TRINOMIALS DEFINING QUINTIC NUMBER FIELDS

BY

JESSE LEIGH PATSOLIC

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

December 2014

Winston-Salem, North Carolina

Approved By:

Jeremy Rouse, Ph.D., Advisor

Kenneth S. Berenhaut, Ph.D., Chair

Fredric T. Howard, Ph.D.

Acknowledgments

I thank my LORD and Saviour Jesus Christ for His affect on my life and for His direction that brought me to Wake Forest University. I thank Him for His continued guidance in my future endevours as I follow His leading.

I would like to thank my advisor, Dr. Jeremy Rouse, for his enthusiasm and willingness to share his knowledge with me throughout my time at Wake Forest. I will forever admire him and aspire to share my enthusiasm as he does. I am very greatful to have had the privilege to work as a research assistant to Professor Jennifer Erway. I thank her for allowing me that oportunity. Much thanks to Professor Kenneth Berenhaut for his help, mentorship, and occasional raiding of my office pantry, of which he always has permission. You have had an impact on my life more than we both know.

I thank my office mates, Joel Barnett & Heather Hardeman, for putting up with me and my eccentricities and for providing much needed study breaks — even when I thought I was too busy. You inspire my nerdiness. I also thank my family for supporting me in my mathematical aspirations. I am very greatful to my parents for teaching me to enjoy learning and that my days of being a student will never end.

Finally, I thank my wife, Heather Gaddy Patsolic, for being my study partner, encourager, sounding board, and best friend: I could not have asked for any better. I look forward to continuing in life together devoted to glorifying our Creator.

Soli Deo Gloria

Table of Contents

List of Figures

Abstract

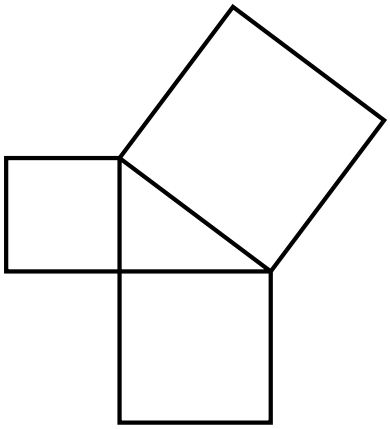
Jesse Leigh Patsolic

Given a number field K, how does one find polynomials $f(x)$, with a root in K, that have a small number of non-zero terms? Is it possible to make this method work to classify all the trinomials that generate a given field?

We start by computing the genus four curve, C_K, that parameterizes the trinomials defining K. We then compute a map from C_K to a cubic curve E. In the case where K is generated by $f(x) = x^5 + x + 3$, the curve E is an elliptic curve, with positive rank, defined over a degree ten number field L. We discuss the method used to compute the map from C_K to E. For future work, we hope to find generators of the set $E(L)$, to provably find, up to equivalence, the trinomials that define K, as mentioned above.

Chapter 1: Introduction

1.1 History



$$x^n + y^n = z^n; \quad n > 2 \tag{1.1}$$

Pierre de Fermat, circa 1637, conjectured that this equation does not have any whole-number solutions. This conjecture is often referred to as Fermat's Last Theorem, because it is the last of Fermat's theorems to elude mathematicians. This conjecture went unsolved until 1994, when Andrew Wiles, after revising errors in his 1993 submission, presented a fully correct proof of the semistable case of the Taniyama-Shimura conjecture which implies Fermat's Last Theorem. [1, 2]

The foundation behind these types of problems has its origins with the Babylonians, the Chinese, and the Greeks. The Greeks, through Pythagoras, usually receive the most credit, despite the fact that we now have evidence that suggests the Babylonians had obtained similar results about 1,000 years earlier. According to historians, Pythagoras lived circa 570 BC and was an avid student and teacher who inspired

a following. He and his students, the Pythagoreans, were very interested in studying triangles that have whole number side lengths. One of the most famous results attributed to the Pythagoreans are integer solutions to the genus zero equation

$$x^2 + y^2 = z^2, \tag{1.2}$$

which we now call Pythagorean triples: A discussion of genus will be given later. The search for these Pythagorean triangles became somewhat of an obsession and led to many good, and bad, ideas.

Let us consider a few examples that will give insight into the methodology that is used in tackling the main problem.

1.2 Fermat's Last Theorem: $n = 4$

Consider the Fermat quartic:

$$F_4 : x^4 + y^4 - z^4 = 0. \tag{1.3}$$

We would like to find all integer solutions to this equation. However, this curve has genus 3 and is not as easy to work with when compared to a curve with genus 1. The goal is to find a map from this curve, F_4, to a curve of lower genus, preferably an elliptic curve. There exists a morphism, $\phi_0(x : y : z) = (xy : z^2 : y^2)$, that relates F_4 to the genus 1 curve

$$D : x^4 + z^4 - y^2z^2 = 0. \tag{1.4}$$

The point $p = (0 : 1 : 1)$ was found on D and by the theory of elliptic curves we can use both D and p to construct a map to an elliptic curve. The map, ϕ_1, and elliptic curve, E, are given by

$$\phi_1(x : y : z) = (2xyz + 2xz^2 : 4yz^2 + 4z^3 : x^3) \tag{1.5}$$

$$E : y^2 = x^3 - 4x. \tag{1.6}$$

Let $\mathcal{G}$ be the Mordell-Weil group of E. Then $\mathcal{G} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ with elements $\{(0:1:0),(0:0:1),(2:0:1),(-2:0:1)\}$. Now, to find the rational points on F_4 we will take the preimages of these four points by backtracking through the series of maps that have been calculated.

This returns a scheme for each of the four points. The rational points on two of these schemes are $(0:-1:1)$, $(0:1:1)$, $(-1:0:1)$, $(1:0:1)$. The other two schemes are pointless. Note that a *scheme* is an algebraic geometric object defined by a system of polynomial equations over a ring.

This shows that the only integer solutions to equation (1.3) have one of x, y or z equal to 0 and this proves Fermat's last theorem for the case $n = 4$.

