, Springer, 2000.

[2] Davenport, *On Waring's Problem for Cubes*, Acta Math. **71** (1939), 123-143.

[3] Dickson, *All Integers Except* $23, 239$ *are Sums of Eight Cubes*, Bull. Amer. Math Soc. **45** (1939), 588-591.

[4] Rachel Gar-el and Leonid Vaserstein, *On The Diophantine Equation* $a^3+b^3+c^3+d^3 = 0$, Journal of Number Theory **94**, (2002), 219-223.

[5] G. Hardy, E. Wright, *An Introduction to the Theory of Numbers*, Fifth Edition, Oxford, 1998.

[6] D.R. Heath-Brown, *The Density Of Rational Points On Cubic Surfaces*, Acta Arith. **79**, (1997), 17-30.

[7] C. Hooley, *On The Representations Of A Number As A Sum Of Two Cubes*, Math. Z. **82** (1963), 259-266.

[8] C. Hooley, *On The Numbers That Are Representable As The Sum Of Two Cubes*, J. Reine Angew. Math. **314** (1980), 146-173.

[9] L.K. Hua, *Introduction to Number Theory*, Springer-Verlag, 1982.

[10] Kempner, Math. Annalen, **72** (1912), 387-399.

[11] Landau, Math. Annalen, **66** (1909), 102-105.

[12] L. Leech, *Some Solutions of Diophantine Equations*, Proc. Cambridge Phil. Soc. 1957, 778-780.

[13] Linnik, Comptes Rendus (Doklady) Acad. Sci. USSR **35** (1942), 162.

[14] Emmanuel Peyre and Yuri Tschinkel, *Tamagawa Numbers Of Diagonal Cubic Surfaces of Higher Rank*, Progress in Math **199**, (2001), 275-305.

[15] H. Rademacher, *On the Pragmen-Lindelof theorem and some applications*, Math Z. **72** (1959), 192-204.

[16] S. Ramanujan, *Collected Papers of Srinvasa Ramanujan*, AMS Chelsea Publishing, 1962, 326-394.

[17] R. Rathbun, NMBRTHRY@listserv.nodak.edu, July 16, 2002.

[18] E. Rosenstiel, J.A. Dardis, and C.R. Rosenstiel, *The four least solutions in distinct positive integers of the Diophantine equation* $s = x^3 + y^3 = u^3 + v^3 = m^3 + n^3$, Bulletin Inst. Math. Appl. 27, 1991, 155-157.

[19] J. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer-Verlag, 1991.

[20] E.C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Second Edition, 1986.

[21] R.C. Vaughan and T.D. Wooley, *Waring's Problem: A Survey*, Number Theory for the Millenium, Vol. III, A.K. Peters, 2002, 301-340.

[22] Wieferich, Math. Annalen, **66** (1909), 95-105.

[23] D. Wilson, *The Fifth Taxicab Number is 48988659276962496*, Journal of Integer Sequences 2, 1999.

[24] T.D. Wooley, *Sums Of Two Cubes*, Internat. Math. Res. Notices 1995 **4**, 181-185.