Geometry of Numbers Approach to Small Solutions to the Extended Legendre Equation

by

Laura M. Nunley

(Under the direction of Pete L. Clark)

Abstract

In this paper, the reader will be introduced to quadratic forms, lattices, and the Legendre Equation. We will extend Legendre's equation to multiple variables, and in the cases where $n \geq 4$, attempt to extend Cochrane and Mitchell's proof of the existence of solutions. It will be proven that the proof does not hold for more than three variables.

Index words: Quadratic forms, Legendre equation, Integral Lattices

Geometry of Numbers Approach to Small Solutions to the Extended Legendre Equation

by

Laura M. Nunley

B.S.Ed., Columbus State University, 2008

A Thesis Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Master of Arts

Athens, Georgia

2010

Geometry of Numbers Approach to Small Solutions to the Extended Legendre Equation

by

Laura M. Nunley

Approved:

Major Professor: Pete L. Clark

Committee: Edward Azoff
Jonathan Hanke

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
May 2010

Dedication

This thesis is dedicated to Jesus Christ. Without Him, my life would be useless, unenjoyable, and perfectly dreadful. He gives me purpose, joy, hope, and determination to do my best. I've been bought with a price, and it is no longer I who live, but Christ who lives in me, the hope of glory. Maranatha.

Acknowledgments

I would like to thank first of all Pete Clark, my advisor, who devoted numerous hours to this project, and who had the insight to guide me to research this topic further. Under his guidance and direction, I have been able to learn what research is truly like. Thanks for teaching me that we cannot decide what is true, no matter how much we want it to be; we just search and discover what is already there. This encouragement helped me continue pressing forward when what I had hoped to be true was not.

I would also like to thank Jon Hanke, without whom this project would not have come together with such perfect timing. Your knowledge of quadratic forms and computer programs was indispensable.

In addition, thanks to Dr. Azoff for his patience with me in his class while being on my thesis committee. Your willingness to help me is greatly appreciated.

Much appreciation goes to my friends in the student Number Theory seminar and John Doyle. They heard the first attempt to relay my ideas and asked me all the tough questions before my defense. Without your aid, I would not have been prepared. Thanks!

Finally, I would like to thank my family and friends. Without each and every one of you, it would have been impossible to succeed. From calling home in tears to needing a break to watch Doctor Who and play Mario Bros., my overall health was kept intact with your help. Thanks to my core: Mom, Dad, and Daniel. Your support through this process kept me steady. Thanks to Brett, Jennifer, and Anna for loving me from so far away. Stacy, thanks for being my gym buddy, and Rebecca, for being my homework buddy and friend. Tom and Ginny, your home provided a great respite for me, nurturing me and allowing me to do my laundry. Two Story, thanks for keeping me fueled.

Table of Contents

Page

Acknowledgments v

List of Figures vii

List of Tables viii

Chapter

1 Preliminaries 1

2 The Legendre Equation 2

2.1 Definitions 2

2.2 The Existence of Solutions 3

2.3 Holzer's Bound 7

2.4 Mordell Enters the Picture 8

2.5 Notes on Cochrane-Mitchell 1998 13

2.6 Extensions of the Legendre Equation 29

3 The Extended Legendre Equation 31

3.1 Definitions 31

3.2 Results and Hopes for $n > 3$ 32

3.3 The Non-Existence of a Mythical Lattice for an ELE when $n \geq 4$ 41

3.4 Further Research Opportunities 45

Bibliography 47

List of Figures

3.1 The first norm has a level set which is the surface of a rectangular solid, as is seen from this picture of solutions of $|(x, y, z)| = \max\left(\frac{|x|}{\sqrt{15}}, \frac{|y|}{\sqrt{10}}, \frac{|z|}{\sqrt{6}}\right) \leq 1$. . . . 33

3.2 The second norm has a level set which is an ellipsoid, as is seen from this picture of solutions of $2x^2 + 3y^2 + 5z^2 < 2$. 34

List of Tables

3.1 A list of small solutions when $n = 5$ and $\alpha = 2$. 38

3.2 A list of small solutions when $n = 5$ and $\alpha = 3$. 38

3.3 A list of small solutions when $n = 4$ and $\alpha = 2$. 38

3.4 A list of small solutions when $n = 4$ and $\alpha = 3$. 39

3.5 A list of small solutions when $n = 4$ and $\alpha = 4$. 39

3.6 A list of small solutions when $n = 4$ and $\alpha = 5$. 39

3.7 A list of small solutions when $n = 4$ and $\alpha = 6$. 39

3.8 A list of small solutions when $n = 4$ and $\alpha = 7$. 39

3.9 A list of small solutions when $n = 4$ and $\alpha = 8$. 40

Chapter 1

Preliminaries

In this paper, we will explore Cochrane-Mitchell's proof of solutions to the Legendre Equation from 1998, and we will explore its validity in the case of more variables than just three [3]. In order to do this, we begin by defining some basic operations for any number of variables that will be used freely throughout the paper.

Let R be an arbitrary commutative ring, with polynomial ring $R[x_1, \ldots, x_n]$. A **quadratic form** is a function $q(\vec{x}) \in R[x_1, \ldots, x_n]$ in which every term has degree 2, giving rise to the term *quadratic*. We will be considering the case where the coefficients are integers and the power of every variable is square. In the case when every term is a square (no cross-terms), the form is called **diagonal**. Every quadratic form can be represented by a symmetric matrix over R, and diagonal forms can be represented by diagonal matrices, giving rise to the term *diagonal*.

A **lattice** is a discrete subgroup of $\mathbb{R}^n$ which is isomorphic to $\mathbb{Z}^n$. We say Λ is a **sublattice** of $\mathbb{Z}^n$ iff $\Lambda \subseteq \mathbb{Z}^n$ is also isomorphic to a free abelian group of rank n. Equivalently, Λ has finite index in $\mathbb{Z}^n$.

Chapter 2

The Legendre Equation

2.1 Definitions

The **Legendre equation** is simply the diagonal conic with $\mathbb{Z}$-coefficients:

$$ax^2 + by^2 + cz^2 = 0,\ abc \in \mathbb{Z} \setminus \{0\}. \tag{2.1}$$

We suppose that there exist non-trivial real solutions. By non-trivial, we mean that the solution is not the zero vector, and we know that such a solution exists exactly when a, b, c do not all have the same sign. The **signature** of a diagonal conic as above is the number of positive coefficents and the number of negative coefficients. For example, if $a, b > 0$ and $c < 0$, then the index of $ax^2 + by^2 + cz^2$ is $(2, 1)$. Then simple manipulations allow one to reduce the Legendre equation to a more specific form, namely

$$ax^2 + by^2 - cz^2 = 0, a, b, c \in \mathbb{Z}^+,\ \gcd(a, b) = \gcd(a, c) = \gcd(b, c) = 1,\ a, b, c \text{ squarefree}. \tag{2.2}$$

We call a Legendre equation of the special form (2.2) **normalized**. Throughout these notes when we refer to "the Legendre equation" we will mean the normalized form (2.2).

Explicitly, here is how you can reduce a Legendre equation to a normalized Legendre equation.

i. a, b, c must not all have the same sign. If they did, then the only real solution would be the trivial one $(0, 0, 0)$ since, if the sum of three positive terms is 0, then each term must be 0.

ii. a, b, c are all squarefree. Suppose not. Then we can get another solution by letting $a = a_1^2 a_2$ and $x' = a_1 x$.

$$\begin{aligned} ax^2 + by^2 + cz^2 &= 0 \\ \Rightarrow a_2(a_1 x)^2 + by^2 + cz^2 &= 0 \\ \Rightarrow a_2(x')^2 + by^2 + cz^2 &= 0. \end{aligned}$$

iii. a, b, c are relatively prime in pairs. If they were not, then suppose $d|a$ and $d|b$, $d > 1$. Then

$$\begin{aligned} ax^2 + by^2 + cz^2 &= 0 \\ \Rightarrow ax^2 + by^2 &= -cz^2 \\ \Rightarrow \frac{a}{d}x^2 + \frac{b}{d}y^2 &= -\frac{c}{d}z^2 \end{aligned}$$

If $d|c$, then divide out and reduce it to an equation with no common divisors. If $d \nmid c$, assuming there exists a solution to the equation, then we know that $d|z^2$. (Otherwise, the only solution would be the trivial one, $(0, 0, 0)$.) Let $z = dz_1$.

$$\begin{aligned} \frac{a}{d}x^2 + \frac{b}{d}y^2 &= -\frac{c}{d}(dz_1)^2 \\ \Rightarrow \frac{a}{d}x^2 + \frac{b}{d}y^2 &= -(cd)z_1^2 \end{aligned}$$

Thus, we have the equation which has pairwise coprime coefficients.

By a **solution** to the Legendre Equation (2.1), we mean $(x, y, z) \in \mathbb{Z}^3$, *not all zero*, such that $ax^2 + by^2 + cz^2 = 0$. Sometimes we say "nontrivial solution" for emphasis, but if ever we mean to consider the trivial solution we shall say so explicitly.

2.2 The Existence of Solutions

The fundamental result on the Legendre equation is as follows. Here we include the proof found in [9] because it utilizes the method of factoring the quadratic form modulo p.

Theorem 1. *(Legendre, 1785) Let a, b, c be nonzero integers such that the product abc is square-free. Necessary and sufficient conditions that $ax^2 + by^2 + cz^2 = 0$ have a solution in integers x, y, z not all zero, are that a, b, c do not have the same sign, and that $-bc, -ac, -ab$ are quadratic residues modulo a, b, c respectively. In other words, there exist $\lambda_1, \lambda_2, \lambda_3 \in \mathbb{Z}$ such that:*

(i) $-bc \equiv \lambda_1^2 \pmod{a}$,

(ii) $-ac \equiv \lambda_2^2 \pmod{b}$,

(iii) $-ab \equiv \lambda_3^2 \pmod{c}$.

Before a proof of this result, Niven, Zuckerman, and Montgomery [9] establish two lemmas and use a theorem they proved previously. We will take these lemmas and theorem for granted here without proof.

Lemma 2. *[9, Lemma 5.12 p. 242] Let λ, μ, ν be positive real numbers with product $\lambda\mu\nu = m$ an integer. Then any congruence $\alpha x + \beta y + \gamma z \equiv 0 \pmod{m}$ has a solution x, y, z, not all zero, such that $|x| \leq \lambda, |y| \leq \mu, |z| \leq \nu$.*

Lemma 3. *[9, Lemma 5.13 pp. 242-3] Suppose that $ax^2 + by^2 + cz^2$ factors modulo m and also modulo n; that is*

$$ax^2 + by^2 + cz^2 \equiv (\alpha_1 x + \beta_1 y + \gamma_1 z)(\alpha_2 x + \beta_2 y + \gamma_2 z) \pmod{m}$$

$$ax^2 + by^2 + cz^2 \equiv (\alpha_3 x + \beta_3 y + \gamma_3 z)(\alpha_4 x + \beta_4 y + \gamma_4 z) \pmod{n}$$

If $(m, n) = 1$ then $ax^2 + by^2 + cz^2$ factors into linear factors modulo mn.

Theorem 4. *[9, Theorem 3.21 pp. 165-6] Suppose that $n > 0$, and let $N(n)$ denote the number of solutions of the congruence $s^2 \equiv -1 \pmod{n}$. Let $R(n)$ denote the number of representations of n as a sum of two squares. That is, $R(n)$ is the number of ordered pairs (x, y) of integers for which $x^2 + y^2 = n$. Let $r(n)$ be the number of such ordered pairs for which $gcd(x, y) = 1$. That is, $r(n)$ is the number of proper representations of n as a sum of two squares. Then $r(n) = 4N(n)$, and $R(n) = \sum r(n/d^2)$ where the sum is extended over all those positive d for which $d^2|n$.*

Proof of Theorem 1. If $ax^2 + by^2 + cz^2 = 0$ has a solution x_0, y_0, z_0 not all zero, then a, b, c are not of the same sign. Dividing $x_0, y_0, z_0 \in \mathbb{Z}$ by $\gcd(x_0, y_0, z_0)$ we have a solution x_1, y_1, z_1 with $\gcd(x_1, y_1, z_1) = 1$.

Next we prove that $\gcd(c, x_1) = 1$. If this were not so there would be a prime p dividing both c and x_1. Then $p \nmid b$ since $p|c$ and abc is square-free. Therefore $p|by_1^2$ and $p \nmid b$, hence $p|y_1^2, p|y_1$, and then $p^2|(ax_1^2 + by_1^2)$ so that $p^2 \mid cz_1^2$. But c is square-free so $p|z_1$. We have concluded that p is a factor of x_1, y_1, and z_1 contrary to $\gcd(x_1, y_1, z_1) = 1$. Consequently, we have $\gcd(c, x_1) = 1$.

Let u be chosen to satisfy $ux_1 \equiv 1 \pmod{c}$. Then the equation $ax_1^2 + by_1^2 + cz_1^2 = 0$ implies $ax_1^2 + by_1^2 \equiv 0 \pmod{c}$, and multiplying this by u^2b we get $u^2b^2y_1^2 \equiv -ab \pmod{c}$. Thus we have established that $-ab$ is a quadratic residue modulo c. A similar proof shows that $-bc$ and $-ac$ are quadratic residues modulo a and b respectively.

Conversely, let us assume that $-bc, -ac, -ab$ are quadratic residues modulo a, b, c respectively. Note that this property does not change if a, b, c are replaced by their negatives. Since a, b, c are not of the same sign, we can change the signs of all of them, if necessary, in order to have one positive and two of them negative. Then, perhaps with a change of notation, we can arrange it so that a is positive and b and c are negative.

Define r as a solution of $r^2 \equiv -ab \pmod{c}$, and a_1 as a solution of $aa_1 \equiv 1 \pmod{c}$. These solutions exist because of our assumptions on a, b, c. Then we can write

$$\begin{aligned} ax^2 + by^2 &\equiv aa_1(ax^2 + by^2) \equiv a_1(a^2x^2 + aby^2) \equiv a_1(a^2x^2 - r^2y^2) \\ &\equiv a_1(ax - ry)(ax + ry) \equiv (x - a_1ry)(ax + ry) \pmod{c}, \end{aligned}$$

$$ax^2 + by^2 + cz^2 \equiv (x - a_1ry)(ax + ry) \pmod{c}.$$

Thus $ax^2 + by^2 + cz^2$ is the product of two linear factors modulo c, and similarly modulo a and modulo b. Applying Lemma 3 twice, we conclude that $ax^2 + by^2 + cz^2$ can be written as the product of two linear factors modulo abc. That is, there exist numbers $\alpha, \beta, \gamma, \alpha', \beta', \gamma'$

such that

$$ax^2 + by^2 + cz^2 \equiv (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \pmod{abc}. \tag{2.3}$$

We now apply Lemma 2 to the congruence

$$\alpha x + \beta y + \gamma z \equiv 0 \pmod{abc} \tag{2.4}$$

using $\lambda = \sqrt{bc}, \mu = \sqrt{|ac|}, \nu = \sqrt{|ab|}$. Thus we get a solution x_1, y_1, z_1 of the congruence (2.4) with $|x_1| \leq \sqrt{bc}$, $|y_1| \leq \sqrt{|ac|}$, $|z_1| \leq \sqrt{|ab|}$. But abc is square-free, so $\sqrt{bc}$ is an integer only if it is 1, and similary for $\sqrt{|ac|}$ and $\sqrt{|ab|}$. Therefore we have

$$\begin{aligned}
&|x_1| \leq \sqrt{bc}, && x_1^2 \leq bc \text{ with equality possible only if } b = c = -1\\
&|y_1| \leq \sqrt{|ac|}, && y_1^2 \leq -ac \text{ with equality possible only if } a = 1, c = -1\\
&|z_1| \leq \sqrt{|ab|}, && z_1^2 \leq -ab \text{ with equality possible only if } a = 1, b = -1.
\end{aligned}$$

Hence, since a is positive and b and c are negative, we have, unless $b = c = -1$,

$$ax_1^2 + by_1^2 + cz_1^2 \leq ax_1^2 < abc$$

and

$$ax_1^2 + by_1^2 + cz_1^2 \geq by_1^2 + cz_1^2 > b(-ac) + c(-ab) = -2abc.$$

Leaving aside the special case when $b = c = -1$, we have

$$-2abc < ax_1^2 + by_1^2 + cz_1^2 < abc.$$

Now x_1, y_1, z_1 is a solution of (2.4) and so also, because of (2.3), a solution of

$$ax^2 + by^2 + cz^2 \equiv 0 \pmod{abc}.$$

Thus the above inequalities imply that

$$ax_1^2 + by_1^2 + cz_1^2 = 0 \quad \text{or} \quad ax_1^2 + by_1^2 + cz_1^2 = -abc.$$

In the first case we have our solution of $ax^2 + by^2 + cz^2 = 0$. In the second case we readily verify that x_2, y_2, z_2, defined by $x_2 = -by_1 + x_1 z_1$, $y_2 = ax_1 + y_1 z_1$, $z_2 = z_1^2 + ab$, form a

solution. In case $x_2 = y_2 = z_2 = 0$ then $z_1^2 + ab = 0$, $z_1^2 = -ab$ and $z_1 = \pm 1$ because ab, like abc, is square-free. Then $a = 1$, $b = 1$, and $x = 1$, $y = -1$, $z = 0$ is a solution.

Finally we must dispose of the special case $b = c = -1$. The conditions on a, b, c now imply that -1 is a quadratic residue modulo a; in other words, that $N(a)$ of Theorem 4 is positive. By Theorem 4 this implies that $r(a)$ is positive and hence that the equation $y^2 + z^2 = a$ has a solution y_1, z_1. Then $x = 1$, $y = y_1$, $z = z_1$ is a solution of $ax^2 + by^2 + cz^2 = 0$ since $b = c = -1$. □

The standard proofs of Theorem 1, as the one above, are nonconstructive: that is, they offer no explicit procedure for finding a solution but merely deduce that such a solution must exist. Once we know the existence result there is an obvious algorithm for finding a solution: for each $N \in \mathbb{Z}^+$, plug in each of the $(2N+1)^3 - 1$ triples $(x, y, z) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ with $\max(|x|, |y|, |z|) \leq N$ into (2.2) until we find one triple which gives a solution!

Of course it would be very desirable to have some upper bound on how long this brute force search will take. This is given by the following theorem of Holzer.

2.3 Holzer's Bound

Holzer gives a non-elementary proof using results of 20th century analytic number theory of a sharp upper bound on the smallest solution to a Legendre equation which has solutions.

Theorem 5. *(Holzer, 1950) Suppose that the normalized Legendre equation has a nontrivial solution. Then there exists a (nontrivial!) solution (x, y, z) satisfying the inequalities*

$$|x| \leq \sqrt{bc}, \ |y| \leq \sqrt{ac}, \ |z| \leq \sqrt{ab}.$$

In particular, if we put $M = \max(|a|, |b|, |c|)$, then Holzer's theorem guarantees a solution (x, y, z) to the Legendre equation with $|x|, |y|, |z| \leq M$, giving an explicit upper bound on the length of the search.

Remark: The Holzer bound is indeed sharp for some Legendre equations. However, for a class of equations, the bound is not actually attained. When we develop more machinery, we will explore these equations further.

2.4 Mordell Enters the Picture

While Holzer's original proof used deep results of Hecke, Louis. J. Mordell published an elementary proof of Holzer's theorem in 1969 [7]. This theorem states that if the equation $ax^2 + by^2 + cz^2 = 0$ taken in the normal form has an integral solution, then a solution exists in which the following inequalities hold:

$$|x| \leq (|bc|)^{1/2} \quad |y| \leq (|ca|)^{1/2} \quad |z| \leq (|ab|)^{1/2}$$

Cochrane and Mitchell [3] claim that Williams [12] filled in some gaps Mordell left out of his proof in 1988, while Cochrane and Mitchell gave a new, elementary proof of Holzer's theorem ten years later. Although it was published that Mordell's argument is incomplete, we will show that it is not. When one takes time to understand the argument thoroughly, verification of the 'missing pieces' of the proof is quite simple.

2.4.1 Mordell's Paper

Mordell uses a definition of the normalized form of a Legendre equation that is a little bit different from our definition of having a, b, and c being positive. Here, however, we will stick to Mordell's convention of $c < 0$, remaining honest to his paper.

Mordell begins his paper by discussing Legendre's exploration in his classic work of nontrivial solutions to the equation

$$ax^2 + by^2 + cz^2 = 0, \tag{2.5}$$

in which he says that the equation can be reduced to a normal form in which the following conditions hold:

i. a, b, c do not all have the same sign.

ii. a, b, c are all squarefree.

iii. a, b, c are relatively prime in pairs.

Legendre proved that the solvability of the congruences

$$bX^2 + c \equiv 0 \pmod{a} \quad cY^2 + a \equiv 0 \pmod{b} \quad aZ^2 + b \equiv 0 \pmod{c}$$

is a necessary and sufficient condition for the existence of integer solutions of (2.5).

Mordell begins by saying we can suppose $a > 0$, $b > 0$, and $c < 0$. Recall the Holzer bound:

$$|x| \leq (b|c|)^{1/2} \quad |y| \leq (|c|a)^{1/2} \quad |z| \leq (ab)^{1/2}. \tag{2.6}$$

We see that the first two inequalities follow from the third. Since $c < 0$,

$$|z| \leq (ab)^{1/2} \Rightarrow ax^2 + by^2 + c\big((ab)^{1/2}\big)^2 \leq 0$$

$$\Leftrightarrow ax^2 + by^2 + abc \leq 0 \tag{2.7}$$

From this, we now derive two inequalities. First, since $\frac{-by^2}{a} \leq 0$ and $-\frac{abc}{a} > 0$,

$$(2.7) \Rightarrow x^2 \leq \frac{-by^2 - abc}{a} = \frac{-by^2}{a} - \frac{abc}{a} \leq b(-c) \Rightarrow |x| < (b|c|)^{1/2}.$$

Secondly, since $\frac{-ax^2}{b} < 0$ and $-\frac{abc}{b} > 0$,

$$(2.7) \Rightarrow y^2 < \frac{-ax^2 - abc}{b} = \frac{-ax^2}{b} - \frac{abc}{b} < a(-c) \Rightarrow |y| < (a|c|)^{1/2}.$$

We can also see that we have strict inequality unless two of the a, b, c are equal to one. To see this, let's suppose $|x| = (b|c|)^{1/2}$. Then $b|c|$ is a perfect square only if $b = |c| = 1$ since b, c are squarefree.

Now, what Mordell shows in his paper is that if a solution (x_0, y_0, z_0) exists with $\gcd(x_0, y_0) = 1$ and $|z_0| > (ab)^{1/2}$, we can find another solution (x, y, z) with $|z| < |z_0|$. Then (2.6) follows since the other inequalities follow from this one. Let's prove it!

Proof. **Step 1:** Put

$$x = x_0 + tX, \qquad y = y_0 + tY, \qquad z = z_0 + tZ,$$

where X, Y, Z are integers to be determined later and $t \neq 0$, $t \in \mathbb{Q}$. Then, by substitution, we get

$$\begin{aligned} 0 &= a(x_0 + tX)^2 + b(y_0 + tY)^2 + c(z_0 + tZ)^2 \\ \Rightarrow 0 &= ax_0^2 + 2ax_0tX + at^2X^2 + by_0^2 + 2by_0tY + bt^2Y^2 + cz_0^2 + 2cz_0tZ + ct^2Z^2 \end{aligned}$$

Regrouping and by our hypothesis that (x_0, y_0, z_0) is a solution, then we get

$$\begin{aligned} \Rightarrow 0 &= (aX^2 + bY^2 + cZ^2)t^2 + 2t(ax_0X + by_0Y + cz_0Z) + ax_0^2 + by_0^2 + cz_0^2 \\ \Rightarrow 0 &= (aX^2 + bY^2 + cZ^2)t + 2(ax_0X + by_0Y + cz_0Z) \end{aligned}$$

since $t \neq 0$. If we solve for t here, we see that we get

$$t = \frac{-2(ax_0X + by_0Y + cz_0Z)}{aX^2 + bY^2 + cZ^2}$$

Plugging this into our formulas for x, y, z, we get the following equations, where $\delta = aX^2 + bY^2 + cZ^2$:

$$\begin{cases} \delta z &= z_0(\delta) - 2Z(ax_0X + by_0Y + cz_0Z), \\ \delta x &= x_0(\delta) - 2X(ax_0X + by_0Y + cz_0Z), \\ \delta y &= y_0(\delta) - 2Y(ax_0X + by_0Y + cz_0Z), \end{cases} \tag{2.8}$$

Step 2: Next, Mordell shows that

$$\delta | c \qquad \text{and} \qquad \delta | y_0X - x_0Y \Longrightarrow x, y, z \in \mathbb{Z}$$

Step 2.1: Show $\gcd(\delta, abx_0y_0) = 1$.

Suppose $\delta | c$ and $\delta | y_0X - x_0Y$. Then it is claimed that $\gcd(\delta, abx_0y_0) = 1$. To show this, suppose that there is some prime p such that $p|\delta$ and $p|abx_0y_0$. Since $\delta|c$ and a, b, c are pairwise relatively prime, $p|x_0y_0$. Suppose $p|x_0$. Then by the equation $ax_0^2 + by_0^2 + cz_0^2 = 0$, we see that $p|by_0^2$. But $p \nmid b$, so $p|y_0^2 \overset{Euclid's Lemma}{\Longrightarrow} p|y_0$, which is a contradiction since we assumed

that $\gcd(x_0, y_0) = 1$.

Step 2.2: Given (2.8), we show that the congruences

$$P = ax_0X + by_0Y \equiv 0 \pmod{\delta}, \qquad Q = aX^2 + bY^2 \equiv 0 \pmod{\delta} \tag{2.9}$$

imply that $x, y, z \in \mathbb{Z}$. This gives that these congruences are all we must show to complete the proof.

Given these two congruences, taking (2.8) modulo δ, we get three true equivalences because $\delta | c$, making x, y, z integers, as desired.

$$\begin{aligned} \delta z &\equiv z_0(Q + cZ^2) - 2Z(P + cz_0Z) \\ 0 &\equiv z_0cZ^2 - 2cz_0Z^2 \\ 0 &\equiv -cz_0Z^2 \\ 0 &\equiv 0 \end{aligned} \qquad \begin{aligned} \delta x &\equiv x_0(Q + cZ^2) - 2X(P + cz_0Z) \\ 0 &\equiv x_0cZ^2 - 2Xcz_0Z \\ 0 &\equiv cZ(x_0 - 2z_0X) \\ 0 &\equiv 0 \end{aligned}$$

$$\begin{aligned} \delta y &\equiv y_0(Q + cZ^2) - 2Y(P + cz_0Z) \\ 0 &\equiv y_0cZ^2 - 2Ycz_0Z \\ 0 &\equiv cZ(y_0Z - 2z_0Y) \\ 0 &\equiv 0 \end{aligned}$$

Step 2.3: Show the truth of congruences (2.9).