1.3 Fermat's Last Theorem: $n = 7$

Consider the degree 7 Fermat equation:

$$F_7 : x^7 + y^7 + z^7 = 0, \tag{1.7}$$

which is related to the curve

$$D : x^3y + y^3z + z^3x = 0, \tag{1.8}$$

known as Klein's Quartic, by the morphism $\varphi_0(x:y:z) = (x^3z : y^3x : z^3y)$.
It is possible to take the quotient of the curve by the automorphism group, G of D, and yield a curve $E = D/G$ of lower genus; doing this, we get a genus 1 curve embedded in $\mathbb{P}^2$, where Ω is the map and F is the image of Ω. $\mathbb{P}^3$ along with a map φ_1.

$$E : \begin{cases} 3xy + 9y^2 - 30yz + 18z^2 + 6xw + 6yw - 12zw + 8w^2 = 0, \\ x^2 - 12xy + 3y^2 + 8xz - 8xw = 0 \end{cases} \tag{1.9}$$

The equations for the map have been omitted due to their complexity. The genus of E is 1, and a non-singular point $p = (1:1:1:0)$ was found on E. Becuase of

this, we have that there exists an elliptic curve, E', in Weierstrass form with a map $\varphi_2 : E \to E'$ that is an isomorphism and $\varphi_2(p) = (0 : 1 : 0)$. This curve is given by

$$E' : y^2 - \frac{27}{4}xy - \frac{5103}{64}y = x^3 + \frac{243}{8}x^2 + \frac{32805}{128}x + \frac{531441}{4096}. \tag{1.10}$$

We now have a map $\Phi : F_7 \to E'$ defined by the composition $\Phi(p) = \varphi_2(\varphi_1(\varphi_0(p)))$. The Mordell-Weil Group of E' is isomorphic to $\mathbb{Z}/2\mathbb{Z}$ with elements

$$\{(0 : 1 : 0), (-81/16 : 729/32 : 1)\}.$$

Computing the preimages of these points, by backtracking with the map Φ, we get that the only integer solutions to equation (1.7) are

$$\{(-1 : 0 : 1), (-1 : 1 : 0), (0 : -1 : 1)\},$$

thus verifying Fermat's Last Theorem for the case $n = 7$.

1.4 Genera

The genus of a curve is an important characteristic that we use frequently throughout this work. It is a topological invariant that provides information about the curve's "niceness." Curves of genus zero and one are easier to work with than their genus greater than one counterparts.

Working with a curve C, of genus greater than one, becomes a problem of finding the proper sequence of maps from curve to curve. In some cases, the genera are in descending order; in other cases, one might map to a higher genus curve with simpler equations and from there map to a lower genus curve. In either case it is a problem of finding the correct rabbit hole to venture down.

Let us give some definitions with auxiliary examples:

Definition 1. *The connected sum of n tori is called a* genus *n surface. A sphere is considered a* genus *zero surface.[3]*

Throughout this thesis, $\mathbb{Q}$ will represent the set of rational numbers and $\mathbb{Q}_p$ will represent the p-adic numbers.

1.4.1 Genus Zero Curves

A genus zero curve will either have infinitely many rational points or none at all. The curve related to equation (1.2),

$$C : x^2 + y^2 - z^2 = 0, \tag{1.11}$$

is an example of a genus zero curve that has infinitely many rational points, namely the Pythagorean triples.

Definition 2. Projective n-space*, denoted* $\mathbb{P}^n$*, is the set of all lines through the origin of a vector space V, of dimension* $n+1$*, in which antipodal points are equivalent. If* K *is a field, then*

$$\mathbb{P}^n(K) = \{(a_0 : a_1 : \cdots : a_n) \mid a_i \in K \text{ but not all } a_i \text{ are zero}\},$$

and for $\lambda \neq 0 \in K$ *we consider*

$$(a_0 : a_1 : \cdots : a_n) \equiv (\lambda a_0 : \lambda a_1 : \cdots : \lambda a_n).$$

Traditionally, λ *is chosen so that one of the coordinates becomes 1.*

A method of finding Pythagorean triples is given by the following theorem:

Theorem 1.1. *If a curve* $\mathcal{C}$ *has genus equal to 0, then it is isomorphic to* $\mathbb{P}^1$*. For* $C : x^2 + y^2 - z^2 = 0$ *the isomorphism is given by* $\Delta : \mathbb{P}^1 \to C$

$$\Delta(m : n) = (m^2 - n^2 : 2mn : m^2 + n^2). \tag{1.12}$$

Thus, given a point $p = (m : n)$ in $\mathbb{P}^1$, the map $\Delta(m:n)$ produces a Pythagorean triple.

Theorem 1.2 (Hasse-Minkowski)**.** *A homogeneous quadratic equation in several variables is solvable by rational numbers, not all zero, if and only if it is solvable in the p-adic numbers for each prime p including the infinite prime. The p-adic numbers at the infinite prime are the real numbers. [4]*

An example of a genus zero curve without rational points is given by the equation

$$C' : x^2 + y^2 - 3z^2 = 0. \tag{1.13}$$

Rearranging the equation to the form, $x^2 + y^2 = 3z^2$, we see that the power of 3 dividing the left-hand side is even, while the power of 3 dividing the right-hand side is odd, which is equivalent to saying that there are no solutions in $\mathbb{Q}_3$. Thus, by theorem (1.2) there cannot be any rational solutions to this equation.

1.4.2 Genus One Curves

Definition 3. *An* elliptic curve *E over a field K is a non-singular cubic curve over K with a given point $O \in E(K)$. [4]*

Theorem 1.3. *If a cubic curve has a rational point, then it can be transformed into* Weierstrass normal form*, which is an equation of the form*

$$y^2 = x^3 + ax^2 + bx + c. \quad [5] \tag{1.14}$$

If C/K is a genus one curve, then there are two cases:

(1) C has a K-rational point and is therefore isomorphic to an elliptic curve E.

or

(2) C does not have K-rational points.

1.4.3 Genus Greater Than One Curves

One of the main conjectures dealing with curves of genus greater than one was made by Mordell around 1922, and later proven by Faltings in 1984. [6] The statement is as follows.

Theorem 1.4 (Faltings)**.** *If $C/\mathbb{Q}$ is a non-singular curve of genus greater than one, then $C(\mathbb{Q})$ is finite.*

At the moment there does not exist an algorithm to determine the finite set $C(\mathbb{Q})$, given a general curve, which is why motivation exists for studying points on such curves.

1.4.4 Motivation

The following is the question we have decided to investigate: Given a number field K, how does one find polynomials $f(x)$, with a root in K, that have a small number of non-zero terms? Is it possible to make this method work to classify all the trinomials that generate a given field? We start by finding the equation for a curve C_K whose rational points are in bijection with the trinomials that generate K. This question warrants investigation as the classification of number fields is not yet well understood.

1.5 Definitions

Here are some theorems and definitions that will be helpful.

Definition 4. *If C and D are curves, a* morphism *from C to D is a map $\phi : C \to D$ where the coordinate functions of ϕ are polynomials, and there is no point on C where all the polynomials are zero.*

Definition 5. *If $\phi : C \to D$ is a morphism, then the degree of ϕ is the "usual" size of the set $\{c \in C \ : \ \phi(c) = p\}$ for a point p on D.*

Theorem 1.5. *If $\phi : C \to D$ is a map of curves of degree n and $g = \mathsf{genus}(D)$, then $\mathsf{genus}(C) \geq ng - n + 1$.*

Definition 6. *For a curve C, $C(\mathbb{Q})$ denotes the set of points on C with rational coordinates.*

Theorem 1.6. *If D is a genus one curve, and $p \in D(\mathbb{Q})$, then there is an elliptic curve E and a morphism $\phi : D \to E$ and an inverse ϕ^{-1} that is also a morphism.*

Definition 7. *If C is a curve, then the set*

$$\mathrm{Aut}(C) = \{\phi := C \to C; \phi, \phi^{-1} \textit{are both morphisms}\}$$

is a group under composition, with identity $\phi(x : y : z) = (x : y : z)$.

Theorem 1.7. *If G is a subgroup of $\mathrm{Aut}(C)$, there is a morphism, ϕ, from C to a curve D so that $\phi(p_1) = \phi(p_2)$ if and only if $p_2 = \sigma(p_1)$ for some $\sigma \in G$. We call D the curve quotient and read C/G as C mod G. The degree of the map ϕ is $|G|$.*

Theorem 1.8. *If C is a genus one curve and $p \in C(\mathbb{Q})$, (and p is non-singular), then there is an elliptic curve $E : y^2 = x^3 + Ax + B$ and a map $\varphi : C \to E$ that is an isomorphism and $\varphi(p) = (0 : 1 : 0)$.*

Chapter 2: The Main Problem

2.1 Trinomials Defining Quintic Number Fields

We have chosen to work with trinomials of the form $x^5 + ax + b$, when dealing with a trinomial of a different form the difference will be made explicit. We start by selecting a specific irreducible quintic trinomial,

$$f(x) = x^5 + x + 3, \tag{2.1}$$

and create the degree five number field $K = \mathbb{Q}[\alpha]$ where α is a root of f. Let $g(x) = x^5 + a_0x + b_0$ [see (A.1)] be a general quintic trinomial, with a root in the number field K. We then let $\beta = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 \in K$ and g be the minimal polynomial of β. We solve for the coefficients a, b, c, d, and e by computing the characteristic polynomial of M, which is the matrix representation of the linear transformation $L(x) = \beta x$ with respect to the basis $\{1, \beta, \ldots, \beta^4\}$. In order to perform this computation, we need the following machinery:

Lemma 1. *Let M be a $d \times d$ matrix of the form*

$$\begin{bmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & 0 & 1 \\ -n_0 & -n_1 & & \cdots & & -n_{d-1} \end{bmatrix},$$

where $n_i \in \mathbb{Z}$ for all i, then the characteristic polynomial of M is

$$x^d + n_{d-1}x^{d-1} + \cdots + n_1 x + n_0.$$

Proof [by induction on d].

Base Cases: Let $d = 2$. Then $B = \{1, \beta\}$ and

$$M = \begin{bmatrix} 0 & 1 \\ -n_0 & -n_1 \end{bmatrix} \tag{2.2}$$

and the characteristic polynomial is given by

$$\det(xI - M') = \begin{vmatrix} x & -1 \\ n_0 & n_1 + x \end{vmatrix} = x^2 + n_1 x + n_0. \quad \clubsuit \tag{2.3}$$

Let $d = 3$. Then

$$M = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ -n_0 & -n_1 & -n_2 \end{bmatrix} \text{ and} \tag{2.4}$$

$$\det(xI - M') = \begin{vmatrix} x & -1 & 0 \\ 0 & x & -1 \\ n_0 & n_1 & n_2 + x \end{vmatrix} \tag{2.5}$$

$$= x^3 + n_2 x^2 + n_1 x + n_0. \quad \clubsuit \tag{2.6}$$

Therefore assume the inductive hypothesis that there exists some natural number m so that $k \leq m$ implies that the characteristic polynomial of the $k \times k$ matrix M_k is $f(x) = x^k + \sum_{i=0}^{k-1} n_i x^i$. This must be shown to hold for $k = m + 1$.

Consider $k = m + 1$. Then

$$(xI - M) = \begin{bmatrix} x & -1 & 0 & 0 & \cdots & 0 \\ 0 & x & -1 & 0 & \cdots & 0 \\ 0 & 0 & x & -1 & \cdots & 0 \\ \vdots & & \ddots & & & \vdots \\ 0 & 0 & \cdots & \ddots & x & -1 \\ n_0 & n_1 & \cdots & n_l & \cdots & n_m \end{bmatrix}. \tag{2.7}$$

Taking advantage of the sparsity of the matrix, the determinant may be calculated easily using cofactor expansion.

$$\det(xI - M) = x \begin{vmatrix} x & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & x & -1 \\ n_1 & n_2 & \cdots & \cdots & n_m \end{vmatrix} - (-1) \begin{vmatrix} 0 & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & x & -1 \\ n_0 & n_2 & \cdots & \cdots & n_m \end{vmatrix} \tag{2.8}$$

By the inductive hypothesis the first term becomes

$$x(x^m + n_m x^{m-1} + \cdots + n_2 x + n_1) = x^{m+1} + n_m x^m + \cdots + n_2 x^2 + n_1 x. \tag{2.9}$$

Consider the cofactor expansion of the second term,

$$\begin{vmatrix} 0 & -1 & 0 & \cdots & 0 \\ 0 & x & -1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \ddots & x & -1 \\ n_0 & n_2 & \cdots & \cdots & n_m \end{vmatrix} = -(-1) \begin{vmatrix} 0 & -1 & \cdots & 0 \\ \vdots & x & \ddots & \vdots \\ 0 & \ddots & x & -1 \\ n_0 & n_3 & \cdots & n_m \end{vmatrix}. \tag{2.10}$$

The right side of equation (2.10) can be further simplified using cofactor expansion:

$$= -(-1) \begin{vmatrix} 0 & -1 & \cdots & 0 \\ \vdots & x & \ddots & \vdots \\ 0 & \ddots & x & -1 \\ n_0 & \mathbf{n_4} & \cdots & n_m \end{vmatrix}. \tag{2.11}$$

Note that for each iteration the column containing $-n_0$ is kept, while the second column is removed. Therefore the $(m-2)$ iteration yields

$$= -(-1)\begin{vmatrix} 0 & -1 \\ n_0 & n_m \end{vmatrix} \tag{2.12}$$

$$= 1\,(0(n_m) - (n_0)(-1)) \tag{2.13}$$

$$= n_0. \tag{2.14}$$

Therefore, substituting equations (2.9) and (2.14) into (2.8) we have

$$\det(xI - M') = x^{m+1} + n_m x^m + \cdots + n_2 x^2 + n_1 x + n_0, \tag{2.15}$$

and the characteristic equation is as stated above. □

Theorem 2.1. *Assume that β is an algebraic number of degree d and $K = \mathbb{Q}[\beta]$. Let $L : K \to K$ be defined by $L(x) = \beta x$ where M is the matrix representation of L with respect to the basis $B = \{1, \beta, \ldots, \beta^{d-1}\}$. Then β is a root of the characteristic polynomial of M.*

Proof.

We have that β satisfies the equation

$$\beta^d + n_{d-1}\beta^{d-1} + \cdots + n_1\beta + n_0 = 0. \tag{2.16}$$

Then

$$L(1) = \beta, \tag{2.17}$$

$$L(\beta) = \beta^2, \tag{2.18}$$

$$\vdots$$

$$L(\beta^{d-1}) = \beta^d = -n_0 - n_1\beta - \cdots - n_{d-1}\beta^{d-1}. \tag{2.19}$$

Equation (2.19) comes from rearanging equation (2.16). And

$$M = \begin{bmatrix} 0 & 1 & 0 & \cdots & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & \vdots \\ 0 & 0 & 0 & 0 & 1 & 0 \\ -n_0 & -n_1 & & \cdots & & -n_{d-1} \end{bmatrix}, \tag{2.20}$$

then by the Lemma it follows that the characteristic polynomial of M is

$$x^d + n_{d-1}x^{d-1} + \cdots + n_1 x + n_0 \tag{2.21}$$

of which β is a root. □

2.1.1 Curves

Using theorem (2.1), we compute the characteristic polynomial of M,

$$x^5 + n_4 x^4 + n_3 x^3 + n_2 x^2 + n_1 x + n_0, \tag{2.22}$$

where the n_i are polynomials in a, b, c, d, and e. Setting n_4, n_3, and n_2 equal to zero and using them as components, we yield a genus four curve, C_K, described by the equations

$$C_K = \begin{cases} n_4 = -5a + 4e = 0 \\ n_3 = 10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2 = 0 \\ n_2 = -10a^3 + 4b^2c - 6ac^2 + 15bc^2 - 12abd + 15b^2d - 45acd - 4cd^2 - 9d^3 + 24a^2e \\ \quad - 45abe + 4c^2e + 8bde + 6cde - 45d^2e - 18ae^2 + 33be^2 - 45ce^2 + 4e^3 = 0. \end{cases} \tag{2.23}$$

This curve, by construction, parameterizes the trinomials that have roots in K. By theorem (1.4) we have that $C_K(\mathbb{Q})$ is finite, and therefore finitely many equivalence classes of trinomials define K. Our goal is to provably find all such trinomials. Due

to how projective space is defined, we have that if $\beta \in K$ is an element such that $p(x)$ is the minimal polynomial of β is a trinomial, then the same is true of $d\beta$ if $d \in \mathbb{Q}$, where

$$\begin{aligned} p(x) &= x^5 + r_1 x + r_0 \text{ and} \\ q(x) &= x^5 + r_1 d^4 x + r_0 d^5 \end{aligned} \tag{2.24}$$

are in the same equivalence class.

2.2 Maps

We make a simplification of the curve C_K by setting $e = \frac{5}{4}a$ and substituting this into the other two equations. This yields the curve C_1, defined by

$$C_1 = \begin{cases} m_1 = -\frac{5}{8}a^2 + \frac{75}{4}ab + 4bd + 2c^2 + 15cd = 0 \\ m_2 = -\frac{5}{16}a^3 - \frac{75}{16}a^2 b - \frac{1125}{16}a^2 c - 2abd - ac^2 - \frac{75}{2}acd - \frac{225}{4}ad^2 \\ \qquad + 4b^2 c + 15b^2 d + 15bc^2 - 4cd^2 - 9d^3 = 0. \end{cases} \tag{2.25}$$

The curves C_1 and C_K are isomorphic with map $\varphi_0 : C_1 \to C_K$, defined by

$$\varphi_0(a : b : c : d) = \left(a : b : c : d : \tfrac{5}{4}a\right) \tag{2.26}$$

and inverse $\varphi_0^{-1} : C_K \to C_1$, defined by

$$\varphi_0^{-1}(a : b : c : d : e) = (a : b : c : d) \tag{2.27}$$

Computing the curve quotient in `Magma`, as in theorem (1.7), was computationally very memory intensive. Some calculations had to be done in a degree 10 number field, which seemed to grind computations to a halt. As such, a method to circumvent `Magma`'s built in routines had to be devised.

The equation

$$f_0(y) = y^{10} - 3y^6 - 33y^5 - 4y^2 + 12y - 9 \tag{2.28}$$

is used to construct $\mathbb{Q}[z]$, where z is a root of f_0. This makes it so that the quintic, equation (2.1), factors as a quadratic, f_1, times a cubic, f_2 over $\mathbb{Q}[z]$. We build the splitting field, L, of $\mathbb{Q}[z]$ using f_1 and f_2. The five roots — α_1, α_2 from f_1 and $\alpha_3, \alpha_4, \alpha_5$ from f_2 — are used to build the Vandermonde matrix, which gives the map

$$\varphi_1 : C_K \to D \text{ defined by} \tag{2.29}$$

$$\varphi_1 (a : b : c : d : e) = \begin{bmatrix} 1 & \alpha_1 & \alpha_1^2 & \alpha_1^3 & \alpha_1^4 \\ 1 & \alpha_2 & \alpha_2^2 & \alpha_2^3 & \alpha_2^4 \\ 1 & \alpha_3 & \alpha_3^2 & \alpha_3^3 & \alpha_3^4 \\ 1 & \alpha_4 & \alpha_4^2 & \alpha_4^3 & \alpha_4^4 \\ 1 & \alpha_5 & \alpha_5^2 & \alpha_5^3 & \alpha_5^4 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix}, \tag{2.30}$$

where D is the curve given by

$$D = \begin{cases} x_1 + x_2 + x_3 + x_4 + x_5 = 0 \\ x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = 0 \\ x_1^3 + x_2^3 + x_3^3 + x_4^3 + x_5^3 = 0. \end{cases} \tag{2.31}$$

There is an automorphism of D, given by

$$\varphi_2 : D \to D \text{ defined by} \tag{2.32}$$

$$\varphi_2(x_1 : x_2 : x_3 : x_4 : x_5) = (x_2 : x_1 : x_3 : x_4 : x_5) \tag{2.33}$$

Composing these maps we construct an automorphism of C_1,

$$\Phi : C_1 \to C_K \to D \to D \to C_1 \text{ defined by} \tag{2.34}$$

$$\Phi(p) = \varphi_0^{-1} \circ \varphi_1^{-1} \circ \varphi_2 \circ \varphi_1 \circ \varphi_0(p). \tag{2.35}$$

The map (2.34) can be represented by

$$\Phi(a : b : c : d) = M \begin{bmatrix} a & b & c & d \end{bmatrix}_{,}^{T} \tag{2.36}$$

where M is a 4×4 matrix, such that $M^2 = I$. The eigenvalues of M are $\{-1, 1\}$. The dimension of the eigenspace associated with -1 is three. We take the basis of

this nullspace, $\{e_2, e_3, e_4\}$ given by (A.2), and obtain a map from C_K to $\mathbb{P}^2$, given by

$$\Omega(a : b : c : d) \to (e_2 : e_3 : e_4).$$

This map is a map to the quotient curve by the automorphism Φ. The automorphism either fixes or negates all of e_2, e_3, and e_4, which implies that acting by the automorphism and then taking the map to the curve is equivalent to just taking the map itself.

Next we describe how to compute the image of Ω which is expected to be a cubic curve. We have the automorphism,

$$M = \begin{bmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} & \gamma_{24} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} & \gamma_{34} \\ \gamma_{41} & \gamma_{42} & \gamma_{43} & \gamma_{44} \end{bmatrix}, \tag{2.37}$$

that acts on polynomials in a, b, c, and d, defined by

$$\begin{aligned} \psi(p(a : b : c : d)) = p(&\gamma_{11}a + \gamma_{12}b + \gamma_{13}c + \gamma_{14}d : \gamma_{21}a + \gamma_{22}b + \gamma_{23}c + \gamma_{24}d : \\ &\gamma_{31}a + \gamma_{32}b + \gamma_{33}c + \gamma_{34}d : \gamma_{41}a + \gamma_{42}b + \gamma_{43}c + \gamma_{44}d) \end{aligned} \tag{2.38}$$

Therefore, any polynomial p can be written as a sum of one fixed by ψ and one sent to its negative by ψ:

$$p = \frac{p + \psi(p)}{2} + \frac{p - \psi(p)}{2}. \tag{2.39}$$

The basis is given by $\{e_1, e_2, e_3, e_4\}$ and we have that, under the automorphism, e_1 is fixed, and e_2, e_3, and e_4 are all sent to their negatives. Thus we have that $\{e_1^i e_2^j e_3^k e_4^l : i + j + k + l = 3\}$ spans the 20 dimensional space, $\mathcal{V}$, of all degree 3 polynomials. Becuase M is diagonalizable, a, b, c, and d can be written as linear combinations of e_1, e_2, e_3, and e_4. Thus, $\mathcal{V} = \mathcal{V}^+ \oplus \mathcal{V}^-$, where $\mathcal{V}^+$ is the subspace that

is fixed under ψ, and $\mathcal{V}^-$ is the subspace sent to its negative by ψ. Explicitly we have

$$\mathcal{V}^+ = \langle e_1^3, e_1e_2^2, e_1e_3^2, e_1e_4^2, e_1e_2e_3, e_1e_2e_4, e_1e_3e_4\rangle \tag{2.40}$$

$$\mathcal{V}^- = \langle e_1^2e_2, e_1^2e_3, e_1^2e_4, e_2^2e_3, e_2^2e_4, e_2e_4^2, e_3e_4^2, e_2e_3e_4, e_2^3, e_3^3, e_4^3\rangle. \tag{2.41}$$

Thus, the dimension of $\mathcal{V}^+$ is 7 and the dimension of $\mathcal{V}^-$ is 13.

There are 10 monomials — in a, b, c, and d — of the form $e_2^ie_3^je_4^k$ for $i+j+k=3$. These, along with $m_1e_2,\ m_1e_3,\ m_1e_4$, and m_2 are used to construct the matrix of their coefficients, M_1. These 14 polynomials all live in $\mathcal{V}^-$ and therefore must be linearly dependent. By computing the nullspace of M_1, we yield a vector, v, that encodes this linear relationship.

Starting with a point p, on C_1, we have that

$$m_1(p) = 0 \tag{2.42}$$

$$m_2(p) = 0, \tag{2.43}$$

and therefore

$$m_1(p)e_2(p) = m_1(p)e_3(p) = m_1(p)e_4(p) = m_2(p) = 0. \tag{2.44}$$

The other 10 monomials provide a map from the genus four curve, C_1, to a general cubic curve F, given by (A.3), living in $\mathbb{P}^2$, where Ω is the map and F is the image of the map Ω.

From the implementation given in [9], using the second case for the non-flex point $p = (0:1:0)$, we are able to transform F into an elliptic curve, E, in Weierstrass form. The curve E has positive rank, and therefore the set $E(L)$ of points with coefficients in L is infinite.

With the set $E(L)$ being infinite we are unable to proceed by backtracking the points to C_1, as compared with the examples given above. For future work, we hope to find generators for $E(L)$ in order to provably conclude, up to equivalence, the trinomials that define K.

2.3 Closing Remarks

To fully understand the specific case, where K is generated by $f(x) = x^5 + x + 3$, different methods will need to be employed. These methods include, elliptic curve Chabauty and n-descents, which are beyond the scope of this thesis.

As for a different case, where K_1 is defined by $h(x) = x^5 - 5x + 12$, `Magma` is able to handle the degree of the number fields in which computations must be made. In this case we have a map $\phi : C_{K_1}/\mathbb{Q} \to \mathbb{P}^1$. The elliptic curve related to C_{K_1} has rank 2. The curve C_{K_1} has at least 8 points on it over K_1 with rational image under ϕ. Only one of these points is in $C_{K_1}(\mathbb{Q})$.

Bibliography

[1] Eric W. Weisstein. Taniyama-Shimura Conjecture. From MathWorld—A Wolfram Web Resource. `http://mathworld.wolfram.com/Taniyama-ShimuraConjecture.html`.

[2] Eli Maor. *The Pythagorean Theorem: a 4,000-year history.* Princeton University Press, Princeton, New Jersey, 2007.

[3] Colin Adams and Robert Franzosa. *Introduction to Topology Pure and Applied.* Pearson, Upper Saddle River, New Jersey, 2008.

[4] Dale Husemöller. *Elliptic Curves.* Springer, New York, 2004.

[5] John Silverman, Joseph H. Tate. *Rational Points on Elliptic Curves.* Springer, New York, 1992.

[6] Eric W. Weisstein. "Mordell Conjecture." From MathWorld—A Wolfram Web Resource. `http://mathworld.wolfram.com/MordellConjecture.html`.

[7] David C. Marshall, Edward Odell, and Michael Starbird. *Number Theory Through Inquiry.* The Mathematical Association of America, 2007.

[8] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[9] Niels Duif. Transforming a general cubic elliptic curve equation to weierstrass form: A Sage implementation. *Technishe Universiteit Eindhoven*, 2011.

Appendix A: Equations and Figures

$$
\begin{aligned}
g(x) = x^5 &+ (-5a + 4e)x^4 + (10a^2 - 16ae + 4bd + 15be + 2c^2 + 15cd + 6e^2)x^3 \\
&+ (-10a^3 + 24a^2e - 12abd - 45abe - 6ac^2 - 45acd - 18ae^2 + 4b^2c \\
&+ 15b^2d + 15bc^2 + 8bde + 33be^2 + 4c^2e - 4cd^2 + 6cde - 45ce^2 - 9d^3 \\
&- 45d^2e + 4e^3)x^2 + (5a^4 - 16a^3e + 12a^2bd + 45a^2be + 6a^2c^2 \\
&+ 45a^2cd + 18a^2e^2 - 8ab^2c - 30ab^2d - 30abc^2 - 16abde - 66abe^2 \\
&- 8ac^2e + 8acd^2 - 12acde + 90ace^2 + 18ad^3 + 90ad^2e - 8ae^3 + b^4 \\
&+ 15b^3c + 4b^2ce + 2b^2d^2 + 39b^2de + 45b^2e^2 - 4bc^2d + 9bc^2e - 21bcd^2 \\
&- 45bcde - 45bd^3 + 4bde^2 + 21be^3 + c^4 + 3c^3d - 45c^3e + 45c^2d^2 \\
&+ 2c^2e^2 - 4cd^2e - 9cde^2 - 54ce^3 + d^4 + 3d^3e + 9d^2e^2 + 135de^3 + e^4)x \\
&- a^5 + 4a^4e - 4a^3bd - 15a^3be - 2a^3c^2 - 15a^3cd - 6a^3e^2 + 4a^2b^2c + 15a^2b^2d \\
&+ 15a^2bc^2 + 8a^2bde + 33a^2be^2 + 4a^2c^2e - 4a^2cd^2 + 6a^2cde - 45a^2ce^2 - 9a^2d^3 \\
&- 45a^2d^2e + 4a^2e^3 - ab^4 - 15ab^3c - 4ab^2ce - 2ab^2d^2 - 39ab^2de - 45ab^2e^2 \\
&+ 4abc^2d - 9abc^2e + 21abcd^2 + 45abcde + 45abd^3 - 4abde^2 - 21abe^3 - ac^4 \\
&- 3ac^3d + 45ac^3e - 45ac^2d^2 - 2ac^2e^2 + 4acd^2e + 9acde^2 + 54ace^3 - ad^4 \\
&- 3ad^3e - 9ad^2e^2 - 135ade^3 - ae^4 + 3b^5 + 12b^3ce + 6b^3d^2 + 45b^3de - 12b^2c^2d \\
&- 45b^2c^2e - 45b^2cd^2 + 12b^2de^2 + 27b^2e^3 + 3bc^4 + 45bc^3d + 6bc^2e^2 - 12bcd^2e \\
&- 63bcde^2 - 135bce^3 + 3bd^4 + 9bd^3e + 135bd^2e^2 + 3be^4 - 9c^5 - 18c^3e^2 + 36c^2d^2e \\
&+ 135c^2de^2 - 9cd^4 - 135cd^3e - 9ce^4 + 27d^5 + 27de^4 - 81e^5
\end{aligned}
\tag{A.1}
$$

$$
\begin{aligned}
e_2 = a + 1/2875232768805(&-255641046116z^9 + 291624576z^8 - 1457815680z^7 \\
&+ 5470264800z^6 + 725947992348z^5 + 8435668448100z^4 - 6999911424z^3 \\
&+ 40444017120z^2 + 932149295264z - 1471994757696)d \\
\\
e_3 = b + 1/8625698306415(&-276076779116z^9 - 306438770424z^8 - 1151259544386z^7 \\
&+ 5467500000z^6 + 803624513748z^5 + 10152853220100z^4 + 13104704464650z^3 \\
&+ 36257021424639z^2 + 964892087264z - 1496548741296)d \\
\\
e_4 = c + 1/63894061529(&30377560z^9 - 151855800z^8 + 569819250z^7 - 4268244375z^6 \\
&- 50632680z^5 - 729157440z^4 + 4212918450z^3 - 9418217625z^2 \\
&+ 102324458856z - 60750000)d
\end{aligned}
\tag{A.2}
$$

$$
\begin{aligned}
F := {} & \mathbf{X^3} + 1/63894061529(222760240z^9 - 1063086600z^8 + 4557114000z^7 - 25620266250z^6 - 376676624z^5 - 5498389560z^4 \\
& + 27789035400z^3 - 100866647250z^2 + 997424530502z - 1917259252014)\mathbf{X^2Y} + 1/8625698306415(-367635801232z^9 \\
& - 1381939128348z^8 + 2308642836228z^7 - 17290763165790z^6 + 1283343198096z^5 + 15416698679700z^4 + 42369325066800z^3 \\
& - 38164781115522z^2 + 675268999287538z - 3337568644992)\mathbf{X^2Z} + 1/63894061529(-1214846400z^9 + 4558554000z^8 \\
& - 34145955000z^7 + 324000000z^6 + 2186416320z^5 + 33703347600z^4 - 75345741000z^3 + 1330720245000z^2 - 3402245760z \\
& + 2187184320)\mathbf{XY^2} + 1/575046553761(981329838464z^9 + 1533846276696z^8 - 1749747456z^7 + 8746894080z^6 \\
& - 2976811104192z^5 - 36739572623400z^4 - 50614010688600z^3 + 41999468544z^2 - 4167983456576z \\
& + 6183062289984)\mathbf{XYZ} + 1/958410922935(388832768z^9 - 1943754240z^8 + 7293686400z^7 - 54633528000z^6 - 648098304z^5 \\
& - 9333215232z^4 + 53925356160z^3 - 120553185600z^2 + 2127597060928z - 3067692553392)\mathbf{XZ^2} \\
& + 1/958410922935(-777665536z^9 + 3887508480z^8 - 14587372800z^7 + 109267056000z^6 + 1296196608z^5 + 18666430464z^4 \\
& - 107850712320z^3 + 241106371200z^2 - 4255194121856z + 1555200000)\mathbf{Y^2Z} + 1/319470307645(-1620000000z^9 \\
& + 7290614400z^8 - 36445392000z^7 + 136756620000z^6 + 2786334464z^5 + 41308156800z^4 - 174997785600z^3 \\
& + 1011100428000z^2 - 5320807183392z + 3110498304)\mathbf{YZ^2} + 1/43128491532075(7850638707712z^9 + 122707702135 68z^8 \\
& - 13997979648z^7 + 69975152640z^6 - 23814488833536z^5 - 293916580987200z^4 - 404912085508800z^3 \\
& + 335995748352z^2 - 33343867652608z + 4946449831 9872)\mathbf{Z^3} = 0
\end{aligned}
\tag{A.3}
$$

$$
E : y^2 = x^3 + a_4x + a_6 \tag{A.4}
$$

where

$$
\begin{aligned}
a_4 = {} & -23400z^9 - 3375z^8 + 151875z^7 + 70200z^5 \\
& + 747225z^4 - 222750z^3 - 5163750z^2 + 93600z - 129600
\end{aligned}
\tag{A.5}
$$

$$
\begin{aligned}
a_6 = {} & -35691460z^9 + 1613139060z^8 + 339840z^7 - 64675800z^6 + 6715380z^5 \\
& - 3177725250z^4 - 53503427250z^3 + 248316840z^2 + 2077305040z - 3128144010
\end{aligned}
\tag{A.6}
$$

Figure A.1: C_K projected into $\mathbb{R}^3$

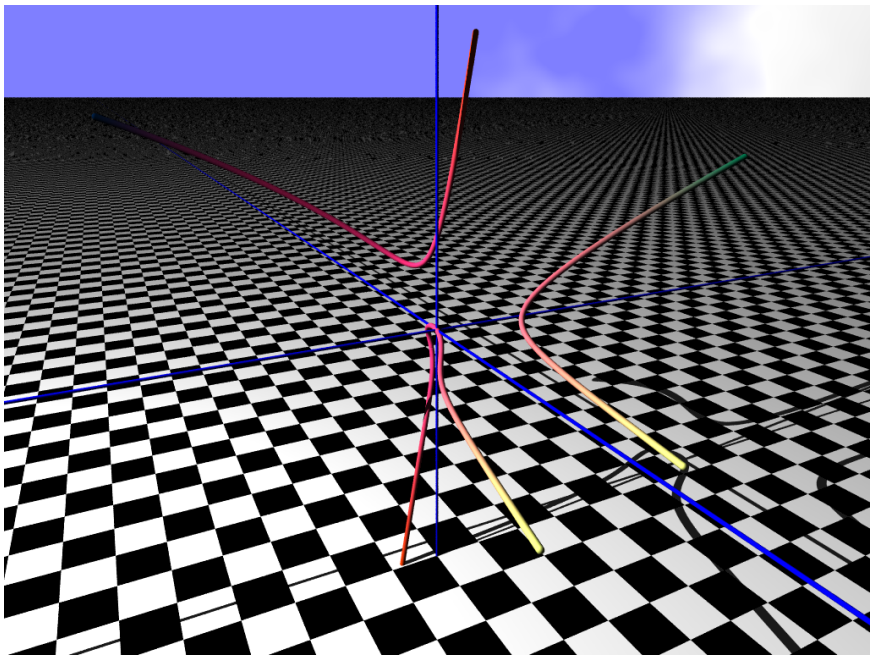


Figure A.2: C_K projected into $\mathbb{R}^3$

Appendix B: Code listings

B.1 FC.magma

```
/*
*   Created by
*   Jesse Leigh Patsolic <patsjl12@wfu.edu>
*   Summer 2013
*   Wake Forest University
*   Department of Mathematics
*   Under the advisement of Dr. Jeremy Rouse
*/

/* Instantiating the Polynomial Rings */
A<a,b,c,d,e> := PolynomialRing(Rationals(),5);
B<t> := PolynomialRing(Rationals());
C<x> := PolynomialRing(A);

f := t^5 + t + 3;

/* Building the number field Q[alpha] */
K<alpha> := NumberField(f);

D<h,i,j,k,l> := PolynomialRing(K,5);

/*
*   Generating the matrix representation
*   of the linear transformation $L(x) = beta*x$,
*   where $beta = a + b*alpha + \dots + e*alpha^4$.
*/

AA := Matrix(D,[[h,i,j,k,l]]);

BB := Matrix(D,[[1],[alpha],[alpha^2],[alpha^3],[alpha^4]]);
CC := Matrix(D,[[alpha],[alpha^2],[alpha^3],[alpha^4],[alpha^5]]);
DD := Matrix(D,[[alpha^2],[alpha^3],[alpha^4],[alpha^5],[alpha
    ^6]]);
EE := Matrix(D,[[alpha^3],[alpha^4],[alpha^5],[alpha^6],[alpha
    ^7]]);
FF := Matrix(D,[[alpha^4],[alpha^5],[alpha^6],[alpha^7],[alpha
    ^8]]);

AABB := AA*BB;
AACC := AA*CC;
AADD := AA*DD;
AAEE := AA*EE;
AAFF := AA*FF;
```

```
41
42 /*  L is the 5x1 matrix with $a_{i1} = L(alpha^{i-1})$ */
43 L := Matrix([[AABB[1][1]],[AACC[1][1]],[AADD[1][1]],[AAEE[1][1]],[
       AAFF[1][1]]]);
44
45 /* Instantiating KK with entries $a^2$ as "null" values */
46 KK := Matrix(A,[[a^2,a^2,a^2,a^2,a^2],[a^2,a^2,a^2,a^2,a^2],[a^2,a
       ^2,a^2,a^2,a^2],[a^2,a^2,a^2,a^2,a^2],[a^2,a^2,a^2,a^2,a^2]]);
47
48 Mlist := []; /* A list to hold the values of JJ */
49 count := 1;
50 for yy in [*1,2,3,4,5*] do
51     for y in [*h,i,j,k,l*] do
52         JJ := y*Matrix(A,[Eltseq(MonomialCoefficient(L[yy][1],y))
               ]);
53                 Append(~Mlist,JJ);
54         MM := &+[a : a in Mlist];
55         if (count eq 5) then
56         KK := InsertBlock(KK,Matrix(A,MM),yy,1);
57         end if;
58         count := count + 1;
59         end for;
60     Mlist := [];
61     count := 1;
62 end for;
63
64 /*
65     Assign KK to M which is then the matrix representation
66     of the linear transformation $L(beta) = beta*x$.
67 */
68
69 M := KK;
70
71 /* Compute the characteristic polynomial of M */
72
73 CM := CharacteristicPolynomial(M);
74
75 polys :=[ Coefficients(CM,4) , Coefficients(CM,3), Coefficients(CM
       ,2) ];
76
77 C<a,b,c,d,e> := Curve(ProjectiveSpace(Rationals(),4),polys);
78
79 G = Genus(C);
80
81 // S.D.G.
```

B.2 Nullspace.magma

```
/*
*   Created by
*   Jesse Leigh Patsolic <patsjl12@wfu.edu>
*   Fall 2013 -- Spring 2014
*   Wake Forest University
*   Department of Mathematics
*   Under the advisement of Dr. Jeremy Rouse
*/

R<x> := PolynomialRing(Rationals());

f := x^10 -3*x^6 -33*x^5 - 4*x^2 + 12*x -9;

Qz<z> := NumberField(f);
S<y> := PolynomialRing(Qz);

ff := y^5 + y + 3;

f1 := Factorization(ff)[1][1];
f2 := Factorization(ff)[2][1];

L , lst := SplittingField([f1,f2] : Abs := false);

lst2 := [ lst[1][1], lst[1][2], lst[2][1], lst[2][2], lst[2][3]];

//  Building the entries for $A$.
seq := [ lst2[i]^j : j in [0..4], i in [1..5]];

// A is the Vandermonde matrix in $\alpha_i$.
A := Matrix(L,5,5,seq);
Ai := A^(-1);

// B is the matrix corresponding to $\alpha^{-1} : C_1\to C$.
B:= Matrix(L
    ,[[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1],[5/4,0,0,0]]);
B2 := Matrix(L
    ,[[0,1,0,0,0],[1,0,0,0,0],[0,0,1,0,0],[0,0,0,1,0],[0,0,0,0,1]])
    ;
B3 := Matrix(L,[[1,0,0,0,0],[0,1,0,0,0],[0,0,1,0,0],[0,0,0,1,0]]);
I4 := Matrix(Qz,[[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]]);

// The matrix $M$ as discussed in the notes from 20131107
M0 := B3*Ai*B2*A*B;


M := Matrix(Qz,4,4, [Qz!M0[i][j] : j in [1..4], i in [1..4]] );
MI  := M-I4;
MII := M + I4;

```

```
47 NsMI := Nullspace(MI);
48
49 NsMII := Nullspace(MII);
50
51 ns1 := NullspaceMatrix(MI);
52 ns2 := NullspaceMatrix(MII);
53
54
55 Qy<a,b,c,d> := PolynomialRing(Qz,4);
56
57 e := Basis(NsMI);
58
59 // Computing the linear polynomials in a,b,c and d
60 // where the coefficients are given by the spanning vectors.
61 e2 := e[1][1]*a + e[1][2]*b + e[1][3]*c + e[1][4]*d;
62 e3 := e[2][1]*a + e[2][2]*b + e[2][3]*c + e[2][4]*d;
63 e4 := e[3][1]*a + e[3][2]*b + e[3][3]*c + e[3][4]*d;
64
65 // Creating the list of degree 3 monomials
66
67 Me := Matrix(Qy,[[e[1][1],e[1][2],e[1][3],e[1][4]],[e[2][1],e
       [2][2],e[2][3],e[2][4]],[e[3][1],e[3][2],e[3][3],e[3][4]]]);
68
69
70 Ma := Matrix(Qy,[[a],[b],[c],[d]]);
71
72 eList := [e2^i*e3^j*e4^k : i in [0..3], j in [0..3], k in [0..3] |
        i + j + k eq 3];
73
74 aList := [a^i * b^j * c^k * d^l : i in [0..3], j in [0..3], k in
       [0..3], l in [0..3] | i+j+k+l eq 3];
75
76
77 zseq := [ 0 : i in [0..279]];
78 ZM := Matrix(Qz,14,20,zseq);
79
80
81 //  Cf1 & Cf2 are the equations defining the curve C
82 Cf1 := -5/8*a^2 + 75/4*a*b + 4*b*d + 2*c^2 + 15*c*d;
83
84 Cf2 := -5/16*a^3 - 75/16*a^2*b - 1125/16*a^2*c - 2*a*b*d - a*c^2
       -75/2*a*c*d -225/4*a*d^2 + 4*b^2*c +15*b^2*d + 15*b*c^2 -4*c*d
       ^2 -9*d^3;
85
86
87 eList := Append(eList,Cf1*e2);
88 eList := Append(eList,Cf1*e3);
89 eList := Append(eList,Cf1*e4);
90 eList := