SOLUTIONS OF THE CUBIC FERMAT EQUATION IN QUADRATIC FIELDS

BY

MARVIN JONES

A Thesis Submitted to the Graduate Faculty of

WAKE FOREST UNIVERSITY GRADUATE SCHOOL OF ARTS AND SCIENCES

in Partial Fulfillment of the Requirements

for the Degree of

MASTER OF ARTS

Mathematics

May 2012

Winston-Salem, North Carolina

Approved By:

Jeremy A. Rouse, Ph.D., Advisor

Fredric T. Howard, Ph.D., Chair

Kenneth S. Berenhaut, Ph.D.

Acknowledgments

First and foremost, I'd like to thank my advisor, Jeremy Rouse. Without his patience and guidance this thesis would have been impossible. Not only did he provide direction to this thesis, but he is also responsible for my entire knowledge of number theory. His passion and enthusiasm for the subject has inspired me to continue my pursuit of mathematics, especially number theory. I am very thankful to have met Dr. Rouse, he has been the most supportive and caring professor that I have had the pleasure of working with.

I would also to acknowledge Dr. Howard and Dr. Berenhaut for their interest and support of my thesis, as well as the changes they suggested.

I am indebted to Jesse Thorner and Rick Freedman for their friendship. I was able to exchange ideas and frustrations with them. They helped me maintain the confidence to continue my work, and offered distractions when a break was needed. I would also like to acknowledge Kristine Hofmann for her proofreading despite having little interest in the subject matter or interest. Thanks to her, the editing process went by much faster.

Finally, I would like to thank my family for their continuing support throughout my life. They have always been there when I was doubtful of my abilities, and I know without them I would not be here.

Table of Contents

Acknowledgments ii

Abstract iv

Chapter 1 Introduction 1

Chapter 2 Preliminaries 6
2.1 Algebra and Number Theory 6
2.2 Elliptic Curves 8
2.3 Modular Forms 11

Chapter 3 The Proof 20
3.1 Introduction 20
3.2 The Fermat cubic and an elliptic curve 21
3.3 Modularity of the Fermat cubic in quadratic fields 29

Bibliography 38

Appendix A Tables 41

Vita 45

Abstract

Marvin Jones

We will examine when there are nontrivial solutions to the equation $x^3 + y^3 = z^3$ in $\mathbb{Q}(\sqrt{d})$ for a squarefree integer d. In this variation of Fermat's Last Theorem, it is possible for nontrivial solutions to exist in $\mathbb{Q}(\sqrt{d})$ for some choices of d, but not for all. Our argument assumes the Birch and Swinnerton-Dyer conjecture and follows a similar argument as Tunnell's solution to the congruent number problem.

Chapter 1: Introduction

In 1637, Pierre de Fermat scribbled that $x^n + y^n = z^n$ has no nontrivial integer solutions for $n > 2$ in his copy of the *Arithmetica*. His 'marvelous' proof was omitted due to narrow margins. A nontrivial solution is a solution where x, y and z are all nonzero. After all of Fermat's other claims had been settled, this statement became affectionately known as Fermat's Last Theorem (FLT). For over three centuries, many mathematicians attempted to prove FLT with little success. For a more thorough history on FLT, see [7, pg 252-258], [19] and [20].

For the most part, the progress made on FLT was proving individual cases; for instance Fermat proved the $n = 4$ case and Euler proved $n = 3$. Any integer $n > 2$ is either a multiple of 4 or a multiple of some prime $p > 2$; this means that showing FLT is true for all n relies on only showing the prime cases and $n = 4$. By 1992, FLT was known to be true for $n \leq 4000000$. Unfortunately, knowing FLT is true for that many cases does not get mathematicians any closer to the general result. Many proofs were produced for FLT for all n, however a correct proof was not achieved prior to 1994.

In the 20^{th} century, the machinery required to prove FLT emerged. In 1957, Taniyama and Shimura conjectured that every rational elliptic curve was modular. In the 1980s, Frey conjectured that FLT and the Taniyama-Shimura conjecture might be dependent. Serre was able to make progress on proving Frey's conjecture; the gap in his argument went on to be known as the $\epsilon-$conjecture. Ribet proved the $\epsilon-$conjecture, thus showing that if Taniyama-Shimura is true then FLT is true. Armed with this relationship, Andrew Wiles dedicated several years to proving the Taniyama-Shimura conjecture. In 1995, Wiles presented a proof of the semistable case of the Taniyama-Shimura conjecture; enough to settle FLT. The rest of the

Taniyama-Shimura conjecture was proved by Breuil, Conrad, Diamond and Taylor in 1999.

While mathematicians were struggling to prove FLT, some turned their attentions to variations of it. For the history and explanations of variations see [19]. Euler showed that there are only trivial solutions to the cubic Fermat equation in $\mathbb{Z}[e^{\frac{2i\pi}{3}}]$ [9]. Liouville used analytic methods to investigate solutions to the Fermat equation in $\mathbb{C}(t)$ for transcendental t. Thèrond showed that if FLT was true and $n < -2$, then $x^n + y^n = z^n$ has no solutions in the nonzero integers.

The variation that we are most interested in deals with finding which quadratic fields contain nontrivial solutions to the cubic Fermat equation. For example

$$(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3$$

shows that there is a nontrivial solutions to the Fermat cubic in $\mathbb{Q}(\sqrt{2})$.

This variation has been tackled by mathematicians such as Burnside, Duarte, Fueter and Aigner; for their work see [2], [3], [4], [6], [8], [10] and [11]. We will list off some of the important theorems they discovered concerning this variation.

Theorem 1.1. *[Burnside/Duarte]*

1. If $k \in \mathbb{Q}$, $k \neq 0, -1$, and

$$x_k = 3 + \sqrt{-3(1 + 4k^3)},$$
$$y_k = 3 - \sqrt{-3(1 + 4k^3)},$$
$$z_k = 6k,$$

then $x_k^3 + y_k^3 + z_k^3 = 0$.

2. If $a \in \mathbb{Q}, a \neq 0$ and $k' = ak$ (with $k \neq 0$), then the solutions corresponding to k and k' by the above method are equivalent if and only if $a = 1$.

3. If (x, y, z) is a nontrivial solution in the quadratic field $\mathbb{Q}(\sqrt{d})$, there exists $k \in \mathbb{Q}$, $k \neq 0, -1$ such that

$$d = -3(1 + 4k^3)u^2,$$

where u is a rational number and (x, y, z) is $\mathbb{Q}(\sqrt{d})$-equivalent to the solution (x_k, y_k, z_k).

The most important result from this theorem for us is that all nontrivial solutions to the Fermat cubic can be expressed in the following form by scaling:

$$x = a + b\sqrt{d},$$

$$y = a - b\sqrt{d} \text{ and}$$

$$z = c$$

for $a, b, c \in \mathbb{Q}$.

Theorem 1.2. *[Aigner/Fueter] The Fermat cubic has a nontrivial solution in $\mathbb{Q}(\sqrt{d})$ if and only if it has a nontrivial solution in $\mathbb{Q}(\sqrt{-3d})$.*

Theorem 1.3. *[Ribenboim] If there is a nontrivial solution to the Fermat cubic in the field $\mathbb{Q}(\sqrt{d})$, then there are infinitely many (pairwise nonequivalent) solutions in the field.*

Aigner developed a graph theoretic method of determining for which choices of squarefree d there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$. Unfortunately, this method is neither simple to understand nor to use. Instead, we will develop a method using the theory of elliptic curves and modular forms. In addition, we will utilize a similar approach that Tunnell employed when solving the congruent number problem. We call n a congruent number if there exists a right triangle with rational sides that has area n; the congruent number problem is the question of determining if a given positive integer n is a congruent number. If we assume that the Birch and Swinnerton-Dyer

(BSD) conjecture is true, then Tunnell's Theorem gives us a full resolution to the congruent number problem. See Section 2.3 for information on BSD.

By using a similar approach to Tunnell's Theorem, we will be able to determine for a given squarefree integer d, if there are nontrivial solutions to the cubic Fermat equation in $\mathbb{Q}(\sqrt{d})$. Since Tunnell's Theorem relies on BSD, then our result will as well. The main result of this thesis will be stated now, see Chapter 3 for the proof.

Theorem 1.4. *Assume BSD and let d be a squarefree integer. If $3|d$ and $d > 0$, there are nontrivial solutions to the Fermat cubic equation in $\mathbb{Q}(\sqrt{d})$ if and only if*

$$\#\{(x,y,z) \in \mathbb{Z}^3 : x^2+3y^2+27z^2 = d/3\} = \#\{(x,y,z) \in \mathbb{Z}^3 : 3x^2+4y^2+7z^2-2yz = d/3\}.$$

If $3 \nmid d$ and $d > 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only if

$$\#\{(x,y,z) \in \mathbb{Z}^3 : x^2+y^2+7z^2+xz = d\} = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2+2y^2+4z^2+xy+yz = d\}.$$

If $3|d$ and $d < 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only there are nontrivial solutions in $\mathbb{Q}(\sqrt{-d/3})$. Finally, if $3 \nmid d$ and $d < 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only if there are nontrivial solutions in $\mathbb{Q}(\sqrt{-3d})$.

In Chapter 2, we provide the background required to prove the results presented in this thesis. In Section 2.1, we will present theorems and concepts from algebra and elementary number theory. We assume that the reader is familiar with groups, rings and fields, and due to this we will only review the First Sylow Theorem. We will state basic theorems from number theory and define the Kronecker symbol. In Section 2.2 and 2.3, we will cover all of the necessary information on elliptic curves and modular forms respectively.

Throughout Chapter 3 we will deal with the elliptic curves $E : y^2 = x^3 - 432$ and $E_d : y^2 = x^3 - 432d^3$. In Section 3.2, we will build the relationship between nontrivial rational solutions to the cubic Fermat equation and the rational points on E, as well

as the relationship between points in $\mathbb{Q}(\sqrt{d})$ on E and rational points on E_d. Using these relationships, we will be able to reprove Theorem 1.3. Finally in Section 3.3, we prove Theorem 1.4 by using Waldspurger's Theorem.

Chapter 2: Preliminaries

2.1 Algebra and Number Theory

In this section we will review some of the concepts from algebra and number theory that will prove useful in this thesis. Our treatment of algebra comes from [5, pg 203-204], and our treatment of elementary number theory comes from [1], [7], and [13].

The only familiarity with algebra we will assume is a basic knowledge of groups, rings and fields. However, for the proof of Theorem 3.8, we will need a corollary to the First Sylow Theorem, so to this end we will state it.

Definition 2.1. *Let G be a group of order n. Let prime $p|n$, and let $n = p^e m$, where the integer m is not divisible by p. If H is a subgroup of G with order p^e, then we call H a Sylow $p-$subgroup of G.*

Theorem 2.2. *[The First Sylow Theorem] A finite group whose order is divisible by a prime p contains a Sylow $p-$subgroup.*

Corollary 2.3. *A finite group whose order is divisible by a prime p contains an element order p.*

Now we will give an overview of the topics from elementary number theory that will be required.

Theorem 2.4. *[Fermat's Little Theorem] Let p be a prime and suppose that $p \nmid a$. Then $a^{p-1} \equiv 1 \pmod{p}$.*

Theorem 2.5. *[Dirichlet Theorem] If a and b are relatively prime positive integers, then the arithmetic progression*

$$a, a+b, a+2b, a+3b, \ldots$$

contains infinitely many primes.

Definition 2.6. *Let p be an odd prime and $gcd(a, p) = 1$. If the quadratic congruence $x^2 \equiv a \pmod{p}$ has a solution, then a is called a quadratic residue. Otherwise, a is called a quadratic nonresidue.*

Using this definition, we can now define the Legendre symbol for odd primes p as follows:

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \text{if } m \text{ is a quadratic residue,} \\ -1 & \text{if } m \text{ is a quadratic nonresidue,} \\ 0 & \text{if } m \equiv 0 \pmod{p}. \end{cases}$$

However, for our purposes we will need the full generalization of the Legendre symbol, the Kronecker symbol, which extents the definition to handle all integers m. First we will extend our definition for -1 in the following manner:

$$\left(\frac{m}{-1}\right) = \begin{cases} 1 & \text{if } m \geq 0, \\ -1 & \text{if } m < 0. \end{cases}$$

Next we will define the Kronecker symbol for $p = 2$ as follows:

$$\left(\frac{m}{2}\right) = \begin{cases} 1 & \text{if } m \equiv \pm 1 \pmod{8}, \\ -1 & \text{if } m \equiv \pm 3 \pmod{8}, \\ 0 & \text{if } m \text{ is even.} \end{cases}$$

In fact, the Kronecker symbol is completely multiplicative on both the bottom and the top.

Definition 2.7. *The Kronecker symbol for $n = \prod_i p_i^{k_i}$ and $m = \prod_j q_j^{l_j}$ is defined as*

$$\begin{aligned} \left(\frac{m}{n}\right) &= \prod_i \left(\frac{m}{p_i}\right)^{k_i} \\ &= \prod_i \prod_j \left(\frac{q_j}{p_i}\right)^{l_j k_i}. \end{aligned}$$

Definition 2.8. *A Dirichlet character is a function* $\chi : \mathbb{Z} \to \mathbb{C}^\times$ *that satisfies:*

1. There is a modulus M *so that* $\chi(n) = 0$ *if* $gcd(n, M) > 1$*, and* $\chi(n + M) = \chi(n)$ *for all* $n \in \mathbb{Z}$*.*

2. For $a, b \in \mathbb{Z}$*,* $\chi(ab) = \chi(a)\chi(b)$*.*

Also, we will make use of the following definition in Section 3.2: $\chi_n(m) = \left(\frac{n}{m}\right)$.

2.2 Elliptic Curves

In this section we will introduce all of the background material required from the theory of elliptic curves for this thesis. Our treatment of elliptic curves come from [15], [21], [23], and [24].

Koblitz provides a general definition of elliptic curves that we will now state, however, in practice, we will be interested in a much more limited definition.

Definition 2.9. *Let* K *be a field so that* K *does not have characteristic 2. Let* $f(x) \in K[x]$ *so that* $f(x)$ *is a cubic with distinct roots. Then the solutions to the equation* $y^2 = f(x)$*, where* $x, y \in K'$*, some extension field of* K*, are called* K'*-points of the elliptic curve.*

For our purposes, we will think of an elliptic curve as the real and complex solutions to an equation of the form $y^2 = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Q}$. More specifically, we will assume that our elliptic curves are non-singular. An elliptic curve E is non-singular provided that there is no point on E so that both of the partial derivatives of $F(x, y) = y^2 - (x^3 + ax^2 + bx + c)$ vanish.

We will also accept as fact that any line connecting two points on an elliptic curve will intersect the curve at a third point counting multiplicity; for more information on this see Bezout's Theorem in [24, pg 237-238].

Definition 2.10. *Let P, Q be points on an elliptic curve E, and let l be the line connecting P and Q. We define $P * Q$ to be the third intersection of l and E.*

We denote the point at infinity with $\mathcal{O}$. Geometrically, we will think of this point as being vertically above all points on the curve E.

Definition 2.11. *Let P, Q be points on the elliptic curve E. We will define the addition by $P + Q = \mathcal{O} * (P * Q)$.*

We will now describe $-P$. Since we want $P - P = \mathcal{O}$, then $P - P = \mathcal{O} * (P * (-P)) = \mathcal{O}$. So, $P * (-P) = \mathcal{O}$. So geometrically, the line connecting P and $-P$ is vertical. This means that if $P = (x, y)$, then $-P = (x, -y)$.

This addition law can be thought of more concretely via the following explicit formulas. Let $P = (x_1, x_2)$ and $Q = (y_1, y_2)$ be points on the elliptic curve $E : y^2 = f(x)$. We will also let $P + Q = (z_1, -z_2)$. So, we have

$$\begin{aligned} P + Q &= (z_1, -z_2) \\ &= \left(\left(\frac{y_2 - x_2}{y_1 - x_1} \right)^2 - a - x_1 - y_1, - \left(\frac{y_2 - x_2}{y_1 - x_1} \right) z_1 - y_2 + \left(\frac{y_2 - x_2}{y_1 - x_1} \right) y_1 \right), \end{aligned}$$

and

$$\begin{aligned} 2P &= (z_1, -z_2) \\ &= \left(\left(\frac{3x_1}{2x_2} \right)^2 - 2x_1, - \left(\frac{f'(x_1)}{2x_2} \right)^3 + 3 \left(\frac{f'(x_1)}{2x_2} \right) x_1 - x_2 \right). \end{aligned}$$

See [24, pg 28-32] for a complete derivation of these formulas. We will use these formulas to prove various results in Section 3.2. Also, these formulas can be used to prove the next theorem.

Theorem 2.12. *Let E be an elliptic curve. The points on E form an abelian group.*

We will denote the set of rational points on E by $E(\mathbb{Q})$. We will now turn our attention to points of finite order on E. The set of points with finite order on E is called the torsion subgroup, and is denoted by $E(\mathbb{Q})_{tors}$. The following theorem will give us all of the possible groups that $E(\mathbb{Q})_{tors}$ can be isomorphic to.

Theorem 2.13 (Mazur)**.** *[17] If E is an elliptic curve, then $E(\mathbb{Q})_{tors}$ is one of the following 15 groups:*

1. $\mathbb{Z}/n\mathbb{Z}$*, with* $1 \leq n \leq 10$ *or* $n = 12$*,*

2. $\mathbb{Z}/2m\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$*, with* $1 \leq m \leq 4$*.*

Next, we will provide more information about a point P of finite order.

Theorem 2.14 (Nagell-Lutz)**.** *Let E be the elliptic curve $y^2 = x^3 + ax + b$. If $(x, y) \in E(\mathbb{Q})_{tors}$ and $(x, y) \neq \mathcal{O}$, then*

1. $x, y \in \mathbb{Z}$*,*

2. either $y = 0$*, or* y^2 *divides* $4a^3 + 27b^2$*.*

From this theorem we can observe that if $P \in E(\mathbb{Q})$ and mP has a non-integral coordinate for some $m \in \mathbb{Z}$, then P has infinite order.

Theorem 2.15. *Let E be an elliptic curve. There is a point P in $E(\mathbb{Q})$ with order two if and only if $P = (x, 0)$. There is a point Q in $E(\mathbb{Q})$ with order three if and only if the $x-$coordinate is a rational root to $\psi_3(x) = 3x^4 + 4ax^3 + 6bx^2 + 12cx + (4ac - b^2)$ so that $x^3 + ax^2 + bx + c$ is a square.*

Theorem 2.16 (Mordell)**.** *[24, pg 83-88] If E is an elliptic curve over $\mathbb{Q}$, then the abelian group $E(\mathbb{Q})$ is finitely generated.*

By what we know about the torsion subgroup and Mordell's Theorem, we are now able to give an explicit description of how $E(\mathbb{Q})$ looks: $E(\mathbb{Q}) = E(\mathbb{Q})_{tors} \oplus \mathbb{Z}^r$. The rank of E is defined to be r.

Definition 2.17. *Let E_1 and E_2 be elliptic curves. We say that E_1 and E_2 are isomorphic, and write $E_1 \cong E_2$, if there are morphisms $\phi : E_1 \to E_2$ and $\psi : E_2 \to E_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ are the identity maps on E_1 and E_2 respectively. We say E_1/K and E_2/K are isomorphic over K if ϕ and ψ can be defined over K.*

Finally, we will look at elliptic curves over finite fields. If p is prime, we will denote a finite field with order p by $\mathbb{F}_p$. Also, we will denote the points of E over a $\mathbb{F}_p$ by $E(\mathbb{F}_p)$. Since $\mathbb{F}_p$ is finitely generated, it is not surprising that $E(\mathbb{F}_p)$ is as well. The computation for $P + Q$ for $P, Q \in E(\mathbb{F}_p)$ uses the same formulas from earlier.

Now we want to determine the size of $E(\mathbb{F}_p)$. To do this, we will make use of the Legendre symbol in the following formula:

$$\#E(\mathbb{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right).$$

2.3 Modular Forms

In this section we will give a brief overview of several topics from the theory of modular forms, including integer and half-integer weight modular forms, $L-$functions, and Waldspurger's Theorem. For more on modular forms see [12], [14], [15], [16], [18], [22], and [25].

The theory of modular forms deals exclusively with meromorphic functions on $\mathbb{H}$, the upper half of the complex plane.

Definition 2.18. *The function f is weakly modular for a subgroup $G \subseteq SL_2(\mathbb{Z})$ if $f : \mathbb{H} \to \mathbb{C}$ satisfies $f(\frac{az+b}{cz+d}) = (cz + d)^k f(z)$ for $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$.*

From the previous definition, we get $f(z+1) = f(z)$ and $f(-1/z) = z^{2k} f(z)$. The first equality tells us that a weakly modular function f is periodic.

Definition 2.19. *Let k be an integer. We say that $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k if:*

1. *f is weakly modular of weight k for $SL_2(\mathbb{Z})$.*
2. *f is holomorphic on $\mathbb{H}$.*
3. *f is holomorphic at ∞.*

A modular form $f(z)$ can be expressed as a Fourier series, $f(z) = \sum_{n=0}^{\infty} a(n)q^n$ for $q = e^{2\pi iz}$. We call $f(z)$ a cusp form for $SL_2(\mathbb{Z})$ if $a(0) = 0$. We denote the space of modular forms with weight k by $M_k(SL_2(\mathbb{Z}))$ and the cuspidal subspace by $S_k(SL_2(\mathbb{Z}))$.