Since $\delta | y_0X - x_0Y$, we have that $y_0X - x_0Y \equiv 0 \pmod{\delta}$ and $X \equiv \frac{x_0Y}{y_0} \pmod{\delta}$. By substitution, we have $P \equiv \frac{Y(ax_0^2 + by_0^2)}{y_0} \equiv 0 \pmod{\delta}$, and $Q \equiv \frac{(ax_0^2 + by_0^2)Y^2}{y_0^2} \equiv 0 \pmod{\delta}$. Therefore, $x, y, z \in \mathbb{Z}$.

Step 3: Now we show that x, y, z satisfy (2.6), or the Holzer bound. We may simply check that $|z| \leq \sqrt{ab}$ and the other inequalities follow. In order to find this, we show how to find a z with $|z| < |z_0|$, and if it is not small enough, we may iterate the process as many times as necessary to find a z with $|z| \leq \sqrt{ab}$, or equivalently, with $z^2 \leq ab$.

To get a useful equation, we manipulate equation (2.8) in a clever way:

$$\begin{aligned}
\delta z &= z_0(aX^2+bY^2+cZ^2) - 2Z(ax_0X+by_0Y+cz_0Z) \\
\frac{\delta z}{cz_0} &= \frac{aX^2+bY^2}{c} + Z^2 - 2Z\left(\frac{ax_0X+by_0Y}{cz_0}\right) - 2Z^2 \\
\frac{-\delta z}{cz_0} &= Z^2 + 2Z\left(\frac{ax_0X+by_0Y}{cz_0}\right) - \frac{aX^2+bY^2}{c} \\
\frac{-\delta z}{cz_0} &= \left(Z+\frac{ax_0X+by_0Y}{cz_0}\right)^2 - \frac{aX^2+bY^2}{c} - \left(\frac{ax_0X+by_0Y}{cz_0}\right)^2 \\
\frac{-\delta z}{cz_0} &= \left(Z+\frac{ax_0X+by_0Y}{cz_0}\right)^2 - \frac{1}{c^2z_0^2}(aX^2cz_0^2+bY^2cz_0^2+a^2x_0^2X^2+b^2y_0^2Y^2+2abx_0y_0XY)
\end{aligned}$$

Using the fact that $cz_0^2 = -ax_0^2 - by_0^2$, and letting $L = \left(Z+\frac{ax_0X+by_0Y}{cz_0}\right)^2$ we see that

$$\begin{aligned}
\frac{-\delta z}{cz_0} &= L - \frac{1}{c^2z_0^2}(aX^2(-ax_0^2-by_0^2)+bY^2(-ax_0^2-by_0^2)+a^2x_0^2X^2+b^2y_0^2Y^2+2abx_0y_0XY) \\
\frac{-\delta z}{cz_0} &= L - \frac{1}{c^2z_0^2}(-a^2x_0^2X^2 - aby_0^2X^2 + -abx_0^2Y^2 - b^2y_0^2Y^2 + a^2x_0^2X^2 + b^2y_0^2Y^2 + 2abx_0y_0XY) \\
\frac{-\delta z}{cz_0} &= L + \frac{ab}{c^2z_0^2}(y_0^2X^2 - 2x_0y_0XY + x_0^2Y^2) \\
\frac{-\delta z}{cz_0} &= L + \frac{ab}{c^2z_0^2}(y_0X - x_0Y)^2
\end{aligned}$$

Thus, we have

$$\frac{-\delta z}{cz_0} = \left(Z+\frac{ax_0X+by_0Y}{cz_0}\right)^2 + \frac{ab}{c^2z_0^2}(y_0X-x_0Y)^2 \tag{2.10}$$

Now, take X, Y as any solution of $y_0X - x_0Y = \delta$. From our assumption that $|z_0| > (ab)^{1/2}$, we can assume that $z_0^2 > ab$. Now there are two cases.

Case 1: Let c be even. In this case, take $\delta = \frac{1}{2}c$, and choose Z so that

$$\left|Z+\frac{ax_0X+by_0Y}{cz_0}\right| \le \frac{1}{2}$$

Then by taking the absolute value of equation (2.10), we have

$$\frac{1}{2}\left|\frac{z}{z_0}\right| \le \frac{1}{4} + \frac{ab}{4z_0^2} < \frac{1}{4}+\frac{1}{4} = 0 \qquad \Longrightarrow \qquad |z| < |z_0|. \tag{2.11}$$

Case 2: Let c be odd. Now, we impose the condition that

$$aX + bY + cZ \equiv 0 \pmod 2.$$

Because a, b, X, Y are chosen already and c is odd, then $Z \equiv aX + bY \pmod 2$. Also, δ is odd because $\delta | c$, so all three of the right-hand sides of the equations in (2.8) are divisible by 2δ. This is easy to see because the terms with the 2s are divisible by 2, and they are divisible by δ because $P = ax_0X + by_0Y \equiv 0 \pmod \delta$, and $\delta | c$. Similarly, the first terms are divisible by δ. However, since we have imposed the condition that $aX + bY + cZ \equiv 0 \pmod 2$, since $\forall\ n \in \mathbb{Z},\ n \equiv n^2 \pmod 2$, we have that $aX^2 + bY^2 + cZ^2 \equiv 0 \pmod 2$ also. Thus, we can take (2.10) and replace δ by 2δ to get

$$\frac{-2\delta z}{cz_0} = \left(Z + \frac{ax_0X + by_0Y}{cz_0}\right)^2 + \frac{ab}{c^2z_0^2}(y_0X - x_0Y)^2.$$

Take $\delta = c$ and choose Z with the desired parity so that

$$\left|Z + \frac{ax_0X + by_0Y}{cz_0}\right| \leq 1.$$

Then instead of (2.11) we have

$$2\left|\frac{z}{z_0}\right| \leq 1 + \frac{ab}{z_0^2} < 1 + 1 = 2 \qquad \Longrightarrow \qquad |z| < |z_0|.$$

While Mordell claimed that this completes his proof, we have yet to show that this new solution is nontrivial (i.e. not $(0, 0, 0)$). To do this, it suffices to check that $z \neq 0$. If $z = 0$, then from equation (2.10), since both of the terms of the right-hand side are positive ($a, b > 0$), they both must equal 0 also. This is absurd since $y_0X - x_0Y = \delta \neq 0$ because $\delta = \frac{1}{2}c$ or $\delta = c$, depending on the parity of c. So $z \neq 0$ or else we would get a contradiction. Therefore, we have found a nontrivial integral solution (x, y, z) to the equation $ax^2 + by^2 + cz^2 = 0$. $\square$

2.5 Notes on Cochrane-Mitchell 1998

In their 1998 paper [3], Cochrane and Mitchell give a simultaneous proof of Legendre's theorem on the existence of solutions to the equation $ax^2 + by^2 + cz^2 = 0$ and Holzer's theorem giving an explicit upper bound on the size of the smallest nonzero solution. The proof, which uses only elementary results in the geometry of numbers, is in many ways more natural and transparent than any of the standard proofs of either Legendre's Theorem or Holzer's theorem.

2.5.1 Two Norms and Back to Holzer

Next, we will introduce two norms on $\mathbb{R}^3$, as done by Cochrane-Mitchell [3]. The first norm is

$$|(x,y,z)| = \max(\frac{|x|}{\sqrt{bc}}, \frac{|y|}{\sqrt{ac}}, \frac{|z|}{\sqrt{ab}}).$$

This is the image of the usual ℓ_∞ norm under the linear change of variables

$$(x',y',z') = (\sqrt{bc}x, \sqrt{ac}y, \sqrt{ab}z.)$$

Note that the change of basis matrix here is simply a diagonal matrix, so that the geometric effect is simply that of dilating each of the axes, but by different amounts. Holzer's theorem can then be restated as:

Theorem 6. *(Holzer restated) If the normalized Legendre equation (2.2) has a nontrivial solution, then it has a nontrivial solution (x,y,z) with $|(x,y,z)| \leq 1$.*

This bound is **sharp** in the sense that equality can occur.

Example: Take $a = b = 1$, $c = p$ a prime. Then the condition for the normalized Legendre equation $x^2 + y^2 = pz^2$ to have a solution is just that -1 is a square modulo p, which is satisfied if $p = 2$ or $p \equiv 1 \pmod 4$. On the other hand, $|(x,y,z)| = \max(\frac{|x|}{\sqrt{p}}, \frac{|y|}{\sqrt{p}}, |z|)$. A solution with $|(x,y,z)| < 1$ would then have $|z| < 1$ – hence $z = 0$ – thus would be $x^2 + y^2 = 0$, which obviously has no nontrivial solutions. Therefore any solution must have $|(x,y,z)| \geq 1$. So, by Theorem 6 we must have a solution with $|(x,y,z)| = 1$. For instance, taking $p = 5$, the solution $(1,2,1)$ satisfies $|(1,2,1)| = 1$. In general, by Fermat's Two squares theorem, under the label Lemma 2.13 in Niven, Zuckerman, and Montgomery's book [9], there exist $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = p$, so that $(x,y,1)$ is a solution with $|(x,y,1)| = 1$ where $p \equiv 1 \pmod 4$.

We call a vector $\vec{x} \in \mathbb{R}^3$ a **small vector** if $|\vec{x}| \leq 1$, and we call a (nontrivial!) solution $\vec{x} \in \mathbb{Z}^3$ to (2.2) a **small solution** if $|\vec{x}| \leq 1$. Thus Holzer's theorem can be restated

once more as saying that if any nontrivial solutions exist at all, then small solutions exist.

Cochrane and Mitchell also introduce a second norm $||(x, y, z)||$, which is an asymetrically dilated version of the standard ℓ_2, or Pythagorean, norm:

$$||(x, y, z)|| = \sqrt{ax^2 + by^2 + cz^2}.$$

Notice that the balls for $|\ |$ are rectangular parallelepipeds, whereas the balls for $||\ ||$ are ellipsoids. Therefore the two norms are "geometrically different", and in particular one cannot get from one to the other by a linear change of variables. However – and this the point for introducing the second norm – upon restriction to solutions to (2.2), the two norms are simply proportional:

Proposition 7. *If $(x, y, z) \in \mathbb{Z}^3$ is a solution to (2.2), then we have*

$$||(x, y, z)|| = \sqrt{2abc}\ |(x, y, z)|.$$

Consequently, a solution (x, y, z) is small iff

$$ax^2 + by^2 + cz^2 \leq 2abc.$$

Proof. First, suppose $(x, y, z) \in \mathbb{Z}^3$ is a solution to (2.2). Then $ax^2 + by^2 = cz^2$, which, when dividing every term in the equation by abc, we get $\frac{x^2}{bc} + \frac{y^2}{ac} = \frac{z^2}{ab}$. Since every term is nonnegative, we see that $\frac{z^2}{ab} \geq \frac{x^2}{bc}$ and $\frac{z^2}{ab} \geq \frac{y^2}{ac}$, from which we may derive that $\frac{|z|}{\sqrt{ab}} \geq \frac{|x|}{\sqrt{bc}}$ and $\frac{|z|}{\sqrt{ab}} \geq \frac{|y|}{\sqrt{ac}}$. By the definition of the first norm, then, we find that $|(x, y, z)| = \frac{|z|}{\sqrt{ab}}$.

To prove the first claim, it is equivalent to show that the squares of both sides are equal. Thus,

$$\left(\sqrt{2abc}\ |(x, y, z)|\right)^2 = 2abc\left(\frac{z^2}{ab}\right) = 2cz^2 = cz^2 + cz^2 = ax^2 + by^2 + cz^2 = ||(x, y, z)||^2.$$

□

2.5.2 Holzer Bound: Unattained

Now, we look at a case where there are solutions to (2.2) but do not actually attain equality with the Holzer bound. Take $a = 1$, $b = 3$, and let c be any prime with $c \equiv 1 \pmod 3$. Letting $z = 1$, we have the following equation:

$$x^2 + 3y^2 - c = 0$$

$$\Rightarrow x^2 + 3y^2 = c$$

From a result proved using a theorem by Thue in Nagell's book [8, Theorem 100 in § 54, p. 188], we see that such a solution always exists provided that c is a prime with $c \equiv 1 \pmod 6$. However, any prime $c > 3$ with $c \equiv 1 \pmod 3$ will be $\equiv 1 \pmod 6$ because it must be odd. Now, Dirichlet's theorem says that there are infinitely many primes congruent to b modulo c whenever b and c are relatively prime positive integers [6, Theorem 1 in § 16.1, p. 251]. Thus, there are infinitely many primes $c \equiv 1 \pmod 3$ since 1 and 3 are relatively prime positive integers.

Notice however, that if we have such a solution $(x, y, 1)$, then we see that

$$||(x, y, 1)||^2 = x^2 + 3y^2 + c(1)^2 = 2c$$

but the square of the Holzer bound is

$$2abc = 2 \cdot 3c = 6c.$$

Thus, we have found a class of equations for which the Holzer bound is not sharp.

This line of reasoning is pushed further in the following result. In order to prepare for the proof, however, we will state a few facts from Cox's book *Primes of the Form* $x^2 + ny^2$ [4].

Lemma 8. *[4, Lemma 9.3 p. 180] Let L be the ring class field of an order $\mathcal{O}$ in an imaginary quadratic field K. Then L is a Galois extension, and its Galois group can be written as a*

semidirect product

$$\mathrm{Gal}(L/\mathbb{Q}) \backsimeq \mathrm{Gal}(L/K) \rtimes (\mathbb{Z}/2\mathbb{Z})$$

where the nontrivial element of $\mathbb{Z}/2\mathbb{Z}$ *acts on* $\mathrm{Gal}(L/K)$ *by sending* σ *to its inverse* σ^{-1}.

We will only be using the first conclusion of this Lemma in our proof.

Theorem 9. *[4, Theorem 9.4 p.181] Let* $n > 0$ *be an integer, and* L *be the ring class field of the order* $\mathbb{Z}[\sqrt{-n}]$ *in the imaginary quadratic field* $K = \mathbb{Q}(\sqrt{-n})$. *If* p *is an odd prime not dividing* n, *then*

$$p = x^2 + ny^2 \iff p \text{ splits completely in } L.$$

Corollary 10. *[4, Corollary 5.21 p. 107] Let* $K \subset L$ *be a Galois extension, and let* $\mathfrak{p}$ *be an unramified prime of* K. *Given a prime* $\mathfrak{B}$ *of* L *containing* $\mathfrak{p}$, *we have:*

(i) If $\sigma \in \mathrm{Gal}(L/K)$, *then*

$$\left(\frac{L/K}{\sigma(\mathfrak{B})}\right) = \sigma \left(\frac{L/K}{\mathfrak{B}}\right) \sigma^{-1}.$$

(ii) The order of $((L/K)/\mathfrak{B})$ *is the inertial degree* $f = f_{\mathfrak{B}|\mathfrak{p}}$.

(iii) $\mathfrak{p}$ *splits completely in* L *if and only if* $((L/K)/\mathfrak{B}) = 1$.

Theorem 11. *[4, Theorem 8.17 p. 170] Let* L *be a Galois extension of* K, *and let* $\langle\sigma\rangle$ *be the conjugacy class of an element* $\sigma \in \mathrm{Gal}(L/K)$. *Then the set*

$$S = \{\mathfrak{p} \in \mathcal{P}_K : \mathfrak{p} \text{ is unramified in } L \text{ and } ((L/K)/\mathfrak{p}) = \langle\sigma\rangle\}$$

has Dirichlet density

$$\delta(S) = \frac{|\langle\sigma\rangle|}{|\mathrm{Gal}(L/K)|} = \frac{|\langle\sigma\rangle|}{[L:K]}.$$

Now to our theorem.

Theorem 12. *For any* $D > 0$, *there are infinitely many primes,* q, *such that* $q = x^2 + Dy^2$. *In particular, take* D *squarefree and relatively prime to* q. *Then solutions of the form* $(x, y, 1)$ *will be small with* $||(x, y, 1)||^2 = 2q \leq 2qD = (\textit{Holzer Bound})^2$. *For* $D \neq 1$, *we find that solutions of the equation will be short of the Holzer bound by a multiple of* D.

Proof. First we show that the Holzer bound is not sharp if $D \neq 1$. From Proposition 7, we know that a solution is small iff $||(x, y, z)||^2 \leq 2abc = (\text{Holzer Bound})^2$. Calculating in this case, we get

$$(\text{Holzer Bound})^2 = (\sqrt{2abc}\ |(x, y, 1)|)^2 = 2abc = 2Dq$$

This bound is not sharp since

$$||(x, y, 1)||^2 = x^2 + Dy^2 + q = 2q.$$

For the proof of the remainder of the theorem, we follow Cox's argument and use the facts we stated before stating this result.

Let $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$ be an order in the imaginary quadratic field $F = \mathbb{Q}[\sqrt{-n}]$. Let L be the ring class field of our order $\mathcal{O}$ and imaginary quadratic field F. Then by Lemma 8, L is a Galois extension of $\mathbb{Q}$. Now, applying Theorem 9, we find that if p is an odd prime not dividing n, then $p = x^2 + ny^2$ iff p splits completely in L. From Corollary 10, we find the following equivalence:

$$\mathfrak{p} \text{ splits completely in } L \iff \left(\frac{L/K}{\mathfrak{p}}\right) = 1.$$

The density of such $\mathfrak{p}$ among all primes in K is $\frac{1}{[L:K]}$ by Theorem 11. In particular, there are infinitely many of them. Taking $K = \mathbb{Q}$ and L to be the ring class field of the quadratic order $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$, we may conclude that there are infinitely many primes p which can be represented at $p = x^2 + ny^2$. □

2.5.3 Small solutions to the Legendre equation

Before moving on, we state a well-known theorem and discuss an extension of it which will be used later.

Theorem 13. *Minkowski's Convex Body Theorem [9, Theorem 6.21 p. 315] Let A be a nonsingular $n \times n$ matrix with real elements, and let $\Lambda = A\mathbb{Z}^n$. If $\mathcal{C}$ is a set in $\mathbb{R}^n$ that is convex, symmetric about $\vec{0}$, and if $\operatorname{Vol}\mathcal{C} > 2^n \operatorname{coVol}\Lambda$, then there exists a lattice point $\vec{x} \in \Lambda$ such that $\vec{x} \neq \vec{0}$ and $\vec{x} \in \mathcal{C}$.*

Notice that if $\mathcal{C}$ is compact (i.e. closed and bounded), then the conclusion of the theorem holds if equality holds in the theorem in addition to the other hypotheses being met. Suppose that $\operatorname{Vol}\mathcal{C} = 2^n \operatorname{coVol}\Lambda$. Then for any decreasing sequence $\epsilon_n > 0$, $\epsilon_n \to 0$, we have that $\operatorname{Vol}(1+\epsilon_n)\mathcal{C} > 2^n \operatorname{coVol}\Lambda$. We may apply Theorem 13 to find a sequence of nonzero lattice points $\{x_n\} \subset \Lambda$ because this sequence is contained in the bounded set $(2+\epsilon_1)\mathcal{C}$. Since there are only finitely many lattice points inside of each $(1+\epsilon_n)\mathcal{C}$ and there is a nonzero lattice point in each of the $(1+\epsilon_n)\mathcal{C}$'s, there must be at least one $x_0 \in \Lambda$ which is in every $(1+\epsilon_n)\mathcal{C}$. Thus, $x_0 \in \overline{\mathcal{C}}$. However, since $\mathcal{C}$ is closed, $\overline{\mathcal{C}} = \mathcal{C}$, and we have found a nonzero lattice point $x_0 \in \Lambda \cap \mathcal{C}$. This means that if we have a compact convex body, then we may have equality in the inequality above and the result of the theorem stills hold.

The key idea that Cochrane-Mitchell introduce that brings in the Geometry of Numbers part of their argument is that solutions to (2.2) are related to vectors in a certain sublattice $\Lambda \subset \mathbb{Z}^3$. Namely, we define Λ to be the set of all $(x, y, z) \in \mathbb{Z}^3$ satisfying

$$by - \lambda_1 z \equiv 0 \pmod{a},\ ax - \lambda_2 z \equiv 0 \pmod{b},\ ax - \lambda_3 y \equiv 0 \pmod{c}. \tag{2.12}$$

Recall that in the normalized Legendre equation, λ_1, λ_2, and λ_3 are fixed integers such that $\lambda_1^2 \equiv bc \pmod{a}$, $\lambda_2^2 \equiv ac \pmod{b}$, and $\lambda_3^2 \equiv -ab \pmod{c}$.

Proposition 14. *Consider the lattice $\Lambda \subset \mathbb{Z}^3$ defined above.*

a) The covolume of Λ is abc.

b) Every element of Λ is a congruential solution to the Legendre equation:

$$(x, y, z) \in \Lambda \implies ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}. \tag{2.13}$$

c) It follows that Λ contains a vector (x, y, z) with $0 < |(x, y, z)| \leq 1$.

d) Any small vector $(x, y, z) \in \Lambda$ is either *a solution to (2.2) or is a solution to the* ***auxiliary equation***

$$ax^2 + by^2 - cz^2 = \pm abc.$$

Proof. a) We claim that a basis for the lattice Λ is

$$B = \big\{(bc, 0, 0), (x_1, a, 0), (x_2, y_2, 1)\big\}$$

for appropriate values of $x_1, x_2, y_2 \in \mathbb{Z}$ chosen as follows:

Rather than simply showing that B is a basis, we will consider a basis in the following form and show one way to choose the entries of each basis vector:

$$\begin{aligned} \vec{e_1} &= (X_1, 0, 0) \\ \vec{e_2} &= (Y_1, Y_2, 0) \\ \vec{e_3} &= (Z_1, Z_2, Z_3). \end{aligned}$$

With these vectors, we will plug them into the congruences in (2.12) and find out what requirements each unknown entry of $\vec{e_1}, \vec{e_2}$, and $\vec{e_3}$ must fulfill.

For $\vec{e_1}$, using the conditions given by Λ, we see that $aX_1 \equiv 0 \pmod{b}$ and $aX_1 \equiv 0 \pmod{c}$. Thus, $b, c | X_1$ and the minimal choice for X_1 is bc.

For $\vec{e_2}$, again from the given conditions since $\vec{e_2} \in \Lambda$, we know that $a|Y_2$ and $b|Y_1$. Suppose that $Y_2 = a$, and let $Y_1 = bY_1'$. Then by the third congruence, we have

$$\begin{aligned} aY_1 - \lambda_3 Y_2 &\equiv 0 \pmod{c} \\ abY_1' - \lambda_3 a &\equiv 0 \pmod{c} \\ bY_1' - \lambda_3 &\equiv 0 \pmod{c} \\ Y_1' &\equiv \lambda_3 b^{-1} \pmod{c} \\ \Rightarrow Y_1 &\equiv b\lambda_3 b^{-1} \pmod{c} \\ Y_1 &\equiv \lambda_3 \pmod{c} \end{aligned}$$

For $\vec{e_3}$, let's take $Z_3 = 1$. By the equivalences (2.12), we see that

$$\begin{aligned} bZ_2 - \lambda_1 \equiv 0 \pmod{a} &\Rightarrow bZ_2 \equiv \lambda_1 \pmod{a} \\ aZ_1 - \lambda_2 \equiv 0 \pmod{b} &\Rightarrow aZ_1 \equiv \lambda_2 \pmod{b} \\ aZ_1 - \lambda_3 Z_2 \equiv 0 \pmod{c} &\Rightarrow Z_1 \equiv Z_2 \equiv 0 \pmod{c} \end{aligned}$$

By the Chinese Remainder Theorem, these equations are independent since a, b, c are pairwise coprime. Also, there is a unique solution solving the first two equations, but there is a choice for the last. Nevertheless, Z_1 and Z_2 may be found.

In this case, it is true that the covolume of Λ is the absolute value of the determinant of the matrix formed by the above basis, which is clearly abc. So we check that B is indeed a basis for Λ.

Suppose (x, y, z) satisfies the congruences (2.12). We want to show that

$$(x, y, z) = \lambda(bc, 0, 0) + \mu(x_1, a, 0) + \nu(x_2, y_2, 1)$$

for ν, μ, λ chosen successively. Simplifying the equation above, we get

$$(x, y, z) = (\lambda bc + \mu x_1 + \nu x_2, \mu a + \nu y_2, \nu).$$

Solving for ν, μ, and λ, we get

$$\nu = z, \qquad \mu = \frac{y - zy_2}{a}, \quad \text{and} \quad \lambda = \frac{q}{bc} \quad \text{where} \quad q = x - \frac{y - zy_2}{a}x_1 - zx_2.$$

Now we must show that $\nu, \mu, \lambda \in \mathbb{Z}$. It is clear that $\nu \in \mathbb{Z}$ since $\nu = z$. For μ, we want to show that $p = y - zy_2 \equiv 0 \pmod{a}$. By plugging $(x_2, y_2, 1)$ into (2.12), we get that $\lambda_1 \equiv by_2 \pmod{a}$. Thus, since $b \not\equiv 0 \pmod{a}$, we see that

$$\begin{aligned} bp &\equiv by - z(by_2) \pmod{a} \\ bp &\equiv by - \lambda_1 z \pmod{a} \\ bp &\equiv by - by \pmod{a} \\ bp &\equiv 0 \pmod{a} \\ p &\equiv 0 \pmod{a} \\ \Rightarrow \mu &\in \mathbb{Z} \end{aligned}$$

For λ, since $(a, b) = 1$, we need only show that $q \equiv 0 \pmod{b}$ and $q \equiv 0 \pmod{c}$. We know that, by plugging $(x_1, a, 0)$ and $(x_2, y_2, 1)$ into (2.12), $x_1 \equiv 0 \pmod{b}$ and $\lambda_2 \equiv ax_2 \pmod{b}$. Since $\lambda_2 a \not\equiv 0 \pmod{b}$ (if it were, $\lambda_2 \equiv 0 \pmod{b}$, but this would mean $0 \equiv \lambda_2^2 \equiv -ac \pmod{b}$, which contradicts that a, b, c are pairwise relatively prime), we have that

$$\begin{aligned}
\lambda_2 aq &\equiv \lambda_2(ax) - \lambda_2(y - zy_2)x_1 - (\lambda_2 z)x_2 \\
&\equiv \lambda_2(ax) - \lambda_2 yx_1 + (\lambda_2 z)y_2 x_1 - (\lambda_2 z)x_2 \\
&\equiv \lambda_2^2 z + \lambda_2 z y_2 x_1 - (\lambda_2 z)ax_2 - \lambda_2 yx_1 \\
&\equiv \lambda_2 z(\lambda_2 + y_2 x_1 - ax_2) - \lambda_2 yx_1 \\
&\equiv \lambda_2 z(ax_2 + y_2 x_1 - ax_2) - \lambda_2 yx_1 \\
&\equiv \lambda_2 z y_2 x_1 - \lambda_2 yx_1 \\
&\equiv \lambda_2 x_1(zy_2 - y)
\end{aligned}$$

$$\begin{array}{rcll}
\lambda_2 aq &\equiv& 0 \pmod{b} & \text{or} \\
q &\equiv& 0 \pmod{b} & \text{or}
\end{array}
\qquad
\begin{array}{rcl}
\lambda_2 aq &\equiv& -\lambda_2 ax_1\mu \pmod{b} \\
q &\equiv& -x_1\mu \equiv 0 \pmod{b}
\end{array}$$

Finally, since, by (2.12) and plugging in members of B, we get $\lambda_3 y \equiv ax \pmod{c}$, $\lambda_3 \equiv x_1 \pmod{c}$, and $\lambda_3 y_2 \equiv ax_2 \pmod{c}$. Since $\lambda_3 \not\equiv 0 \pmod{c}$, we have

$$\begin{aligned}
\lambda_3 aq &\equiv \lambda_3 ax - \lambda_3 yx_1 + \lambda_3 z y_2 x_1 - \lambda_3 azx_2 \\
&\equiv \lambda_3 ax - \lambda_3 yx_1 + \lambda_3 z y_2 x_1 - \lambda_3^2 z y_2 \\
&\equiv \lambda_3 ax - \lambda_3 yx_1 + \lambda_3^2 z y_2 - \lambda_3^2 z y_2 \\
&\equiv \lambda_3 ax - \lambda_3^2 y \\
aq &\equiv ax - \lambda_3 y \\
aq &\equiv \lambda_3 y - \lambda_3 y \\
aq &\equiv 0 \\
q &\equiv 0 \pmod{c}
\end{aligned}$$

Thus, $q \equiv 0 \pmod{bc}$ and $\lambda \in \mathbb{Z}$, allowing B to be a basis for Λ.

b) Suppose $(x, y, z) \in \Lambda$. We want to show that $ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$. To do this, since a, b, c are pairwise relatively prime, by the Chinese Remainder Theorem, it is enough to show that $ax^2 + by^2 - cz^2 \equiv 0 \pmod{a}$, $\equiv 0 \pmod{b}$, and $\equiv 0 \pmod{c}$.

$$\begin{aligned} 0 &\equiv by - \lambda_1 z \pmod{a} \\ &\equiv (by - \lambda_1 z)(by + \lambda_1 z) \\ &\equiv b^2y^2 - \lambda_1^2 z^2 \\ &\equiv b^2y^2 - bcz^2 \\ &\equiv by^2 - cz^2 \\ 0 &\equiv ax^2 + by^2 - cz^2 \pmod{a} \end{aligned} \qquad \begin{aligned} 0 &\equiv ax - \lambda_2 z \pmod{b} \\ &\equiv (ax - \lambda_2 z)(ax + \lambda_2 z) \\ &\equiv a^2x^2 - \lambda_2^2 z^2 \\ &\equiv a^2x^2 - acz^2 \\ &\equiv ax^2 - cz^2 \\ 0 &\equiv ax^2 + by^2 - cz^2 \pmod{b} \end{aligned}$$

$$\begin{aligned} 0 &\equiv ax - \lambda_3 y \pmod{c} \\ &\equiv (ax - \lambda_3 y)(ax + \lambda_3 y) \\ &\equiv a^2x^2 - \lambda_3^2 y^2 \\ &\equiv a^2x^2 + aby^2 \\ &\equiv ax^2 + by^2 \\ 0 &\equiv ax^2 + by^2 - cz^2 \pmod{c} \end{aligned}$$

c) Let $\mathcal{P} = \{(x, y, z) \in \mathbb{R}^3 \mid |(x, y, z)| \leq 1\}$. The region $\mathcal{P}$ is a closed rectangular prism with side-lengths $2\sqrt{bc},\ 2\sqrt{ac},\ 2\sqrt{ab}$. Thus

$$\mathrm{Vol}(\mathcal{P}) = 8abc = 2^3 \,\mathrm{coVol}(\Lambda).$$

Since $\mathcal{P}$ is compact, the compact version of Minkowski's Convex Body Theorem (Theorem 13) which we described above applies to give $(x, y, z) \in \Lambda$ with $0 < |(x, y, z)| \leq 1$.

d) Part b) allows us to simply show that $-2abc < ax^2 + by^2 - cz^2 < 2abc$.

First, suppose $z \neq 0$. Since we know that $z^2 \leq ab$, then $-cz^2 \geq -abc$, and we have

$$-2abc < -abc \leq ax^2 + by^2 - cz^2 \leq ax^2 + by^2 - cz^2 \leq 2abc - cz^2 < 2abc.$$

Now, suppose that $z = 0$. This forces $x \neq 0$ or $y \neq 0$, and we have

$$0 < ax^2 + by^2 - cz^2 = ax^2 + by^2 \leq 2abc.$$

All we must do to finish is to show that $ax^2 + by^2 \neq 2abc$. Assume we have equality. Then we must have $x^2 = bc$ and $y^2 = ac$. (This is because $x^2 \leq bc$ and $y^2 \leq ac$, so if we have equality, the only possibility is that these must be equal.) Going mod a, we see that $a \mid by^2 \Rightarrow a \mid y^2 \Rightarrow a^2 \mid y^2 \Rightarrow a^2 \mid ac \Rightarrow a \mid c \Rightarrow a = 1$. A similar argument shows that $b = 1$ also. This means, however, that $x^2 = c \Rightarrow c = 1$. Thus, this is an exceptional case when $a = b = c = x = y = 1$, and $z = 0$. □

Before arriving at the main result of this section, consider the positive definite ternary integral quadratic form $q(x, y, z)$ with defining matrix $A^t \operatorname{diag}(a, b, c)A$. We need to recall the following elementary result of Gauss in order to complete the upcoming proof.

Theorem 15. *Let $q(x, y, z) \in \mathbb{Z}[x, y, z]$ be a positive definite ternary quadratic form given by a symmetric matrix $q(\vec{x}) = \vec{x}^t M \vec{x}$. We write* $\operatorname{disc} q$ *for* $\det M$.
a) There is an integral vector $\vec{u} \neq \vec{0}$ such that

$$q(\vec{u}) \leq (2 \operatorname{disc} q)^{1/3}.$$

b) Further, there is an integral vector $\vec{u} \neq \vec{0}$ such that

$$q(\vec{u}) < (2 \det(M))^{1/3}$$

unless q is integrally equivalent to a multiple of the form

$$q_0(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3.$$

Proof. See [1, Theorem II.III p. 33-4] or [10, § XI.6 p.112-7]. □

Here is the main result.

Theorem 16. *[3, Cochrane-Mitchell] Under the hypotheses of Legendre's theorem, there exists a small vector $(x, y, z) \in \Lambda$ which is a solution of (2.2).*

Remark: An element $\vec{v} \in \Lambda \setminus \{\vec{0}\}$ with $|\vec{v}|$ minimal need not be a solution to (2.2).

Proof. Suppose first that $a = b = 1$, so that as above, Legendre's conditions reduce to the existence of $\lambda_3 \in \mathbb{Z}$ such that $-1 \equiv \lambda_3^2 \pmod{c}$. In this special case the lattice Λ above reduces to the one defined by the single congruence condition

$$ax - \lambda_3 y \equiv 0 \pmod{c}.$$

Since this equation does not involve z, in this case Λ can be viewed as the set of all translates by integers $z = N$ of a lattice in the (x, y)-plane of volume c. This remark is useful because we can apply the two-dimensional Minkowksi's theorem to get the existence of a nonzero point (x_0, y_0) in the lattice with $x_0^2 + y_0^2 < 2c$. (To check this: the area of the disk $x^2 + y^2 < 2c$ is $2\pi c$, and $\pi > 2$, so the area of the disk is greater than 2^2 times the area of the lattice, which is $4c$.) Multiplying the congruence

$$x_0 - \lambda_3 y_0 \equiv 0 \pmod{c}$$

by $(x_0 + \lambda_3 y_0)$, we get

$$x_0^2 + y_0^2 \equiv (x_0 + \lambda_3 y_0)(x_0 - \lambda_3 y_0) \equiv (x_0 + \lambda_3 y_0) \cdot 0 \equiv 0 \pmod{c}.$$

So $x_0^2 + y_0^2$ is positive, less than $2c$ and congruent to 0 mod c; therefore we must have $x_0^2 + y_0^2 = c$ and thus

$$x_0^2 + y_0^2 - c(1)^2 = 0,$$

so $(x_0, y_0, 1)$ is a solution to the Legendre equation. Moreover

$$|(x_0, y_0, 1)| = \max\left(\frac{|x_0|}{\sqrt{c}}, \frac{|y_0|}{\sqrt{c}}, 1\right) = 1.$$

Suppose now that $\max(a, b) > 1$. By considering various cases we will construct an index 2 sublattice $\Lambda' \subset \Lambda$ with the following two properties:

(P1): Every vector $(x, y, z) \in \Lambda'$ satisfies the stronger congruence

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{2abc}. \tag{2.14}$$

(P2): Λ' contains a small solution.

This would certainly suffice to prove the theorem: let (x, y, z) be a small vector of Λ'. By Proposition 14, we have either $ax^2 + by^2 - cz^2 = 0$ or $ax^2 + by^2 - cz^2 = abc$, but now (P1) rules out the second alternative.

In what follows, we will construct different sublattices Λ' and show, on a case-by-case basis, that they satisfy (P1). Then at the end we will give an all-inclusive argument that they satisfy (P2).

Case 1: If a, b, c are all odd, then Λ' is simply the sublattice of Λ defined by the additional condition $x + y + z \equiv 0 \pmod 2$. No problem to see that this does what is claimed above.

Case 2: Suppose that one of a and b is even – WLOG we may suppose that a is even. Then any point in Λ satisfies $y \equiv z \pmod 2$.

Case 2a): If $b \equiv c \pmod 4$, then we take Λ' to be the index 2 sublattice defined by the additional congruence $x \equiv 0 \pmod 2$. Any point in Λ' satisfies

$$ax^2 + by^2 - cz^2 \equiv b(y^2 - z^2) \equiv 0 \pmod 4,$$

and therefore satisfies (2.14).

Case 2b): If $b \equiv -c \pmod 4$, we define Λ' by the additional congruence $x \equiv y \pmod 2$.

The congruence

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{abc}$$

implies

$$0 \equiv ax^2 + by^2 - cz^2 \equiv y^2 - z^2 \pmod{2},$$

so also $y \equiv z \pmod{2}$ and thus $x \equiv y \equiv z \pmod{2}$ and hence $x^2 \equiv y^2 \equiv z^2 \pmod{4}$. So any point in Λ' satisfies

$$ax^2 + by^2 - cz^2 \equiv x^2(2 + b - c) \equiv x^2(2 + 2b) \equiv x^2(2 + 2(2k + 1)) \equiv 4x^2(k + 1) \equiv 0 \pmod{4}$$

and is therefore a solution to (2.14).

Case 3: Suppose that c is even (hence a and b are odd), so any point in Λ satisfies

$$ax^2 + by^2 - cz^2 \equiv x^2 + y^2 \pmod{2},$$

so $x \equiv y \pmod{2}$.

Case 3a): If $a + b \equiv 2 \pmod{4}$, let Λ' be the index 2 sublattice satisfying $x \equiv z \pmod{2}$. As above we then have $x^2 \equiv y^2 \equiv z^2 \pmod{4}$, so any vector $(x, y, z) \in \Lambda'$ satisfies

$$ax^2 + by^2 - cz^2 \equiv x^2(a + b - 2) \equiv 0 \pmod{4}$$

and is therefore a solution to (2.14).

Case 3b): If $a + b \equiv 0 \pmod{4}$, let Λ' be the index 2 sublattice satisfying $z \equiv 0 \pmod{2}$. Then any point in Λ' satisfies

$$ax^2 + by^2 - cz^2 \equiv x^2(a + b) \equiv 0 \pmod{4}.$$

Thus, for every possible case, we have constructed an index 2 sublattice Λ' which satisfies property (P1). All that is left is to show that this Λ' satisfies (P2), or that it contains a small solution.

Let A be the 3×3 matrix such that

$$\Lambda' = A\mathbb{Z}^3.$$

The determinant of A is equal to the covolume of Λ', hence

$$\det A = 2abc.$$

Consider the positive definite ternary integral quadratic form $q(x, y, z)$ with defining matrix $A^t \operatorname{diag}(a, b, c)A$. Then Theorem 15 applies. Thus, we know that there is an integral vector $\vec{u} \neq 0$ such that $q(\vec{x}) < (2 \det(M))^{1/3}$ unless q is integrally equivalent to a multiple of the form $q_0(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2 + x_1x_2 + x_1x_3 + x_2x_3$.

Can our quadratic form q be integrally equivalent to a scalar multiple of q_0? Recall that $q(\vec{x}) = \vec{x}^t M \vec{x}$. If q is integrally equivalent to q_0, then this would mean that there exists some matrix $B \in GL_n(\mathbb{Z})$ such that, for $\vec{x} = B\vec{x'}$, we have $q(\vec{x}) = (\vec{x'})^t B^t M B \vec{x'}$. Since

$$M_{q_0} = \begin{pmatrix} 1 & \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & 1 & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} & 1 \end{pmatrix},$$

we have $\operatorname{disc} q_0 = \frac{1}{2}$. On the other hand,

$$\operatorname{disc} q = \det(A^t \operatorname{diag}(a, b, c)A) = \det(A)^2 abc = 4(abc)^3.$$

If we scale all entries of a 3×3 matrix by λ, then the determinant scales by λ^3, so if $q \cong \lambda q_0$ for some $\lambda \in \mathbb{Z}$, which means that q is integrally equivalent to a scalar multiple (λ) of q_0 as defined above, we must have $\lambda = 2abc$. From this it would follow that

$$\forall (x, y, z) \in \Lambda',\ ax^2 + by^2 + cz^2 \equiv 0 \pmod{2abc}.$$

But for all vectors in Λ' we have

$$ax^2 + by^2 - cz^2 \equiv 0 \pmod{2abc},$$

and these two congruences imply

$$z \equiv 0 \pmod{ab}.$$

But it is easy to check that in all cases except 3b) above, Λ' has a vector of the form $(x, y, 1)$, whereas in Case 3b) Λ' has a vector of the form $(x, y, 2)$, which gives a contradiction (since we are assuming $\max(a, b) > 1$, having already dealt with the case when $a = b = 1$). The contradiction is that, in Case 3b), ab is odd, and we can find a solution which has z even. Thus, $z \not\equiv 0 \pmod{ab}$.

Therefore there exists $\vec{v} \in \mathbb{Z}^3 \setminus \{\vec{0}\}$ with

$$q(\vec{v}) < (2 \operatorname{disc} q)^{1/3} = 2abc,$$

or equivalently, a nonzero vector $\vec{v} = (x_0, y_0, z_0) \in \Lambda'$ with

$$ax_0^2 + by_0^2 + cz_0^2 < 2abc.$$

It follows that

$$|ax_0^2 + by_0^2 - cz_0^2| < 2abc$$

and therefore

$$ax_0^2 + by_0^2 - cz_0^2 = 0.$$

□

2.6 Extensions of the Legendre Equation

There has been some work on extending the Legendre Equation to more than 3 variables. Notably, Hasse and Minkowski proved when solutions exist in the four-variable case. They proved further proved the following result:

Theorem 17. *[2, Theorem 6.1.1 p.75, given in this language on p. 3] Let $q(\vec{x}) \in \mathbb{Z}[x_1, \ldots, x_n]$ be a quadratic form. Suppose there exists a nonzero vector $\vec{0} \neq \vec{x} \in \mathbb{R}^n$ such that $q(\vec{x}) = 0$*

(this means that $q(\vec{x})$ is indefinite - not positive definite and not negative definite), and also that for all $N \in \mathbb{Z}^+$, there exist $x_1, \ldots, x_n \in \mathbb{Z}$ such that $q(x_1, \ldots, x_n) \equiv 0 \pmod{N}$ and $gcd(x_1, \ldots, x_n, N) = 1$ ($\vec{x}$ is primitive), then there exists $\vec{0} \neq \vec{x} \in \mathbb{Z}^n$ such that $q(\vec{x}) = 0$.

This work was done in the late 19th century, about 100 years after Legendre's original theorem in 1785. Then, Meyer, in 1884, proved that for $n \geq 5$, any quadratic form $q(\vec{x})$ which is not positive definite or negative definite (i.e. all coefficients are not the same sign) and not necessarily diagonal, then the equation $q(\vec{x}) = 0$ has an integral solution [2, Corollary 6.1.1 p. 75].

Chapter 3

The Extended Legendre Equation

3.1 Definitions

Let the **Extended Legendre Equation (ELE)** be the diagonal quadratic form with $\mathbb{Z}$-coefficients:

$$q(\vec{x}) = a_1x_1^2 + a_2x_2^2 + \cdots + a_{n-1}x_{n-1}^2 + a_nx_n^2 = 0, \quad a_i \in \mathbb{Z} \setminus \{0\} \quad \forall i \tag{3.1}$$

Specifically, we will consider the case in which we place the following restrictions on the coefficients:

$$a_1x_1^2 + a_2x_2^2 + \cdots + a_{n-1}x_{n-1}^2 - a_nx_n^2 = 0 \;\; a_i \in \mathbb{Z}^+ \setminus \{0\}, \; a_i \text{ squarefree and pairwise coprime} \tag{3.2}$$

Throughout these notes when we refer to "an Extended Legendre Equation," or "ELE," we will mean an equation of the form (3.2). The ELE **associated** with the quadratic form $q(\vec{x})$ is the ELE defined by $q(\vec{x}) = 0$. Notice that the *signature* of any ELE is $(n-1, 1)$, where there are $n-1$ coefficients which are positive and 1 which is negative. For $n > 3$, it is not true that any quadratic form in n variables is equivalent over $\mathbb{Z}$ to an ELE (e.g. one which has signature $(n-2, 2)$, for example). Even if an equation has signature $(n-1, 1)$, it still may not be able to be reduced over $\mathbb{Z}$ to an ELE, as could be done when $n = 3$. For example, the quadratic form $q(\vec{x}) = 2x_1^2 + 6x_2^2 + x_3^2 - x_4^2$ cannot be reduced to be an ELE with pairwise coprime coefficients. Thus, our assumptions on an ELE exclude many diagonal quadratic forms.

By a **solution** to the ELE (3.2), we mean $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, *not all zero*, such that $a_1x_1^2 + \cdots + a_{n-1}x_{n-1}^2 - a_nx_n^2 = 0$. Sometimes we say "nontrivial solution" for emphasis, but if ever we mean to consider the trivial solution we shall say so explicitly.

3.2 Results and Hopes for $n > 3$

Given a diagonal quadratic form in n variables, we want to find all of the solutions of the ELE associated with this quadratic form (i.e. we set the quadratic form $q(\vec{x}) = 0$). It was proven by Hasse-Minkowski in the late 19th century when such a quadratic form has a nontrivial solution (see Section (2.6)). Taking inspiration from Cochrane and Mitchell's 1998 paper, we wanted to prove it in a more elementary way than Hasse-Minkowski's, and in addition, to demonstrate a method for finding the solutions. We began by proving the results given in Cochrane and Mitchell's paper for n variables, where $n \in \mathbb{Z}^+$ and $n \geq 3$.

First, we define two norms which are analogous to those defined in Cochrane and Mitchell's paper.

3.2.1 Two Norms and Small Vectors

We generalize two norms introduced by Cochrane and Mitchell on $\mathbb{R}^3$. First, on $\mathbb{R}^n$, in our own notation,

$$|(x_1, x_2, \ldots, x_n)| = \max\Big(\frac{|x_i|}{\sqrt{a_1 \cdots a_{i-1}a_{i+1} \cdots a_n}}\Big),\ i = 1, 2, \ldots n.$$

This norm is an orthogonally rescaled ℓ_∞-norm, which has level sets which are rectangular boxes.

Cochrane and Mitchell also introduce a second norm which we generalize to $\mathbb{R}^n$:

$$||(x_1, x_2, \ldots, x_n)|| = \sqrt{a_1x_1^2 + a_2x_2^2 + \cdots + a_nx_n^2}.$$

This norm is an orthogonally rescaled ℓ^2-norm with level sets which are ellipsoids.

We will call a vector $\vec{x} \in \mathbb{R}^n$ **small vector** if $|(x_1, x_2, \ldots, x_n)| \leq 1$. We call a solution $\vec{x} \in \mathbb{Z}^n$ a **small solution** if $q(\vec{x}) = 0$ and $|\vec{x}| \leq 1$.

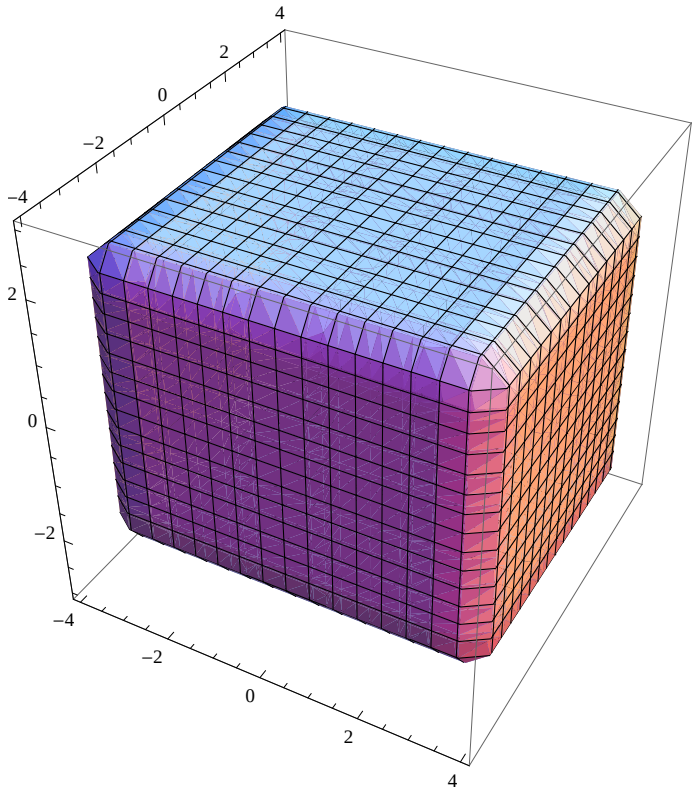

Figure 3.1: The first norm has a level set which is the surface of a rectangular solid, as is seen from this picture of solutions of $|(x, y, z)| = \max\left(\frac{|x|}{\sqrt{15}}, \frac{|y|}{\sqrt{10}}, \frac{|z|}{\sqrt{6}}\right) \leq 1$.

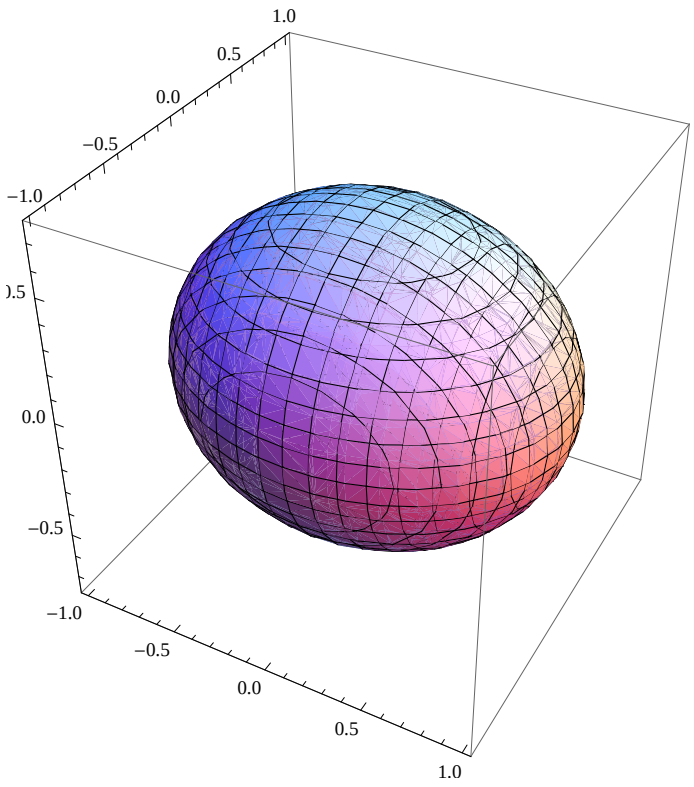

Figure 3.2: The second norm has a level set which is an ellipsoid, as is seen from this picture of solutions of $2x^2 + 3y^2 + 5z^2 < 2$.

Now we prove a result regarding solutions to (3.2).

Proposition 18. *If $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ is a solution to (3.2), then we have*

$$||(x_1, x_2, \ldots, x_n)|| = \sqrt{2a_1a_2\cdots a_{n-1}a_n}\ |(x_1, x_2, \ldots, x_n)|.$$

Consequently, a solution $(x_1, x_2, \ldots, x_n)$ is small iff

$$a_1x_1^2 + a_2x_2^2 + \cdots a_{n-1}x_{n-1}^2 + a_nx_n^2 \leq 2a_1a_2\cdots a_{n-1}a_n.$$

Proof. First, suppose $(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$ is a solution to (3.2). Then $a_1x_1^2 + a_2x_2^2 + \cdots + a_{n-1}x_{n-1}^2 = a_nx_n^2$, which, since every term in the equation is nonnegative, forces $|(x_1, x_2, \ldots, x_n)| = \frac{|x_n|}{\sqrt{a_1a_2\cdots a_{n-1}}}$. To prove the first claim, it is equivalent to show that the squares of both sides are equal. Thus,

$$\left(\sqrt{2a_1a_2\cdots a_{n-1}a_n}\,|(x_1, x_2, \ldots, x_n)|\right)^2 = 2a_1a_2\cdots a_{n-1}a_n\left(\frac{x_n^2}{a_1a_2\cdots a_{n-1}}\right) = 2a_nx_n^2 = a_nx_n^2 + a_nx_n^2$$

$$= a_1x_1^2 + a_2x_2^2 + \cdots + a_{n-1}x_{n-1}^2 + a_nx_n^2 = ||(x_1, x_2, \ldots, x_n)||^2.$$

□

3.2.2 The Existence of Small Solutions to a Quadratic Form in n Variables

In order for a proof like Cochrane and Mitchell's to succeed for an ELE $q(\vec{x}) = 0$ in n variables, we need to be able to find a **mythical lattice** $\Lambda \subset \mathbb{Z}^n$ with the following properties:

(L1) The covolume of Λ is $\alpha = a_1a_2\cdots a_n$.

(L2) If $\vec{x} = (x_1, \ldots, x_n)$ and $\vec{x} \in \Lambda$, then $q(\vec{x}) \equiv 0 \pmod{\alpha}$.

Proposition 19. *Let $n \geq 3$, and $(a_1, \ldots, a_n)$ be squarefree, pairwise coprime positive integers. Suppose that $q(\vec{x})$ is as in (3.2) and $q(\vec{x}) \equiv 0 \pmod{N}$ has nontrivial solutions for all positive integers N. Suppose also that we can find a mythical lattice $\Lambda \subset \mathbb{Z}^n$ which contains a sublattice $\Lambda' \subset \Lambda$ of index $n-1$ which has the property that $\vec{v} \in \Lambda' \implies q(\vec{v}) \equiv 0 \pmod{(n-1)\alpha}$. Then there exists $\vec{x} = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ with $q(\vec{x}) = 0$ and $0 < |\vec{x}| \leq 1$ (i.e. $q(\vec{x}) = 0$ has a small solution).*

Proof. The argument here is only valid for $n > 3$; the case $n = 3$ was given a complete treatment in Cochrane-Mitchell [3]. Moreover, we may assume that $\alpha = a_1 \cdots a_n > 1$, since the case $a_1 = \cdots = a_n = 1$ is trivial: there are nontrivial solutions $\vec{x}$ with $|\vec{x}| = 1$, $||\vec{x}|| = \sqrt{2}$, and these bounds are best possible.

Let $\mathcal{P}_1 = \{\vec{x} \in \mathbb{R}^n | \ |\vec{x}| \leq 1\}$ be the set of all small vectors in $\mathbb{R}^n$. Let $\vec{x} = (x_1, \ldots, x_n) \in \mathcal{P}_1$ be a small solution. We claim that

$$|q(\vec{x})| < (n-1)\alpha. \tag{3.3}$$

Case 1: Suppose $x_n \neq 0$. From $|\vec{x}| \leq 1$, we have $a_n x_n^2 \leq \alpha$ because an ELE has signature $(n-1, 1)$, so

$$-(n-1)\alpha < -\alpha \leq a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 - a_n x_n^2$$

Also,

$$a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 - a_n x_n^2 \leq (n-1)\alpha - a_n x_n^2 < (n-1)\alpha$$

Case 2: Suppose $x_n = 0$. Then, since $\vec{x} \neq \vec{0}$ and $|\vec{x}| \leq 1$ we have $x_i^2 \leq \prod_{j \neq i} a_j \Rightarrow a_i x_i^2 \leq \alpha$, and hence $a_i x_i^2 \leq \alpha \forall i = 1, \ldots, n$. Thus,

$$0 < a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 = a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 - a_n x_n^2 \leq (n-1)\alpha$$

It remains to show that $a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 \neq (n-1)\alpha$. But if we have equality, then all $n-1$ of our inequalities must be sharp:

$$x_1^2 = a_2 \cdots a_n, \ x_2^2 = a_1 a_3 \cdots a_n, \ \ldots, \ x_{n-1}^2 = a_1 \cdots a_{n-2} a_n$$

Since the a_i's are squarefree and pairwise coprime, the right hand sides of all the equations above are squarefree. Since the left hand sides are squares, we get complete degeneration: $x_1 = \cdots = x_{n-1} = a_1 = \cdots = a_n = 1$, so $\alpha = a_1 \cdots a_n = 1$, contrary to the assumption made at the beginning of the proof. Therefore, $|q(\vec{x})| < (n-1)\alpha$ for $\vec{x} \in \mathcal{P}_1$.

Assuming now that $n > 3$, we apply Minkowski's Convex Body Theorem to $\mathcal{P}_1$ and the index $n-1$ sublattice Λ' of Λ assumed to exist in the statement of the proof. To satisfy the

hypotheses of the theorem, we want to show that the covolume of Λ times 2^n is less than or equal to the volume of $\mathcal{P}_1$, which can be calculated by finding the product of all of the side lengths of the rectangular box generated by the orthogonalized ℓ_∞ norm being less than or equal to 1. The side length in the ith direction, then, will be $2\sqrt{a_1 \cdots a_{i-1} a_{i+1} \cdots a_n}$. Hence, the volume of $\mathcal{P}_1$ will be the product of all of the side lengths, or $\operatorname{Vol} \mathcal{P}_1 = 2a_1^{\frac{n-1}{2}} \cdots 2a_n^{\frac{n-1}{2}} = 2^n \alpha^{\frac{n-1}{2}}$. Thus, $\operatorname{Vol} \mathcal{P}_1 = 2^n \alpha^{\frac{n-1}{2}}$ and $\operatorname{coVol} \Lambda' = [\Lambda : \Lambda'] \operatorname{coVol} \Lambda = (n-1)\alpha$, Minkowski's Theorem may be applied *provided*

$$\operatorname{Vol} \mathcal{P}_1 \geq 2^n \operatorname{coVol} \Lambda'$$

$$2^n \alpha^{\frac{n-1}{2}} \geq 2^n (n-1)\alpha$$

or equivalently, provided that

$$\alpha \geq (n-1)^{\frac{2}{n-3}} \tag{3.4}$$

Since $n > 3$, $\frac{n-3}{2} > 0$, and therefore for any fixed n and all but finitely many tuples $(a_1, \ldots, a_n) \in (\mathbb{Z}^+)^n$, the inequality (3.4) holds. Thus, apart from finitely many exceptional tuples, there exists a vector $\vec{x} \in \Lambda' \subset \Lambda$ with $0 < |\vec{x}| \leq 1$. By the hypothesis on Λ', we have $q(\vec{x}) \equiv 0 \pmod{(n-1)\alpha}$, whereas by (3.3) we have $|q(\vec{x})| < (n-1)\alpha$. We conclude that $q(\vec{x}) = 0$, i.e. $\vec{x} \in \mathbb{Z}^n$ is a small solution to the ELE associated with $q(\vec{x})$.

For each $n > 3$, we must deal with the finite set of tuples $(a_1, \ldots, a_n)$ such that $\alpha < (n-1)^{\frac{2}{n-3}}$. Put $C(n) = (n-1)^{\frac{2}{n-3}}$. Then a calculus exercise shows that $\lim_{n \to \infty} C(n) = 1$ and that $C(n) \leq 2$ for all $n \geq 9$. Note that when $n \geq 9$, we have $C(n) \leq 2$, and $\alpha \geq 2$. In these cases, all $q(\vec{x})$ which are not the case when $a_i = 1$ are valid to use Minkowski. Thus, the set of exceptions is empty except possibly in the range of $4 \leq n < 9$. For $4 \leq n \leq 8$ we simply enumerate the exceptional tuples and show one by one that small solutions exist.

Case 1: $6 \leq n \leq 8$. Then $2 < C(n) < 3$, so the only exceptional tuples are those with $\alpha = 2$ (and $\alpha = 1$, which we dealt with at the beginning of the proof). In other words, exactly one of the a_i's is equal to 2 and the remainder are 1. If $a_n = 1$, then we can choose $I < n$ with

$a_I = 1$ and take $x_I = x_n = 1$, $x_i = 0$ for all other i: this is a small solution. If $a_n = 2$ and $a_i = 1$ for all $1 \leq i \leq n-1$, take $x_1 = x_2 = x_n = 1$, $x_i = 0$ for $2 < i < n$.

Case 2: $n = 5$. We see that $C(n) = 4$, so the exceptional tuples are those with $\alpha = 2$ or $\alpha = 3$. First, we check to find small solutions for every possible combination of coefficients that will make $\alpha = 2$. We present our results using the following tables, where $\vec{a}$ is the vector which lists the coefficients, and $\vec{x}$ is the small solution that was found. Notice that because the first $n-1$ variables have the same signed coefficients, they are symmetric. Thus, checking only one of the possibilities for the positive coefficients suffices.

Table 3.1: A list of small solutions when $n = 5$ and $\alpha = 2$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 4$
$(2,1,1,1,1)$	$(0,1,0,0,1)$	2	Yes!
$(1,1,1,1,2)$	$(1,1,0,0,1)$	4	Yes!

Table 3.2: A list of small solutions when $n = 5$ and $\alpha = 3$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 6$
$(3,1,1,1,1)$	$(0,1,0,0,1)$	2	Yes!
$(1,1,1,1,3)$	$(1,1,1,0,1)$	6	Yes!

From the above tables, we see that for all values of α when $n = 5$, small vectors can be found.

Case 3: $n = 4$. $C(4) = 9$, so there are many more exceptions, those with $\alpha = 2, 3, 4, 5, 6, 7, 8$. We list our results in the tables below.

Table 3.3: A list of small solutions when $n = 4$ and $\alpha = 2$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 4$
$(2,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,2)$	$(1,1,0,1)$	4	Yes!

Table 3.4: A list of small solutions when $n = 4$ and $\alpha = 3$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 6$
$(3,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,3)$	$(1,1,1,1)$	6	Yes!

Table 3.5: A list of small solutions when $n = 4$ and $\alpha = 4$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 8$
$(4,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,4)$	$(2,0,0,1)$	8	Yes!
$(2,1,1,2)$	$(1,0,0,1)$	4	Yes!
$(2,2,1,1)$	$(0,0,1,1)$	2	Yes!

Table 3.6: A list of small solutions when $n = 4$ and $\alpha = 5$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 10$
$(5,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,5)$	$(1,2,0,1)$	10	Yes!

Table 3.7: A list of small solutions when $n = 4$ and $\alpha = 6$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 12$
$(6,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,6)$	$(1,1,2,1)$	12	Yes!
$(2,3,1,1)$	$(0,0,1,1)$	2	Yes!
$(2,1,1,3)$	$(1,1,0,1)$	6	Yes!
$(3,1,1,2)$	$(0,1,1,1)$	4	Yes!

Table 3.8: A list of small solutions when $n = 4$ and $\alpha = 7$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 14$
$(7,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,7)$	$---$	$None$	No

Table 3.9: A list of small solutions when $n = 4$ and $\alpha = 8$.

$\vec{a}$	$\vec{x}$	$\|\|\vec{x}\|\|^2$	$\|\|\vec{x}\|\|^2 \overset{?}{\leq} 2\alpha = 16$
$(8,1,1,1)$	$(0,1,0,1)$	2	Yes!
$(1,1,1,8)$	$(2,2,0,1)$	16	Yes!
$(4,2,1,1)$	$(0,0,1,1)$	2	Yes!
$(4,1,1,2)$	$(0,1,1,1)$	4	Yes!
$(2,1,1,4)$	$(0,2,0,1)$	8	Yes!
$(2,2,2,1)$	$(1,1,0,2)$	8	Yes!
$(2,2,1,2)$	$(0,1,0,1)$	4	Yes!

In Table 3.8, we have our first encounter with a small solution not being found. However, using the Three-Squares Theorem and a lemma from Davenport-Cassels, we can show that the equation $x_1^2 + x_2^2 + x_3^2 = 7x_4^2$ does not have any solutions. A quick argument of that follows: The Three Squares Theorem by Lagrange states that a positive integer $n \in \mathbb{Z}^+$ can be written as the sum of three integral squares iff $n \neq 4^a(8k+7)$ for $a \geq 0,\ k \in \mathbb{Z}$. Thus, $7 = 4^0(8(0)+7)$ cannot be written as the sum of three integral squares. Since we can write the equation above as

$$\left(\frac{x_1}{x_4}\right)^2 + \left(\frac{x_2}{x_4}\right)^2 + \left(\frac{x_3}{x_4}\right)^2 = 7$$
$$\implies X^2 + Y^2 + Z^2 = 7$$

we know that no integers X, Y, Z exist which satisfy the equation. By the contrapositive of the Davenport-Cassels Lemma [11], there exist no rational numbers $X', Y', Z' \in \mathbb{Q}$ such that $X'^2 + Y'^2 + Z'^2 = 7$. Thus, this equations has no solutions at all in $\mathbb{Z}$ or in $\mathbb{Q}$. We couldn't possibly have found a small solution, then!

Notice that we found small solutions to every ELE which we needed to check by hand which did, indeed, have solutions. Because of this, we have shown that we can find a small solution to every $q(\vec{x})$ which has solutions, and the proof is complete. □

Now that we had proved all of these beautiful theorems, all that was left was to find the existence of this mysterious lattice, Λ which has a covolume α and in which for every member $\vec{v}$ of the lattice, $q(\vec{v}) \equiv 0 \pmod{\alpha}$.

3.3 The Non-Existence of a Mythical Lattice for an ELE when $n \geq 4$

Now, we have come to the main result of this chapter. The foreshadowing nature of the name of a mythical lattice may have given you a clue. We will prove that for $n \geq 4$, a mythical lattice does not exist. To prepare for the argument, a derivation is introduced.

3.3.1 Derivation

Let k be a field, and let $R = k[x_1, \ldots, x_n]$ be the polynomial ring formed by adjoining finitely many variables to k. A **k-derivation** on R is a map $d : R \to R$ such that the following hold:

1. $d(\alpha) = 0 \quad \forall \quad \alpha \in k$
2. $d(x + y) = d(x) + d(y)$
3. $d(xy) = \big(d(x)\big)y + x\big(d(y)\big)$

Because of these properties, a derivation is completely determined by what it does on the adjoined elements $x_1, \ldots, x_n$. Also, note that the derivation as described above, sometimes denoted $Der_k(R, R)$, is a k-vector space, with a basis given by $\frac{\partial}{\partial x_1}, \ldots, \frac{\partial}{\partial x_n}$, where we define

$$\frac{\partial}{\partial x_i} x_j = \begin{cases} 1 & , \quad i = j \\ 0 & , \quad i \neq j \end{cases}$$

Let $f : k^n \to k$ be a function in R. We define the **gradient of** f to be $\bigtriangledown f = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right)$. We say a point $\vec{x} \in k^n$ is **singular** if $\bigtriangledown f(\vec{x}) = \vec{0}$, and we call the set of all singular points of f the **locus of singularity of** f.

Now we are ready for the main result.

3.3.2 Non-Existence Result

Theorem 20. *For an ELE in $n \geq 4$ variables,*

$$q(\vec{x}) = a_1 x_1^2 + \cdots + a_{n-1} x_{n-1}^2 - a_n x_n^2 = 0, \qquad a_i \in \mathbb{Z}^+ \setminus \{0\} \quad \forall i$$

when $\alpha = a_1 \cdots a_n$ is divisible by an odd prime, there does not exist a mythical lattice.

Proof. Let $q(\vec{x})$ be given as in the statement of the theorem. Let p be an odd prime dividing α. Since the a_i's are pairwise coprime and squarefree, then p must divide exactly one of the a_i's. Without loss of generality, suppose $p|a_1$. Suppose a mythical lattice, $\Lambda \subseteq \mathbb{Z}^n$, exists. Then we know that it satisfies properties (L1) and (L2). Define $\iota : \Lambda \longrightarrow (\mathbb{Z}/p\mathbb{Z})^n$ to be the natural map which takes a vector in Λ, considers it as a vector in $\mathbb{Z}^n$, and then takes each entry of the vector modulo p. Let $\iota(\Lambda) = \overline{\Lambda}$. It may be seen that $\overline{\Lambda}$ is a hyperplane in $(\mathbb{Z}/p\mathbb{Z})^n$. In other words, $\overline{\Lambda}$ is $(n-1)$-dimensional. A brief argument is given here.

First, note that by identifying Λ with the subgroup $\Lambda \leq \langle \Lambda, p\mathbb{Z}^n \rangle \leq \mathbb{Z}^n$, by the Isomorphism Theorems, $[(\mathbb{Z}/p\mathbb{Z})^n : \overline{\Lambda}] = [\mathbb{Z}^n : \langle \Lambda, p\mathbb{Z}^n \rangle]$. Let $m := [\mathbb{Z}^n : \langle \Lambda, p\mathbb{Z}^n \rangle]$. Then, since $[\mathbb{Z}^n : \Lambda] = \alpha$ and $[\mathbb{Z}^n : (p\mathbb{Z})^n] = p^n$ and m divides them both, then m divides their gcd, and $\gcd(\alpha, p^n) = p$. Hence, $m = 1$ or $m = p$. Our goal is to show that $m \neq 1$.

Since $p|\alpha = [\mathbb{Z}^n : \Lambda]$, by Cauchy's Theorem (a special case of Sylow's First Theorem), there exists an element $\vec{x} \in \mathbb{Z}^n/\Lambda$ of order p. In other words, $\exists\ \vec{x} \notin \Lambda$ such that $p\vec{x} \in \Lambda$. Take this $\vec{x}$.

Claim: $\vec{x} \neq \vec{v} + p\vec{w}$, where $\vec{v} \in \Lambda,\ \vec{w} \in \mathbb{Z}^n$. Suppose the contrary. Then, if $\alpha = p\beta$ where $\gcd(p, \beta) = 1$, we can find $a, b \in \mathbb{Z}$ with $1 = a\beta + bp$. Then, multiplying through by β, we get

$$\beta\vec{x} = \beta\vec{v} + \beta p\vec{w} = \beta\vec{v} + \alpha\vec{w}$$

But $\vec{w} \in \mathbb{Z}^n$, and $[\mathbb{Z}^n : \Lambda] = \alpha$, so $\alpha\vec{w} \in \Lambda$. Hence, $\beta\vec{x} \in \Lambda$. However, we know that

$$\vec{x} = 1 \cdot \vec{x} = (a\beta + bp)\vec{x} = a(\beta\vec{x}) + b(p\vec{x}) \in \Lambda$$

which contradicts our assumption that $\vec{x} \notin \Lambda$. Thus, $\vec{x} \notin \langle \Lambda, p\mathbb{Z}^n \rangle$, and $m \neq 1$, which forces $m = p$. Therefore, $\overline{\Lambda}$ is $(n-1)$-dimensional.

Now, define $Q = \{\vec{v} \in (\mathbb{Z}/p\mathbb{Z})^n : q(\vec{v}) \equiv 0 \pmod{p}\}$. Clearly, $\overline{\Lambda} \subseteq Q$, since for any element $\vec{v} \in \overline{\Lambda}$, $q(\vec{v}) \equiv 0 \pmod{\alpha} \Rightarrow q(\vec{v}) \equiv 0 \pmod{p}$ since p divides α.

Since Λ is a lattice, it is defined by a linear function, and going modulo p, this function defines the hyperplane we have called $\overline{\Lambda}$. We may suppose that the function $L_1(\vec{x}),\ \vec{x} \in (\mathbb{Z}/p\mathbb{Z})^n$ defines $\overline{\Lambda}$. We claim that $L_1(\vec{x})$ divides $q(\vec{x})$ over $\mathbb{Z}/p\mathbb{Z}$. This means that $q(\vec{x})$ is the product of two linear factors since if L_1 divides q and q is quadratic, the other factor must also be linear. This would mean that $q(\vec{x}) \equiv L_1(\vec{x})L_2(\vec{x}) \pmod{p}$.

Take the associated bilinear form of $q(\vec{x})$ to be

$$B(\vec{v}, \vec{w}) := \frac{1}{2}(q(\vec{v} + \vec{w}) - q(\vec{v}) - q(\vec{w}))$$

Choose a basis, say $\vec{e_1}, \ldots, \vec{e_{n-1}}$ for $\overline{\Lambda}$ over $\mathbb{F}_p$. Then this bilinear form has an associated square matrix, say M, which is $(n-1) \times (n-1)$. We know that $M(i,j) = B(\vec{e_i}, \vec{e_j})$ by the definition of the associated matrix. But since for every $\vec{x} \in \overline{\Lambda}$, we have $q(\vec{x}) \equiv 0 \pmod{p}$, $B(\vec{e_i}, \vec{e_j}) = \frac{1}{2}(0-0-0) = 0 \ \ \forall\, i,j \in \{1, \ldots, n-1\}$. Hence, $M = 0$, the zero matrix. Now, let K be any field extension of $\mathbb{F}_p$. Then $\overline{\Lambda}$ determines an $(n-1)$-dimensional subspace of K^n, defined by the linear equation $L_1(\vec{x}) = 0$. Also, we may consider q as a quadratic form on K^n. Performing all of the above calculations in the same way, but considering the coefficients to be in K rather than in $\mathbb{F}_p$, we see that they all hold true. Hence, M is the same zero matrix as above! Defining $\overline{\Lambda}(K) = \{\vec{x} \in K^n : L_1(\vec{x}) = 0\}$, we see that for all $\vec{v} \in \overline{\Lambda}(K)$, we have $q(\vec{v}) = 0$. Since this is true for all field extensions K of $\mathbb{F}_p$, we may take K to be an algebraic closure of $\mathbb{F}_p$. Exploiting Nullstellensatz [5], we see that $L_1(\vec{x}) | q(\vec{x})$ over K^n. By the uniqueness of the results in the Euclidean algorithm, we find that since we have found a factorization over K^n, it must be the same factorization over the subfield $\mathbb{F}_p^n$.

Thus, we may now define $L_1(\vec{x}) := c_1x_1 + \cdots + c_nx_n$ and $L_2(\vec{x}) := d_1x_1 + \cdots + d_nx_n$, where $c_i, d_i \in \mathbb{Z}/p\mathbb{Z}$, and with $q(\vec{x}) \equiv L_1(\vec{x})L_2(\vec{x}) \pmod{p}$. Let $f(\vec{x}) = L_1(\vec{x})L_2(\vec{x})$ for convenience. Now, consider all of the points where q and f are singular. We do this by looking at each of

their gradients and setting them equal to zero.

$$\bigtriangledown q(\vec{x}) = \left(\frac{\partial q}{\partial x_1}, \ldots, \frac{\partial q}{\partial x_n}\right) = (2a_1x_1, \ldots, 2a_{n-1}x_{n-1}, -2a_nx_n)$$

$$\equiv (0, 2a_2x_2, \ldots, 2a_{n-1}x_{n-1}, -2a_nx_n) \pmod{p}$$

If we now set the gradient congruent to 0 modulo p, we will find all of the place where q is singular.

$$\bigtriangledown q(\vec{x}) \equiv 0 \pmod{p} \Leftrightarrow \vec{x} = (y, 0, \ldots, 0), \quad y \in \mathbb{Z}/p\mathbb{Z}$$

Thus, the locus of singularity for q is the line $\ell(y) = \{(y, 0, 0, 0) | y \in \mathbb{Z}/p\mathbb{Z}\}$, and lines are 1-dimensional. Now, we do the same for f.

$$\bigtriangledown f(\vec{x}) = \left(\frac{\partial f}{\partial x_1}, \ldots, \frac{\partial f}{\partial x_n}\right) = \Big(c_1L_2(\vec{x}) + d_1L_1(\vec{x}), \ldots, c_nL_2(\vec{x}) + d_nL_1(\vec{x})\Big)$$

Note that if $\vec{v}$ is a solution to both L_1 and L_2 (i.e. $L_1(\vec{v}) \equiv 0 \equiv L_2(\vec{v}) \pmod{p}$), then $\bigtriangledown f(\vec{v}) \equiv (0, \ldots, 0)$. Thus, the intersection of these two linear equations is contained in the locus of singularity for $f = L_1L_2$. But, calculating the dimension, we get $\dim(L_1 \cap L_2) \geq n - 1 - 1 = n - 2$.

Since the locus of singularity of q is 1-dimensional and the locus of singularity of f is *at least* $n - 2 > 1$, q and f have different loci of singularity. Thus, $q(\vec{x}) \neq L_1(\vec{x})L_2(\vec{x})$, and it *must* be false that we can factor q into linear factors modulo p. Therefore, we conclude that no such mythical lattice exists. □

Recall that in the case of $n = 3$, Cochrane and Mitchell did indeed find a (not so) mythical lattice. The contradiction used in this proof does not apply to that case since the dimension of the intersection of two 2-dimensional planes is indeed a 1-dimensional line, and the dimensions of the loci of singularity match.

Also, if $p = 2$, $\bigtriangledown q(\vec{x}) = (2a_1x_1, \ldots, 2a_{n-1}x_{n-1}, -2a_nx_n) \equiv (0, \ldots, 0) \pmod{2}$. There is no contradiction here, and any point where $L_1(\vec{x}) = -\frac{c_i}{d_i}L_2(\vec{x})$ for all i gives a point in the gradient of both functions. This implies the function is always factorable here.

Note that we did not yet address the case when α is *not* divisible by an odd prime. In these cases, it is easy to see that the existence of a small solution exists without too much trouble. We will list the cases here:

(1) If $\alpha = 1$, then $a_i = 1 \ \ \forall i$. Hence, the solution $\vec{x} = (1, 0, \ldots, 0, 1)$ has $|\vec{x}| = 1$, and hence is small.

(2) If $\alpha = 2$, then because of the symmetric nature of $a_1, \ldots, a_{n-1}$, there are two sub-cases.

   (a) Suppose, without loss of generality, that $a_1 = 2$ and $a_i = 1$ for $i \neq 1$. Then a solution $\vec{x} = (0, \ldots, 0, 1, 1)$ is indeed small since $|\vec{x}| = \frac{1}{\sqrt{2}} \leq 1$.

   (b) Suppose now that $a_1 = \cdots = a_{n-1} = 1$ and $a_n = 2$. Then a solution is $\vec{x} = (0, \ldots, 0, 1, 1, 1)$, which is also small because $|\vec{x}| = 1$.

Hence, the cases when α is not divisible by an odd prime are not a bother to us since we can easily find a small solution without constructing a lattice.

3.4 Further Research Opportunities

Although we discovered that we cannot find a mythical lattice in the case of an ELE, there are more questions that could be researched related to this topic. Here are a few of them.

- The biggest open problem is to get *sharp* bounds on the size of a solution in more variables than three. Although Hasse and Minkowski proved the existence of solutions and Ou-Williams proved a bound, they are not the best possible as Holzer's bound is in three variables.

- Is it possible to prove Hasse-Minkowski by a geometry of numbers argument?

- Is it possible to construct a mythical lattice if we are given an ELE whose coefficients are *not* pairwise coprime?

- Given a quadratic form which you know has solutions, or even a solution which is "small" in some way, how do you go about finding it explicitly? Brute force is a bit slow, especially for large coefficients.

Bibliography

[1] Cassels J.W.S. An introduction to the geometry of numbers [corrected reprint of the 1971 edition]. Classics in Mathematics. Berlin: Springer-Verlag; 1997.

[2] Cassels J.W.S. Rational quadratic forms. London: Academic Press; 1978.

[3] Cochrane T., Mitchell P. Small solutions of the Legendre equation. J. Number Theory. 1998; 70(1):62-66.

[4] Cox D.A. Primes of the form $x^2 + ny^2$: Fermat, class field theory and complex multiplication. New York: John Wiley & Sons, Inc.; 1989.

[5] Dummit D.S., Foote R.M. Abstract algebra. 3rd ed. Hoboken, NJ: John Wiley & Sons, Inc.; 2004.

[6] Ireland K., Rosen M. A classical introduction to modern number theory. 2nd ed. New York: Springer-Verlag; 1990.

[7] Mordell L.J. On the magnitude of the integer solutions of the equation $ax^2 + by^2 + cz^2 = 0$. J. Number Theory. 1969; 1: 1-3.

[8] Nagell T. Introduction to number theory. 2nd ed. New York: Chelsea Publishing Company; 1964.

[9] Niven I., Zuckerman H.S., Montgomery H.L. An introduction to the theory of numbers. 5th ed. New York: John Wiley & Sons, Inc.; 1991.

[10] Siegel C.L. Lectures on the geometry of numbers. Berlin: Springer-Verlag; 1989.

[11] Small C. Sums of three squares and levels of quadratic number fields. The American Mathematical Monthly. 1986; 93(4): 276-9.

[12] Williams K.S. On the size of a solution of Legendre's equation. Utilitas Math. 1998;34:65-72.