Definition 2.20. *Let N be an integer. We define the following sets:*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) : a \equiv d \equiv 1 \pmod{N} \right\}, \text{ and}$$

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) : b \equiv 0 \pmod{N} \right\}.$$

It is simple to show that $\Gamma(N) \subseteq \Gamma_1(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z})$ is a chain of subgroups. Another important fact about these subgroups is that

$$[SL_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N} \left(1 + \frac{1}{p}\right),$$

$$[\Gamma_0(N) : \Gamma_1(N)] = N \prod_{p|N} \left(1 - \frac{1}{p}\right), \text{ and}$$

$$[\Gamma_1(N) : \Gamma(N)] = N.$$

We can now define $f(z)$ to be a modular form for a congruence subgroup of $SL_2(\mathbb{Z})$.

Definition 2.21. *The weight k operator $|[\gamma]_k$ on functions $f : \mathbb{H} \to \mathbb{C}$ is defined by $(f|[\gamma]_k(z) = (cz+d)^{-k} f(\frac{az+b}{cz+d})$ for $z \in \mathbb{H}$ and $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$.*

Definition 2.22. *Consider the congruence subgroup $\Gamma(N)$ for some integer N and let k be an integer. We say that $f : \mathbb{H} \to \mathbb{C}$ is a modular form of weight k and level N if:*

1. *f is holomorphic on $\mathbb{H}$.*
2. *f is weakly modular for $\Gamma(N)$.*
3. *$f|[\alpha]_k$ is holomorphic at ∞ for all $\alpha \in SL_2(\mathbb{Z})$.*

The preceding definition can be generalized for any congruence subgroups Γ, but for our purposes this definition is sufficient.

Definition 2.23. *Let $f(z)$ be a nonzero weakly modular form of weight k for Γ. We define $v_\infty(f)$ to be the index of the first nonvanishing term in the Fourier expansion of f.*

Theorem 2.24 (Sturm)**.** *Let $\Gamma \subset SL_2(\mathbb{Z})$ be a congruence subgroup of index M and let $f \in M_k(\Gamma)$. If $v_\infty(f) > M\frac{k}{12}$, then f is identically zero.*

We call $M\frac{k}{12}$ the Sturm bound. Using Sturm's Theorem, we can determine if two modular forms $f(z)$ and $g(z)$ are equal by checking the coefficients of their difference up to the Sturm bound.

The next several definitions are only used so that we can define what it means for a modular form $f(z)$ to be a newform.

Definition 2.25. *Let N be positive integer, and let d be any divisor of N. We define the inclusion i_d in the following way:*

$$i_d : S_k(\Gamma_1(N/d)) \times S_k(\Gamma_1(N/d)) \to S_k(\Gamma_1(N))$$
$$(f(z), g(z)) \longmapsto f(z) + g(dz).$$

Definition 2.26. *We define the space of oldforms at level* $\Gamma_1(N)$ *to be*

$$S_k^{old}(\Gamma_1(N)) = \sum_{p|N} i_p(S_k(\Gamma_1(N/p)) \times S_k(\Gamma_1(N/p)).$$

We will find the following quotient group to be useful for the next definition, $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z}/\{\pm 1\}$.

Definition 2.27. *Let* Γ *be a congruence subgroup, let* k *be an integer and let* F *be a fundamental domain for* Γ*. Let* $f, g \in M_k(\Gamma)$*, with at least one of* f *and* g *being a cuspidal form, and let* $\overline{g}$ *be the complex conjugate of* g*. We define the Petersson inner product to be*

$$\langle f, g\rangle = \frac{1}{[PSL_2(\mathbb{Z}) : PSL_2(\mathbb{Z}) \cap \Gamma]} \int_F f(z)\overline{g(z)}y^k \frac{dxdy}{y^2}.$$

Definition 2.28. *We define the space of newforms at level* $\Gamma_1(N)$ *to be the orthogonal complement of the space of oldforms with respect to the Petersson inner product in* $S_k(\Gamma_1(N))$*. So,*

$$S_k^{new}(\Gamma_1(N)) = (S_k^{old}(\Gamma_1(N))^{\perp}.$$

The next several definitions are of operators on integer weight modular forms. The result of each of these operators on a modular form is also a modular form.

Definition 2.29. *Let* n *be a positive integer and let* M *be the set of matrices* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ *with determinant* n*. We define the Hecke operator* T_n *to be*

$$f(z)|T_n = n^{k-1} \sum_{\mu \in SL_2(\mathbb{Z})\backslash M} f|[\mu]_k.$$

Definition 2.30. *We say a function* $f : \mathbb{H} \to \mathbb{C}$ *which is holomorphic on* $\mathbb{H}$ *and is holomorphic at the cusps of* $\Gamma_1(N)$ *is a modular form of weight* k *for* $\Gamma_0(N)$ *with character* χ *if* $f|[\gamma]_k = \chi(d)f$ *for all* $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$*.*

Definition 2.31. *If* $f(z) \in M_k(\Gamma_0(N), \chi)$ *and* $p|N$*, then we define* $f(z)|U(p) = \sum_{n=1}^{\infty} a(pn)q^n$.

Definition 2.32. *If* $f(z) \in M_k(\Gamma_0(N), \chi)$ *and* $p|N$*, then we define* $f(z)|V(p) = \sum_{n=1}^{\infty} a(n)q^{pn}$.

Definition 2.33. *Let* f *be a modular form. If for every positive integer* n *there exists* $\lambda_n \in \mathbb{C}$ *such that* $T_n f = \lambda_n f$*, then we say that* f *is an eigenform. Moreover, if* $f(z) \in S_k^{new}(\Gamma_1(N))$ *is a Hecke eigenform that has been normalized so that* $a(1) = 1$*, then we call* $f(z)$ *a newform.*

We will now define half integer weight modular forms. Some of the theorems and operators we have discussed generalizes to half integer weight forms.

Definition 2.34. *Let* λ *be a nonnegative integer,* N *be a positive integer,* χ *be a Dirichlet character modulo* $4N$*. A holomorphic function* $g(z)$ *on* $\mathbb{H}$ *is called a holomorphic half-integral weight modular form with Nebentypus* χ *and weight* λ *+ 1/2 if it is holomorphic at the cusps of* Γ*, and if*

$$g\left(\frac{az+b}{cz+d}\right) = \chi(d)\left(\frac{c}{d}\right)^{2\lambda+1} \epsilon_d^{-1-2\lambda}(cz+d)^{\lambda+1/2} g(z)$$

for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(4N)$.

Let $M_{\lambda+1/2}(\Gamma_0(4N), \chi)$ be the space of holomorphic half-integer weight modular forms, and let $S_{\lambda+1/2}(\Gamma_0(4N), \chi)$ be the subspace of cusp forms.

Definition 2.35. *Given a symmetric matrix* $A = \begin{pmatrix} a & b & c \\ b & d & e \\ c & e & f \end{pmatrix}$ *with all positive eigenvalues, let* $Q(x, y, z) = ax^2 + 2bxy + dy^2 + 2cxz + 2eyz + fz^2$ *be the quadratic form with Gram matrix* A.

Theorem 2.36. *We have* $\theta_Q(z) = \sum_{n=0}^{\infty} r_Q(n)q^n \in M_{3/2}(\Gamma_0(2N), \chi_{4detA})$ *for* $r_Q(n) = \{(x,y,z) \in \mathbb{Z}^3 : Q(x,y,z) = n\}$, *and* N *is the smallest positive integer so that* NA^{-1} *has even integer entries.*

A combination of Sturm's Theorem and quadratic forms offers a more pleasing way to represent certain half integer weight modular forms.

Definition 2.37. *Let* E *be an elliptic curve. If* p *is a good reduction, then let* $a_p = p + 1 - \#E(\mathbb{F}_p)$. *If* p *is a prime of bad reduction then we have*

$$a_p = \begin{cases} 0 & \textit{additive reduction,} \\ 1 & \textit{split multiplicative reduction,} \\ -1 & \textit{non-split multiplicative reduction.} \end{cases}$$

For prime powers, we define $a_1 = 1$, *and for* $r \geq 2$,

$$a_{p^r} = \begin{cases} a_p a_{p^{r-1}} - p a_{p^{r-2}} & \textit{if } p \textit{ is a prime of good reduction,} \\ a_p^r & \textit{if } p \textit{ is a prime of bad reduction.} \end{cases}$$

Finally, if $n = \prod_{i=1}^{n} p_i^{e_i}$, *then we define* $a_n = \prod_{i=1}^{n} a_{p_i^{e_i}}$.

For information on different types of reduction refer to [23, pg 180]. We will now define $L-$functions for both elliptic curves and modular forms.

Definition 2.38. *If* E *is an elliptic curve, we define* $L(E,s) = \sum_{n=1}^{\infty} \frac{a_n(E)}{n^s}$. *Let* $f(z) = \sum_{n=0}^{\infty} a(n)q^n \in S_k(\Gamma_1(N))$. *We define* $L(f(z),s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ *for* $Re(s) > c+1$ *and* $|a(n)| = O(n^c)$.

Theorem 2.39 (Modularity of Elliptic Curves)**.** *If* $E/\mathbb{Q}$ *is an elliptic curve, then* $E/\mathbb{Q}$ *is modular. That is* $L(E,s) = L(f(z),s)$ *for some newform* $f(z) \in S_2(\Gamma_0(N))$.

The theory explaining how to find the modular form that corresponds to an elliptic curve is quite complicated. In practice, we will compute the modular form $f(z)$ corresponding to E using a computer algebra system such as MAGMA or Sage.

Definition 2.40. *Let E be an elliptic curve and $f(z)$ be the modular form corresponding to E. We call conductor of E the level of $f(z)$.*

It is possible for the conductor to be defined without mention of modular forms, however this is sufficient for our purposes.

Theorem 2.41. *If $E/\mathbb{Q}$ is an elliptic curve, let $\Lambda(E,s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L(E,s)$, where $\Gamma(s) = \int_0^\infty x^{s-1}e^{-x}dx$. Then $\Lambda(E,s) = \epsilon\Lambda(E,2-s)$ where $\epsilon = \pm 1$ is the root number of E.*

For our purposes, we will use MAGMA to compute the root number of a given elliptic curve.

Theorem 2.42. *Let E be an elliptic curve with conductor N and root number ϵ, then* $L(E,1) = (1+\epsilon)\sum_{n=1}^{\infty} \frac{a_n(E)}{n} e^{\frac{-2\pi n}{\sqrt{N}}}$.

We are now able to state an important conjecture that we will assume for our main result.

Conjecture 2.43 (weak Birch and Swinnerton-Dyer)**.** *If E is an elliptic curve, then $rank(E(\mathbb{Q})) = ord_{s=1}L(E,s)$. In particular, E has infinitely many rational points if and only if $L(E,1) = 0$.*

Definition 2.44. *For a character $\chi : \mathbb{F}_p \to \mathbb{C}$, we define the Gauss sum $\tau(\chi)$ by*

$$\tau(\chi) = \sum_{x=0}^{p-1} \chi(x)\zeta_p^x, \text{ where } \zeta_p = e^{2\pi i/p}.$$

Definition 2.45. *Suppose that* $f(z) = \sum_{n=1}^{\infty} a(n)q^n \in M_k(\Gamma_0(N), \chi)$. *If* ψ *is a Dirichlet character, then the* $\psi-$*twist of* $f(z)$ *is defined by* $f(z) \otimes \psi = \sum_{n=0}^{\infty} \psi(n)a(n)q^n$.

We will occasionally find it more convenient to denote the $\psi-$twist of a modular form $f(z)$ by $f(z)_\psi$. The following theorem will only be used to prove Lemma 3.14.

Theorem 2.46. *If* $g(z)$ *be a modular form with weight* $\lambda + 1/2$ *and level* N *with Dirichlet character* ψ, *then* $g(z)_\psi \in M_{\lambda+1/2}(\Gamma_0(Nm^2), \psi\chi^2)$ *for a Dirichlet character* χ *with modulus* m.

Definition 2.47. *The Fricke involution* $|_k W(N)$ *on* $M_k(\Gamma_0(N))$ *is given by* $f(z)|_k W(N) = N^{-k/2} f(\frac{-1}{Nz})$.

Theorem 2.48. *If* $E/\mathbb{Q}$ *is an elliptic curve with modular form* G *then* $G|W(N) = \alpha G$ *for* $\alpha = \pm 1$. *Moreover, the root number of* E *is* $\epsilon = -\alpha$. *If* χ *is a primitive Dirichlet character with modulus* r *so that* r *is coprime to* N, *then* $G \otimes \chi \in S_2^{new}(\Gamma_0(Nr^2))$. *Then we have* $(G \otimes \chi)|W(Nr^2) = \alpha\chi(N)\frac{\tau(\chi)^2}{r}$.

The theorems we have stated for integer weight modular forms also hold for half-integer weight forms. We will now state two important theorems for this thesis that relate the two types of forms together.

Theorem 2.49 (Shimura Correspondence)**.** *Suppose that*

$$g(z) = \sum_{n=1}^{\infty} b(n)q^n \in S_{\lambda+1/2}(\Gamma_0(4N), \chi)$$

is a half-integral weight cusp form with $\lambda \geq 1$. *Let* t *be a positive squarefree integer,and define the Dirichlet character* $\psi_t(n) = \chi(n)\left(\frac{-1}{n}\right)^{\lambda}\left(\frac{t}{n}\right)$. *If complex numbers* $A_t(n)$ *are*

defined by

$$\sum_{n=1}^{\infty} \frac{A_t(n)}{n^s} = \sum_{n=1}^{\infty} \sum_{d|n} \psi_t\left(\frac{n}{d}\right)\left(\frac{n}{d}\right)^{\lambda-1} b(td^2)\frac{b(tn^2)}{n^2},$$

then

$$\mathcal{S}_t(g(z)) = \sum_{n=1}^{\infty} A_t(n)q^n$$

is a weight 2λ *modular form in* $M_{2\lambda}(\Gamma_0(2N), \chi^2)$.

Theorem 2.50. *There are half-integer weight Hecke operators* T_{p^2} *that are analogous to the integer weight operators. Let* f *be a half-integer weight modular form with level* $4N$ *and* t *be a positive integer. If prime* $p \nmid 4tN$ *then* $\mathcal{S}_t(f|T_{p^2}) = \mathcal{S}_t(f)|T(p)$.

Theorem 2.51 (Waldspurger)**.** *[25] Suppose that* $f \in S_{\lambda+1/2}(\Gamma_0(N), \chi)$ *so that* $f(z) = \sum_{n=1}^{\infty} a(n)q^n$ *and* $f|T(p^2) = \lambda(p)f$ *for all prime* $p \nmid N$*. If* $F(z)$ *is the unique newform such that* $F(z)|T(p) = \lambda(p)F(z)$ *for all* $p \nmid N$*, then*

$$a(n_1)^2 L(F \otimes \chi^{-1}\chi_{n_2(-1)^\lambda}, \lambda)\chi\left(\frac{n_2}{n_1}\right) n_2^{\lambda-1/2} = a(n_2)^2 L(F \otimes \chi^{-1}\chi_{n_1(-1)^\lambda}, \lambda) n_1^{\lambda-1/2},$$

provided n_1, n_2 *are squarefree positive integers so that* $\left(\frac{n_1/n_2}{p}\right) = 1$ *for odd prime* $p|N$*. If* $2|N$*, we also assume* $\frac{n_1}{n_2} \equiv 1 \pmod 8$.

Chapter 3: The Proof

3.1 Introduction

FLT tells us that there are only trivial solutions to $x^3 + y^3 = z^3$ in the rationals. However, FLT does not tell us anything about the existence of nontrivial solutions in quadratic fields.

It may be possible to generate a solution to the Fermat cubic equation in $\mathbb{Q}(\sqrt{d})$ for a particular value of d by careful use of algebra and a computer search; alternatively, we could use Theorem 1.1. The following are examples of nontrivial solutions in the field $\mathbb{Q}(\sqrt{d})$ with $d = 2, 5$ and -6 respectively:

$$(18 + 17\sqrt{2})^3 + (18 - 17\sqrt{2})^3 = 42^3,$$

$$(18 + 2\sqrt{5})^3 + (18 - 2\sqrt{5})^3 = 24^3,$$

$$(18 + 3\sqrt{-6})^3 + (18 - 3\sqrt{-6})^3 = 18^3.$$

As we mentioned in the introduction, for some choices of squarefree d, there may only be trivial solutions in $\mathbb{Q}(\sqrt{d})$. So, our goal is to derive criteria to help us determine when there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$.

In Section 2, we will establish the relationship between the Fermat cubic and the elliptic curve $E : y^2 = x^3 - 432$. Next, we will develop the tools to help us show how $E(\mathbb{Q}(\sqrt{d}))$ relates to $E_d : y^2 = x^3 - 432d^3$. Once all of these tools have been developed we will be able to prove Theorem 1.3 in the language of elliptic curves. In Section 3, we examine the modular form $F(z)$ that corresponds to E. In particular, our goal in this section will be to find a linear combination of quadratic forms so that the d^{th} coefficient is 0 if and only if there are nontrivial solutions to the Fermat cubic equation in $\mathbb{Q}(\sqrt{d})$. To do this we will need the Shimura correspondence, Waldspurger's Theorem, and

BSD. For an overview of each of these topics see Section 2.3.

3.2 The Fermat cubic and an elliptic curve

If we require z to be nonzero, then we can reduce the Fermat cubic to $X^3 + Y^3 = 1$. After doing this, it is not difficult to see that nontrivial solutions to the Fermat cubic equation and nontrivial solutions to $X^3 + Y^3 = 1$ correspond to each other via $f(x, y, z) := (\frac{x}{z}, \frac{y}{z})$. It should also be noted that we do not lose anything from this simplification, since we are only interested in nontrivial solutions. We will presently demonstrate the purpose of expressing the Fermat cubic equation in this form.

Theorem 3.1. *The elliptic curves $C : x^3 + y^3 = 1$ and E are isomorphic.*

Proof. Let $f : C \to E$ be defined by $f((x, y)) = (\frac{12}{x+y}, 36\frac{y-x}{x+y})$. Hence $f \in \mathbb{Q}^2(x, y)$.

We now want to verify that f is a morphism from C to E; translating, we want to show that f maps a point from $C(\mathbb{Q})$ to a point in $E(\mathbb{Q})$. Let $(x, y) \in C(\mathbb{Q})$, then $f((x, y)) = (\frac{12}{x+y}, 36\frac{y-x}{y+x})$. If we substitute $f((x, y))$ into the equation for E, then after using basic algebra we can simplify to get the equation for C. Thus, f is a morphism from C to E.

Finally, to finish our argument we need to show that f is invertible. Let $\alpha = \frac{12}{x+y}$ and $\beta = 36\frac{y-x}{x+y}$. Note that $\frac{12}{\alpha} = x + y$ and $\frac{\beta}{3\alpha} = x - y$. Let $g : E \to C$ be defined by

$$g((\alpha, \beta)) = \left(\frac{\frac{12}{\alpha} + \frac{\beta}{3\alpha}}{2}, \frac{\frac{12}{\alpha} - \frac{\beta}{3\alpha}}{2} \right).$$

After making use of the equalities and basic algebra, we get (x, y) out. Hence f is invertible.

Therefore, C and E are isomorphic. □

Since the only rational solutions to the Fermat cubic are trivial, $C(\mathbb{Q}) = \{\infty, (1,0), (0,1)\}$. Recall from Section 2.1 that the set of rational points on an elliptic curve forms an abelian group. Since $C(\mathbb{Q})$ is a group of order 3, then $C(\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$. Thus by Theorem 3.1, we have $E(\mathbb{Q}) = \{(12,-36), (12,36), \infty\} \cong \mathbb{Z}/3\mathbb{Z}$.

Next, we will begin to develop the machinery required to build a relationship between the elliptic curves E and E_d.

Lemma 3.2. *Let d be a squarefree integer so that $d \neq 1$. Let $\sigma : \mathbb{Q}(\sqrt{d}) \to \mathbb{Q}(\sqrt{d})$ be defined by $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Then σ has the following properties:*
a) If $x, y \in \mathbb{Q}(\sqrt{d})$, then $\sigma(x + y) = \sigma(x) + \sigma(y)$.
b) Let $x \in \mathbb{Q}(\sqrt{d})$. Then $x \in \mathbb{Q}$ if and only if $\sigma(x) = x$.
c) If $x \in \mathbb{Q}(\sqrt{d})$, then $x + \sigma(x) \in \mathbb{Q}$ and $x\sigma(x) \in \mathbb{Q}$.

Proof. Let $a + b\sqrt{d}$ and $m + n\sqrt{d} \in \mathbb{Q}(\sqrt{d})$.
a) We have

$$\begin{aligned}\sigma((a + b\sqrt{d}) + (m + n\sqrt{d})) &= a + m - (b + n)\sqrt{d} \\ &= a - b\sqrt{d} + m - n\sqrt{d} \\ &= \sigma(a + b\sqrt{d}) + \sigma(n + m\sqrt{d}).\end{aligned}$$

Next, we have

$$\begin{aligned}\sigma((a + b\sqrt{d})(n + m\sqrt{d})) &= \sigma(am + bnd + (an + bm)\sqrt{d}) \\ &= am + bnd - (an + bm)\sqrt{d} \\ &= (a - b\sqrt{d})(n - m\sqrt{d}) \\ &= \sigma(a + b\sqrt{d})\sigma(m + n\sqrt{d}).\end{aligned}$$

b) ($\Rightarrow$) Suppose that $a + b\sqrt{d} \in \mathbb{Q}$. Then it is clear that $b = 0$. Thus

$$\begin{aligned}\sigma(a) &= \sigma(a + 0\sqrt{d}) \\ &= a - 0\sqrt{d} \\ &= a.\end{aligned}$$

($\Leftarrow$) Now suppose that $\sigma(a + b\sqrt{d}) = a + b\sqrt{d}$. By definition $\sigma(a + b\sqrt{d}) = a - b\sqrt{d}$. Hence $a + b\sqrt{d} = a - b\sqrt{d}$. Hence $b = 0$.

c) We have

$$\begin{aligned}(a + b\sqrt{d}) + \sigma(a + b\sqrt{d}) &= a + b\sqrt{d} + a - b\sqrt{d} \\ &= 2a,\end{aligned}$$

and

$$\begin{aligned}(a + b\sqrt{d})\sigma(a + b\sqrt{d}) &= (a + b\sqrt{d})(a - b\sqrt{d}) \\ &= a^2 + ab\sqrt{d} - ab\sqrt{d} - b^2 d \\ &= a^2 - b^2 d.\end{aligned}$$

□

Lemma 3.3. *Define* $\sigma(P) = (\sigma(x), \sigma(y))$ *for* $P \in E(\mathbb{Q}(\sqrt{d}))$. *If* $P, Q \in E(\mathbb{Q}(\sqrt{d}))$ *then* $\sigma(P + Q) = \sigma(P) + \sigma(Q)$.

Proof. Let $P, Q \in E(\mathbb{Q}(\sqrt{d}))$. We will make use of the explicit formulas for the addition law from Section 2.2.

First suppose that $P \neq Q$ so that $P = (x_1, x_2)$ and $Q = (y_1, y_2)$. Let $P + Q =$

$(z_1, -z_2)$. Then

$$\begin{aligned}
\sigma(P+Q) &= \sigma\left(\left(\frac{y_2-x_2}{y_1-x_1}\right)^2 - x_1 - y_1, -z_2\right) \\
&= \left(\sigma\left(\left(\frac{y_2-x_2}{y_1-x_1}\right)^2 - x_1 - y_1\right), \sigma(-z_2)\right) \\
&= \left(\sigma\left(\frac{y_2-x_2}{y_1-x_1}\right)^2 - \sigma(x_1) - \sigma(y_1), -\sigma(z_2)\right) \\
&= \left(\left(\frac{\sigma(y_2-x_2)}{\sigma(y_1-x_1)}\right)^2 - \sigma(x_1) - \sigma(y_1), -\sigma(z_2)\right) \\
&= \left(\left(\frac{\sigma(y_2)-\sigma(x_2)}{\sigma(y_1)-\sigma(x_1)}\right)^2 - \sigma(x_1) - \sigma(y_1), -\sigma(z_2)\right)
\end{aligned}$$

Recall that $z_2 = \left(\frac{y_2-x_2}{y_1-x_1}\right) z_1 + y_2 - \left(\frac{y_2-x_2}{y_1-x_1}\right) y_1$. So:

$$\begin{aligned}
&= \left(\sigma(z_1), -\sigma\left(\left(\frac{y_2-x_2}{y_1-x_1}\right) z_1 + y_2 - \left(\frac{y_2-x_2}{y_1-x_1}\right) y_1\right)\right) \\
&= \left(\sigma(z_1), -\left(\sigma\left(\left(\frac{y_2-x_2}{y_1-x_1}\right) z_1\right) + \sigma(y_2) - \sigma\left(\left(\frac{y_2-x_2}{y_1-x_1}\right) y_1\right)\right)\right) \\
&= \left(\sigma(z_1), -\left(\left(\frac{\sigma(y_2)-\sigma(x_2)}{\sigma(y_1)-\sigma(x_1)}\right)\sigma(z_1) + \sigma(y_2) - \left(\frac{\sigma(y_2)-\sigma(x_2)}{\sigma(y_1)-\sigma(x_1)}\right)\sigma(y_1)\right)\right) \\
&= \sigma(P) + \sigma(Q).
\end{aligned}$$

Now consider $P = Q$. Note that if $f(x) = x^3 - 432$ then $f'(x) = 3x^2$. So by the

duplication formula given in Section 2.2:

$$\begin{aligned}
\sigma(2P) &= \sigma\left(\left(\frac{3x_1}{2x_2}\right)^2 - 2x_1, -\left(\frac{3x_1}{2x_2}\right)^3 + 3\left(\frac{3x_1}{2x_2}\right)x_1 - x_2\right) \\
&= \left(\sigma\left(\left(\frac{3x_1}{2x_2}\right)^2 - 2x_1\right), \sigma\left(-\left(\frac{3x_1}{2x_2}\right)^3 + 3\left(\frac{3x_1}{2x_2}\right)x_1 - x_2\right)\right) \\
&= \left(\sigma\left(\left(\frac{3x_1}{2x_2}\right)^2\right) - \sigma(2x_1), -\sigma\left(\left(\frac{3x_1}{2x_2}\right)\right)^3 + \sigma\left(3\left(\frac{3x_1}{2x_2}\right)x_1\right) - \sigma(x_2)\right) \\
&= \left(\left(\frac{3\sigma(x_1)}{2\sigma(x_2)}\right)^2 - 2\sigma(x_1), -\left(\frac{3\sigma(x_1)}{2\sigma(x_2)}\right)^3 + 3\left(\frac{3\sigma(x_1)}{2\sigma(x_2)}\right)\sigma(x_1) - \sigma(x_2)\right) \\
&= 2\sigma(P)
\end{aligned}$$

Hence $\sigma(P+Q) = \sigma(P) + \sigma(Q)$. □

Lemma 3.4. *If $Q = P - \sigma(P)$ and $Q = (x, y)$, then $x \in \mathbb{Q}$ and $\frac{y}{\sqrt{d}} \in \mathbb{Q}$.*

Proof. We have

$$\begin{aligned}
\sigma(Q) &= \sigma(P - \sigma(P)) \\
&= \sigma(P) - P \\
&= -Q.
\end{aligned}$$

Since $Q = (x, y)$, then $-Q = (x, -y)$ and $\sigma(Q) = (\sigma(x), \sigma(y))$. Hence

$$(x, -y) = (\sigma(x), \sigma(y)).$$

By Lemma 3.2, $x \in \mathbb{Q}$. Suppose that $y = a + b\sqrt{d}$. It follows from basic algebra that $a = 0$. Thus $\frac{y}{\sqrt{d}} \in \mathbb{Q}$. □

Lemma 3.5. *Define a function τ on $\{Q : Q = P - \sigma(P)$ for $P \in E(\mathbb{Q}(\sqrt{d}))\}$ by $\tau(x, y) = (xd, yd^{3/2})$ and $\tau(\mathcal{O}) = \mathcal{O}$. Then $\tau(Q) \in E_d(\mathbb{Q})$.*

Proof. Let $P - \sigma(P) = (x, y)$. Note that by Lemma 3.4, $x, \frac{y}{\sqrt{d}} \in \mathbb{Q}$. So $\tau((x, y)) = (xd, yd^{3/2})$. Substituting this into E_d, we have

$$(yd^{3/2})^2 = (xd)^3 - 432d^3.$$

This reduces back down to the equation for E. Hence $\tau(x, y) \in E_d(\mathbb{Q})$. □

Lemma 3.6. *Let $p \equiv 2 \pmod 3$. If $a \in \mathbb{F}_p^\times$, then $x^3 \equiv a \pmod p$ is solvable.*

Proof. Suppose $a \in \mathbb{F}_p^\times$ so that a has order 3. So $a^3 \equiv 1 \pmod p$. Hence

$$a^3 - 1 \equiv (a - 1)(a^2 + a + 1) \equiv 0 \pmod p.$$

Since $a \neq 1$ and a has order 3, then $p|a^2 + a + 1$. Also, we know that by Theorem 2.4, $a^{p-1} \equiv 1 \pmod p$. Hence $3|p - 1$. Thus $p \equiv 1 \pmod 3$. This is impossible since by $p \equiv 2 \pmod 3$ by hypothesis. Therefore no element in $\mathbb{F}_p^\times$ has order 3.

Suppose $a, b \in \mathbb{F}_p^\times$ so that $a^3 \equiv b^3 \pmod p$. Hence $(\frac{a}{b})^3 \equiv 1 \pmod p$. Thus $a \equiv b \pmod p$. Hence x^3 is a bijection on congruence classes in $\mathbb{Z}/p\mathbb{Z}$. Therefore $x^3 \equiv a \pmod p$ is solvable. □

Theorem 3.7. *If $p > 2$ is a prime so that $p \equiv 2 \pmod 3$, then $\#E_d(\mathbb{F}_p) = p + 1$.*

Proof. Let p be a prime so that $p \equiv 2 \pmod 3$, and let $f(x) = x^3 - 432d^3$. By definition,

$$\#E_d(\mathbb{F}_p) = p + 1 + \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right).$$

Since $x^3 \equiv a \pmod p$ has a solution for all $a \in \mathbb{F}_p$, then $f(x) \equiv b \pmod p$ has a solution for all $b \in \mathbb{F}_p$. Hence $\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) = 0$. Therefore $\#E_d(\mathbb{F}_p) = p + 1$. □

Recall from Section 2.2 that points on an elliptic curve with finite order have integral coordinates. Also, recall that the $y-$coordinate of a point of order 2 is zero. Using these two facts, it is simple to prove that E_d has no points with order 2 for all squarefree d. Using this, we are now going to show that there are two possibilities for the torsion subgroup of $E_d(\mathbb{Q})$ which we will denote by T.

Theorem 3.8. *The torsion subgroup of $E_d(\mathbb{Q})$ is either trivial or isomorphic to $\mathbb{Z}/3\mathbb{Z}$.*

Proof. Since there are no elements of order two in $E_d(\mathbb{Q})$, then by Corollary 2.3, we have $2 \nmid |T|$. We want to show that $|T| = 3^k$ for some integer k. Suppose not, then $q||T|$ for some prime $q > 3$. Let x be an integer relatively prime to $3q$ so that $x \equiv 2 \pmod 3$ and $x \equiv 1 \pmod q$. By Theorem 2.5, there exist infinitely many primes p so that $p \equiv x \pmod{3q}$. If we take a sufficiently large p so that we have an element of order q in $E_d(\mathbb{F}_p)$, then we get:

$$\begin{aligned} q||E_d(\mathbb{F}_p)| &= p + 1 \\ &\equiv x + 1 \pmod q \\ &\equiv 2 \pmod q. \end{aligned}$$

Clearly this is impossible, hence $|T| = 3^k$.

Now we want to show that $|T| = 1$ or 3. Suppose not, then $9||T|$. By Theorem 2.5, there are infinitely many primes $p \equiv 2 \pmod 9$. Similarly to the first step, if we take a sufficiently large p, then we have:

$$\begin{aligned} 9||E_d(\mathbb{F}_p)| &= p + 1 \\ &\equiv 3 \pmod 9. \end{aligned}$$

This is impossible, hence $|T| = 1$ or 3. □

Corollary 3.9. *The torsion subgroup $E_d(\mathbb{Q})_{tors} \cong \mathbb{Z}/3\mathbb{Z}$ if and only if $d = 1$ or -3.*

Proof. By Theorem 3.8, $|T| = 1$ or 3. Suppose that $E_d(\mathbb{Q})$ has a point with order 3. Then the $x-$coordinate of the point must be a root of $\psi_3(x) = 3x^4 - 12(432)d^3x$. Once we factor, we get

$$3x^4 - 12(432)d^3x = 3x(x - 12d)(x^2 + 12dx + 144d^2).$$

Since $x^2 + 12dx + 144d^2$ has a discriminant of $-432d^2$, its roots are complex for all values of d. Our other possible solutions are $x = 0$ and $x = 12d$.

Suppose that $x = 0$. We have $y^2 = -432d^3$ which is only a perfect square for $d = -3$. If $d = -3$, we get $y = \pm 108$.

Suppose that $x = 12d$. We have,

$$\begin{aligned} y^2 &= (12d)^3 - 432d^3 \\ &= 1728d^3 - 432d^3 \\ &= 1296d^3 \end{aligned}$$

Since 1296 is a perfect square, then $d = 1$ is the only possibility for the $y-$coordinate to be an integer. □

Now, using all of the theory that we have developed in this section, we will mirror the results of Theorem 1.3 in the language of elliptic curves.

Theorem 3.10. *Let d be a squarefree integer. Then C has a nontrivial solution in $\mathbb{Q}(\sqrt{d})$ if and only if $E_d(\mathbb{Q})$ has positive rank.*

Proof. ($\Rightarrow$) Let (x, y) be a nontrivial solution to C in $\mathbb{Q}(\sqrt{d})$. By Theorem 3.1, $(x, y) \to (\frac{12}{x+y}, 36\frac{y-x}{x+y}) = P \in E(\mathbb{Q}(\sqrt{d}))$. By Lemma 3.5, $\tau(P - \sigma(P)) \in E_d(\mathbb{Q})$.

Suppose that $d \notin \{1, -3\}$ and that $P - \sigma(P) = \mathcal{O}$. Then we have $P = \sigma(P)$. This tells us that the $y-$coordinate is rational. Hence $P \in E(\mathbb{Q})$, and this contradicts FLT. Thus $\tau(P - \sigma(P))$ is a nonidentity rational point on E_d. Since the contrapositive of Corollary 3.9 tells us that T is trivial, then $E_d(\mathbb{Q})$ has positive rank.

Since $d = 1$ reduces to looking for nontrivial rational solutions to the Fermat cubic, then by FLT none exist. Also by Theorem 1.2, there are only trivial solutions in $\mathbb{Q}(\sqrt{-3})$.

($\Leftarrow$) Suppose that $E_d(\mathbb{Q})$ has positive rank. Let $(x, y) \in E_d(\mathbb{Q})$. So, we have $y^2 = x^3 - 432d^3$. If we divide through by d^3, then we get $(\frac{y}{d^{3/2}})^2 = (\frac{x}{d})^3 - 432$. If we rationalize the denominator of $\frac{y}{d^{3/2}}$, then we get $\frac{y\sqrt{d}}{d^2}$. Hence $(\frac{x}{d}, \frac{y\sqrt{d}}{d^2}) \in E(\mathbb{Q}(\sqrt{d}))$.

Recall from Theorem 3.1 that we have a map $g : E(\mathbb{Q}(\sqrt{d})) \to C(\mathbb{Q}(\sqrt{d}))$. So, we have

$$g\left(\frac{x}{d}, \frac{y\sqrt{d}}{d^2}\right) = \left(\frac{\frac{12d}{x} + \frac{y\sqrt{d}}{3dx}}{2}, \frac{\frac{12d}{x} - \frac{y\sqrt{d}}{3dx}}{2}\right).$$

Suppose that this is a trivial solution, then either the $x-$coordinate or the $y-$coordinate is zero.

Consider that the $x-$coordinate is zero, then we have $\frac{\frac{12d}{x} + \frac{y\sqrt{d}}{3dx}}{2} = 0$. Hence $y = -36d^{3/2}$. Thus $y \notin \mathbb{Q}$ for $d \neq 1$. Since E_d has positive rank, then $d \neq 1$ by hypothesis. A similar conclusion holds if we suppose the $y-$coordinate is zero. Hence (x, y) is a nontrivial solution to C in $\mathbb{Q}(\sqrt{d})$. □

3.3 Modularity of the Fermat cubic in quadratic fields

Let $F(z)$ be the modular form corresponding to the elliptic curve E. Since E has conductor 27, then by the modularity of elliptic curves we have $F(z) \in S_2(\Gamma_0(27))$. In fact, $F(z) = q\prod_{n=1}^{\infty}(1 - q^{3n})^2(1 - q^{9n})^2$ [16, pg. 2].

As mentioned in the introduction, we will be employing a similar approach as Tunnell's Theorem. To give motivation on the proceeding calculations, we will briefly explain the approach.

First, we will want to use the Shimura correspondence to find a modular form that essentially lifts to $F(z)$. For the hypotheses of the Shimura correspondence, we will take $N = 27$, $k = 3$ and let χ_1 be the trivial Dirichlet character for modulus 108. Next, we want to find a eigenform $f(z) \in S_{3/2}(\Gamma_0(108), \chi_1)$ that lifts to $F(z)$ or a linear combination of $F(z)$ and $F(z)|V(d)$ for some $d|108$.

Once we have $f(z)$, we will apply Waldspurger's Theorem to $F(z)$ and $f(z)$ to get equalities of the form

$$a(n_1)^2 L(E_{-n_2}, 1) = \sqrt{\frac{n_2}{n_1}} a(n_2)^2 L(E_{-n_1}, 1)$$

where $a(n)$ is the n^{th} coefficient of $f(z)$. By taking cases, we will be able to prove our Theorem 1.4 for $d < 0$ so that $d \equiv 2 \pmod 3$. Then we will perform a similar procedure for $d < 0$ so that $d \equiv 6 \pmod 9$.

Recall that Theorem 1.2 tells us that the existence of nontrivial solutions of the Fermat cubic in $\mathbb{Q}(\sqrt{d})$ and $\mathbb{Q}(\sqrt{-3d})$ are dependent. Due to this, we would also like a theorem that relates the $L-$functions of E_d and E_{-3d}.

Theorem 3.11. *If d be a squarefree integer, then $L(E_d, 1) = L(E_{-3d}, 1)$.*

Proof. We have $L(E_d, 1) = L(F \otimes \chi_d, 1)$, where $F(z) = q \prod_{n=1}^{\infty} (1-q^{3n})^2 (1-q^{9n})^2$. Also,

$$\begin{aligned} F \otimes \chi_{-3d} &= (F \otimes \chi_{-3}) \otimes \chi_d \\ &= \left(\sum_{n=1}^{\infty} a(n) \chi_{-3}(n) q^n \right) \otimes \chi_d \\ &= \left(\sum_{n=1}^{\infty} a(n) \left(\frac{n}{3} \right) q^n \right) \otimes \chi_d \\ &= F(z) \otimes \chi_d. \end{aligned}$$

From $F(z)$ it follows that if $a(n) \neq 0$, then $n \equiv 1 \pmod 3$ and so $a(n) = a(n)\left(\frac{n}{3}\right)$ for all $n \geq 1$. $\square$

Now that we have an outline of our argument, we will proceed with the computations for the case with squarefree $d < 0$ so that $d \equiv 2 \pmod 3$.

First we will note that $\dim(\mathrm{S}_{3/2}(\Gamma_0(108), \chi_1)) = 5$. We also have the following basis for $S_{3/2}(\Gamma_0(108), \chi_1)$:

$$g_1(z) = q - q^{10} - q^{16} - q^{19} - q^{22} + 2q^{28} + \cdots,$$
$$g_2(z) = q^2 - q^5 + q^8 - q^{11} + q^{14} - 2q^{17} - q^{20} + \cdots,$$
$$g_3(z) = q^3 - 2q^{12} + \ldots,$$
$$g_4(z) = q^4 - q^{10} + q^{13} - q^{16} - q^{19} - q^{22} - q^{25} + q^{28} + \cdots,$$
$$g_5(z) = q^7 - q^{10} + q^{13} - q^{16} - q^{22} - q^{25} + \cdots$$

By Sturm's Theorem, we have

$$\mathcal{S}_1(g_1(z) + g_4(z)) = F(z) + F(z)|V(2),$$
$$\mathcal{S}_2(g_1(z) + g_4(z)) = 0,$$
$$\mathcal{S}_3(g_1(z) + g_4(z)) = 0,$$
$$\mathcal{S}_1(g_1(z) + g_5(z)) = F(z),$$
$$\mathcal{S}_2(g_1(z) + g_5(z)) = 0, \text{ and}$$
$$\mathcal{S}_3(g_1(z) + g_5(z)) = 0.$$

Since we took $t = 1, 2,$ and 3, then by Theorem 2.50 we have $\mathcal{S}_t((g_1(z)+g_4(z))|T_{p^2}) = \mathcal{S}_t((g_1(z) + g_4(z))|T(p)$ for primes $p > 3$. Since $F(z)$ and $F(z)|V(2)$ are both Hecke eigenforms, $F(z)|T(p) = \lambda(p)F(z)$ and $F(z)|V(2)|T(p) = \lambda(p)F(z)|V(2)$ for primes $p > 3$ where $\lambda(p)$ is equal to the p^{th} coefficient of $F(z)$. Also, since 1, 2 and 3 divide $4N$, then we have $(g_1(z) + g_4(z)|T_{p^2} - \lambda(p)(g_1(z) + g_4(z)$ is in: $\ker(\mathcal{S}_1)$, $\ker(\mathcal{S}_2)$, and $\ker(\mathcal{S}_3)$. By MAGMA computations, $\ker(\mathcal{S}_1) \cap \ker(\mathcal{S}_2) \cap \ker(\mathcal{S}_3) = 0$. This implies that

$g_1(z)+g_4(z)$ is a Hecke eigenform. Similar computations can be done and conclusions drawn for $g_1(z)+g_5(z)$.

For the ease of computing, we will take the quadratic forms $Q_1(x,y,z) = x^2 + 3y^2 + 27z^2$ and $Q_2(x,y,z) = 3x^2 + 4y^2 - 2yz + 7z^2$. These forms correspond to the matrices

$$A_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 27 \end{pmatrix} \text{ and}$$

$$A_2 = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 4 & -1 \\ 0 & -1 & 7 \end{pmatrix} \text{ respectively.}$$

We have $\theta_{Q_1}, \theta_{Q_2} \in M_{3/2}(\Gamma_0(108), \chi_1)$. Also by Sturm's Theorem, we have

$$\theta_{Q_1}(z) - \theta_{Q_2}(z) = -2(g_1(z)+g_5(z)) + 4(g_1(z)+g_4(z)).$$

Since $g_1(z)+g_4(z)$ and $g_1(z)+g_5(z)$ are both Hecke eigenforms, so is $\theta_{Q_1}(z)-\theta_{Q_2}(z)$.

We have shown that $\theta_{Q_1}(z) - \theta_{Q_2}(z)$ is a Hecke eigenform, and we have $F(z) - F(z)|V(2)$ which is a Hecke eigenform. We will denote the n^{th} coefficient of $\theta_{Q_1}(z) - \theta_{Q_2}(z)$ by $a(n)$. By Waldspurger's Theorem, we have

$$a(n_1)^2 L(E_{-n_2}, 1) = \sqrt{\frac{n_2}{n_1}} a(n_2)^2 L(E_{-n_1}, 1)$$

for n_1 and n_2 squarefree so that $\left(\frac{n_1/n_2}{p}\right) = 1$ for $p = 3$ and $\frac{n_1}{n_2} \equiv 1 \pmod 8$. After doing some arithmetic, we get

$$L(E_{-n_2}, 1) = \sqrt{\frac{n_2}{n_1}} \left(\frac{a(n_2)}{a(n_1)}\right)^2 L(E_{-n_1}, 1).$$

Let $n_2 \equiv 1 \pmod 3$. The table below shows the cases that we have from Waldspurger's Theorem by picking appropriate choices of n_1. These cases cover all possibilities for $n_2 \equiv 1 \pmod 3$.

Table 1

n_2	n_1	$a(n_1)$	$L(E_{-n_1}, 1)$
$n_2 \equiv 1 \pmod{24}$	1	2	$1.52995\ldots$
$n_2 \equiv 34 \pmod{48}$	34	4	$1.04953\ldots$
$n_2 \equiv 19 \pmod{24}$	19	-6	$0.70199\ldots$
$n_2 \equiv 13 \pmod{24}$	13	2	$0.42434\ldots$
$n_2 \equiv 22 \pmod{48}$	22	-4	$1.30474\ldots$
$n_2 \equiv 7 \pmod{24}$	7	-2	$1.15653\ldots$
$n_2 \equiv 10 \pmod{36}$	10	-4	$1.93525\ldots$
$n_2 \equiv 46 \pmod{48}$	46	4	$0.90231\ldots$

Hence for squarefree integer $d < 0$ so that $d \equiv 2 \pmod 3$, $L(E_d, 1) = 0$ if and only if $a(-d) = 0$. Furthermore, if we apply Theorem 3.11 then

$$L(E_{3n_2}, 1) = \sqrt{\frac{n_2}{n_1}} \left(\frac{a(n_2)}{a(n_1)}\right)^2 L(E_{-n_1}, 1).$$

Thus for $d > 0$ so that $d \equiv 3 \pmod 9$, $L(E_d, 1) = 0$ if and only if $a(d/3) = 0$.

Now, we want to investigate the case for $d < 0$ so that $3|d$ and $d \equiv 6 \pmod 9$. We will look at $S_{3/2}(\Gamma_0(108), \chi_3)$. The dimension of $S_{3/2}(\Gamma_0(108), \chi_3)$ is 5, and we have the basis:

$$h_1(z) = q - 2q^{13} - q^{25} - 2q^{28} + \cdots$$

$$h_2(z) = q^2 + q^5 - q^8 - q^{11} - q^{14} - q^{20} - 2q^{23} + 2q^{26} + \cdots$$

$$h_3(z) = q^4 - q^{13} - 2q^{16} + 2q^{25} - q^{28} + \cdots$$

$$h_4(z) = q^7 - q^{13} - q^{19} + \cdots$$

$$h_5(z) = q^{10} - q^{16} - q^{19} - q^{22} + q^{25} + \cdots$$

By Sturm's Theorem, we have

$$\mathcal{S}_1(h_1(z) - h_4(z) + 2h_5(z)) = F(z),$$

$$\mathcal{S}_2(h_1(z) - h_4(z) + 2h_5(z)) = 0,$$

$$\mathcal{S}_3(h_1(z) - h_4(z) + 2h_5(z)) = 0,$$

$$\mathcal{S}_1(h_1(z) - 4h_3(z) - 5h_4(z) + 10h_5(z)) = F(z) + 4F(z)|V(2),$$

$$\mathcal{S}_2(h_1(z) - 4h_3(z) - 5h_4(z) + 10h_5(z)) = 0, \text{ and}$$

$$\mathcal{S}_3(h_1(z) - 4h_3(z) - 5h_4(z) + 10h_5(z)) = 0.$$

Since we took $t = 1, 2$, and 3, then by Theorem 2.50 we have $\mathcal{S}_t((h_1(z) - h_4(z) + 2h_5(z))|T_{p^2}) = \mathcal{S}_t((h_1(z) - h_4(z) + 2h_5(z))|T(p)$ for primes $p > 3$. Also, since 1, 2 and 3 divide $4N$, then we have $(h_1(z) - h_4(z) + 2h_5(z))|T_{p^2} - \lambda(p)(h_1(z) - h_4(z) + 2h_5(z))$ in: $\ker(\mathcal{S}_1)$, $\ker(\mathcal{S}_2)$, and $\ker(\mathcal{S}_3)$. By MAGMA computations, $\ker(\mathcal{S}_1) \cap \ker(\mathcal{S}_2) \cap \ker(\mathcal{S}_3) = 0$. This implies that $h_1(z) - h_4(z) + 2h_5(z)$ is a Hecke eigenform. Similar computations can be done and conclusions drawn for $h_1(z) - 4h_3(z) - 5h_4(z) + 10h_5(z)$.

Again we want forms that are simple to compute, so we will take the quadratic forms $Q_3(x, y, z) = x^2 + y^2 + 7z^2 + xz$ and $Q_4(x, y, z) = x^2 + 2y^2 + 4z^2 + xy + yz$. The forms correspond to

$$B_1 = \begin{pmatrix} 1 & 0 & 1/2 \\ 0 & 1 & 0 \\ 1/2 & 0 & 7 \end{pmatrix} \text{ and}$$

$$B_2 = \begin{pmatrix} 1 & 1/2 & 0 \\ 1/2 & 2 & 1/2 \\ 0 & 1/2 & 4 \end{pmatrix} \text{ respectively.}$$

Also, we will denote the theta series corresponding to Q_3 and Q_4 by θ_{Q_3} and θ_{Q_4} respectively. We have $\theta_{Q_3}, \theta_{Q_4} \in M_{3/2}(\Gamma_0(108), \chi_3)$. By Sturm's Theorem, $\theta_{Q_3} - \theta_{Q_4} = 2h_1(z) - 4h_3(z) - 6h_4(z) + 12h_5(z)$. Hence, $\mathcal{S}_1(\theta_{Q_3} - \theta_{Q_4}) = 2F(z) - 4F(z)|V(2)$.

By Waldspurger's Theorem, we have

$$L(E_{-3n_2},1)=\sqrt{\frac{n_2}{n_1}}\left(\frac{a(n_2)}{a(n_1)}\right)^2 L(E_{-3n_1},1).$$

Table 2

n_2	n_1	$a(n_1)$	$L(E_{-3n_1},1)$
$n_2\equiv 1 \pmod{24}$	1	2	0.58887...
$n_2\equiv 34 \pmod{48}$	34	12	1.81785...
$n_2\equiv 19 \pmod{24}$	19	-6	0.60794...
$n_2\equiv 13 \pmod{24}$	13	6	1.46993...
$n_2\equiv 22 \pmod{48}$	22	-12	2.25989...
$n_2\equiv 7 \pmod{24}$	7	-6	1.00159...
$n_2\equiv 10 \pmod{36}$	10	12	3.35196...
$n_2\equiv 46 \pmod{48}$	46	-12	1.56286...

Therefore for $d<0$ so that $d\equiv 6 \pmod 9$, $L(E_d,1)=0$ if and only if $a(-d/3)=0$. Furthermore by Theorem 3.11, we have

$$L(E_{n_2},1)=\sqrt{\frac{n_2}{n_1}}\left(\frac{a(n_2)}{a(n_1)}\right)^2 L(E_{-3n_1},1)$$

for $n_2\equiv 1 \pmod 3$. Thus for squarefree $d>0$ so that $d\equiv 1 \pmod 3$, $L(E_d,1)=0$ if and only if $a(d)=0$.

There are two pairs of cases related by Theorem 3.11 that we have not yet addressed: the first case is $d>0$ so that $d\equiv 6 \pmod 9$ and $d<0$ so that $d\equiv 1 \pmod 3$, and the second case is $d>0$ so that $d\equiv 2 \pmod 3$ and $d\equiv 3 \pmod 9$.

Theorem 3.12. *If d is a squarefree integer so that $d\equiv 2 \pmod 3$, then $L(E_d,1)=0$.*

Proof. Let ϵ be the root number of E_d. From Theorem 2.48, we know that $\epsilon=-\alpha$. Also, $\alpha=-\chi_d(27)\chi_d(-1)=-\chi_d(-27)$. Hence $\epsilon=\chi_d(-27)$.

Let squarefree $d > 0$ so that $d \equiv 2 \pmod 3$. So, we have:

$$\begin{aligned}\left(\frac{d}{-27}\right) &= \left(\frac{d}{-1}\right)\left(\frac{d}{27}\right)\\ &= \left(\frac{d}{3}\right)^3\\ &= \left(\frac{d}{3}\right)\\ &= \left(\frac{2}{3}\right)\\ &= -1.\end{aligned}$$

Hence $\epsilon = -1$.

Since $\epsilon = -1$ for $d > 0$ so that $d \equiv 2 \pmod 3$, then $L(E_d, 1) = 0$ by Theorem 2.42. □

Lemma 3.13. *Let* $Q_1(x, y, z) = x^2+3y^2+27z^2 = Q_2(x, y, z) = 3x^2+4y^2-2yz+7z^2$. *If squarefree* $d > 0$ *so that* $d \equiv 6 \pmod 9$, *then there are no solutions to* $Q_1(x, y, z) = d$ *or* $Q_2(x, y, z) = d$.

Proof. Let $d > 0$ be a squarefree integer such that $-d/3 \equiv 1 \pmod 3$. We have $x^2 + 3y^2 + 27z^2 \equiv 0$ or $1 \pmod 3$. Also, we have

$$\begin{aligned}3x^2 + 4y^2 - 2yz + 7z^2 &\equiv y^2 + yz + z^2\\ &\equiv y^2 + 4yz + 4z^2\\ &\equiv (y + 2z)^2\\ &\equiv 0 \text{ or } 1 \pmod 3.\end{aligned}$$

Hence $r_{Q_1}(d) = r_{Q_2}(d) = 0$. □

Combining this lemma and Theorem 3.12, if squarefree $d < 0$ so that $d \equiv 1 \pmod 3$ then the d^{th} coefficient of $\theta_{Q_1} - \theta_{Q_2}$ is zero.

Lemma 3.14. *Let ψ be the Dirichlet character with modulus 3, then $(\theta_{Q_3}(z) - \theta_{Q_4}(z))_\psi = \theta_{Q_3}(z) - \theta_{Q_4}(z)$.*

Proof. We have $(\theta_{Q_3}(z) - \theta_{Q_4}(z))_\psi = \sum_{n=0}^{\infty} c(n)\chi_3(n)q^n \in M_{3/2}(\Gamma_0(972), \psi_3)$ where ψ has modulus 3, and $c(n)$ is the n^{th} coefficient of $\theta_{Q_3}(z) - \theta_{Q_4}(z)$. By Sturm's Theorem, $\theta_{Q_3}(z) - \theta_{Q_4}(z) = (\theta_{Q_3}(z) - \theta_{Q_4}(z))_\psi$. □

Lemma 3.15. *If $d > 0$ and $d \equiv 2 \pmod 3$, then $r_{Q_3}(d) = r_{Q_4}(d)$.*

Proof. From Lemma 3.14 we have $(\theta_3(z) - \theta_4(z))_\psi = \theta_3(z) - \theta_4(z)$. Hence $b(n)\psi(n) = b(n)$ for all $n \geq 1$. If $d \equiv 2 \pmod 3$, then $\psi(d) = -1$. Thus $b(d) = -b(d)$. Hence, $b(d) = 0$. □

Finally, everything from this section comes together to allow us to prove our main result.

Theorem 3.16. *Assume BSD and let d be a squarefree integer. If $3|d$ and $d > 0$, there are nontrivial solutions to the Fermat cubic equation in $\mathbb{Q}(\sqrt{d})$ if and only if*

$$\#\{(x,y,z) \in \mathbb{Z}^3 : x^2+3y^2+27z^2 = d/3\} = \#\{(x,y,z) \in \mathbb{Z}^3 : 3x^2+4y^2+7z^2-2yz = d/3\}.$$

If $3 \nmid d$ so that $d > 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only if

$$\#\{(x,y,z) \in \mathbb{Z}^3 : x^2+y^2+7z^2+xz = d\} = \#\{(x,y,z) \in \mathbb{Z}^3 : x^2+2y^2+4z^2+xy+yz = d\}.$$

If $3|d$ and $d < 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only there are nontrivial solutions in $\mathbb{Q}(\sqrt{-d/3})$. Finally, if $3 \nmid d$ and $d < 0$, there are nontrivial solutions in $\mathbb{Q}(\sqrt{d})$ if and only if there are nontrivial solutions in $\mathbb{Q}(\sqrt{-3d})$.

Proof. Throughout this section, we have shown when $L(E_d, 1) = 0$. Let d be one of these such values. By BSD since $L(E_d, 1) = 0$, then $\text{rank}(E_d) > 0$. Hence by Theorem 3.10, there are nontrivial solutions to the Fermat cubic in $\mathbb{Q}(\sqrt{d})$. □

Bibliography

[1] William W. Adams and Larry Joel Goldstein. *Introduction to number theory.* Prentice-Hall Inc., Englewood Cliffs, N.J., 1976.

[2] Alexander Aigner. Ein zweiter Fall der Unmöglichkeit von $x^3 + y^3 = z^3$ in quadratischen Körpern mit durch 3 teilbarer Klassenzahl. *Monatsh. Math.*, 56:335–338, 1952.

[3] Alexander Aigner. Weitere Ergebnisse über $x^3 + y^3 = z^3$ in quadratischen Körpern. *Monatsh. Math.*, 56:240–252, 1952.

[4] Alexander Aigner. Die kubische Fermatgleichung in quadratischen Körpern. *J. Reine Angew. Math.*, 195:3–17 (1955), 1956.

[5] Michael Artin. *Algebra.* Prentice Hall Inc., Englewood Cliffs, NJ, second edition, 2011.

[6] W. Burnside. On the rational solutions $x^3+y^3+z^3 = 0$ in quadratic fields. *Proc. London Math. Soc.*, 14:1–4, 1915.

[7] David M. Burton. *Elementary number theory.* McGraw Hill Publishing Company Ltd, Dubuque, IA, sixth edition, 2007.

[8] F. J. Duarte. On the equation $x^3 + y^3 + z^3 = 0$. *Estados Unidos de Venezuela. Bol. Acad. Ci. Fís. Mat. Nat.*, 8:971–979, 1944.

[9] L. Euler. Vollstndige anleitung zur algebra. 1770. St. Petersburg.

[10] R. Fueter. Die diophantische gleichung $\xi^3 + \eta^3 + \zeta^3 = 0$. *Sitzungsberichte Heidelberg Akad. d. Wiss.*, 25:25, 1913.

[11] R. Fueter. Über kubische diophantische gleichungen. *Comm. Math. Helv.*, 2:69–89, 1930.

[12] Henryk Iwaniec. *Topics in classical automorphic forms*, volume 17 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1997.

[13] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53 of *American Mathematical Society Colloquium Publications*. American Mathematical Society, Providence, RI, 2004.

[14] L. J. P. Kilford. *Modular forms*. Imperial College Press, London, 2008. A classical and computational introduction.

[15] Neal Koblitz. *Introduction to elliptic curves and modular forms*, volume 97 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 1993.

[16] Yves Martin and Ken Ono. Eta-quotients and elliptic curves. *Proc. Amer. Math. Soc.*, 125(11):3169–3176, 1997.

[17] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[18] Ken Ono. *The web of modularity: arithmetic of the coefficients of modular forms and q-series*, volume 102 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 2004.

[19] Paulo Ribenboim. *13 lectures on Fermat's last theorem*. Springer-Verlag, New York, 1979.

[20] Paulo Ribenboim. *Fermat's last theorem for amateurs*. Springer-Verlag, New York, 1999.

[21] Karl Rubin and Alice Silverberg. Ranks of elliptic curves. *Bull. Amer. Math. Soc. (N.S.)*, 39(4):455–474 (electronic), 2002.

[22] J.-P. Serre. *A course in arithmetic*. Springer-Verlag, New York, 1973. Translated from the French, Graduate Texts in Mathematics, No. 7.

[23] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[24] Joseph H. Silverman and John Tate. *Rational points on elliptic curves*. Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1992.

[25] J.-L. Waldspurger. Sur les coefficients de Fourier des formes modulaires de poids demi-entier. *J. Math. Pures Appl. (9)*, 60(4):375–484, 1981.

Appendix A: Tables

Let d be a squarefree integer so that $0 < d < 141$ and $3|d$. The table below lists the rank and rank number of E_d, as well as the $(d/3)^{th}$ coefficients of θ_{Q_1} and θ_{Q_2}.

d	Rank	Root Number	$r_{Q_1}(d/3)$	$r_{Q_2}(d/3)$
3	0	1	2	0
6	1	−1	0	0
15	1	−1	0	0
21	0	1	4	6
30	0	1	0	4
33	1	−1	0	0
39	0	1	4	2
42	1	−1	0	0
51	1	−1	0	0
57	0	1	4	10
66	0	1	0	4
69	1	−1	0	0
78	1	−1	0	0
87	1	−1	0	0
93	2	1	16	16
102	0	1	8	4
105	1	−1	0	0
111	0	1	4	2
114	1	−1	0	0
123	1	−1	0	0
129	0	1	16	4
138	0	1	8	4
141	1	−1	0	0

From Theorem 3.11 we have $L(E_d, 1) = L(E_{-d/3}, 1)$. The table below demonstrates this using the choices of d from the previous table.

d	Rank	Root Number	$r_{Q_1}(-d)$	$r_{Q_2}(-d)$
-1	0	1	2	0
-2	1	-1	0	0
-5	1	-1	0	0
-7	0	1	4	6
-10	0	1	0	4
-11	1	-1	0	0
-13	0	1	4	2
-14	1	-1	0	0
-17	1	-1	0	0
-19	0	1	4	10
-22	0	1	0	4
-23	1	-1	0	0
-26	1	-1	0	0
-29	1	-1	0	0
-31	2	1	16	16
-34	0	1	8	4
-35	1	-1	0	0
-37	0	1	4	2
-38	1	-1	0	0
-41	1	-1	0	0
-43	0	1	16	4
-46	0	1	8	4
-47	1	-1	0	0

Let $d < 0$ so that $0 < d < 50$ and $3 \nmid d$. The table below lists the rank and rank number of E_d, as well as the d^{th} coefficients of θ_{Q_1} and θ_{Q_2}.

d	Rank	Root Number	$r_{Q_3}(d)$	$r_{Q_4}(d)$
1	0	1	4	2
2	1	-1	4	4
5	1	-1	8	8
7	0	1	4	10
10	0	1	16	4
11	1	-1	8	8
13	0	1	20	14
14	1	-1	8	8
17	1	-1	16	16
19	0	1	4	10
22	0	1	8	20
23	1	-1	16	16
26	1	-1	8	8
29	1	-1	24	24
31	0	1	16	4
34	0	1	16	4
35	1	-1	16	16
37	0	1	28	34
38	1	-1	16	16
41	1	-1	16	16
43	2	1	24	24
46	0	1	8	20
47	1	-1	16	16

From Theorem 3.11 we have $L(E_d, 1) = L(E_{-3d}, 1)$. The table below demonstrates this using the choices of d from the previous table.

$-3d$	Rank	Root Number	$r_{Q_3}(-d/3)$	$r_{Q_4}(-d/3)$
-3	0	1	4	2
-6	1	-1	4	4
-15	1	-1	8	8
-21	0	1	4	10
-30	0	1	16	4
-33	1	-1	8	8
-39	0	1	20	14
-42	1	-1	8	8
-51	1	-1	16	16
-57	0	1	4	10
-66	0	1	8	20
-69	1	-1	16	16
-78	1	-1	8	8
-87	1	-1	24	24
-93	0	1	16	4
-102	0	1	16	4
-105	1	-1	16	16
-111	0	1	28	34
-114	1	-1	16	16
-123	1	-1	16	16
-129	2	1	24	24
-138	0	1	8	20
-141	1	-1	16	16

Vita

Marvin Jones

Education:

- M.A. in Mathematics,

  Wake Forest University, 2012.

  Thesis title: *Solutions of the cubic Fermat equation in quadratic fields.*

  Advisor: Jeremy Rouse

- B.S. in Mathematics,

  Winthrop University, 2010,

Conferences:

• A Computational Approach to $L-$functions, University of North Carolina at Greensboro, Greensboro, NC, May 14-18, 2012.

• *Solutions of the cubic Fermat equation in quadratic fields*, 2012 Southeastern Regional meeting on Numbers (SERMON), Western Carolina University, Cullowhee, NC, March 30-April 1, 2012.

Professional Activities:

• Member of ACM, AMS, and MAA.

Undergraduate Experience:

• Research Experience in Mathematics, Winthrop University, Summer 2010.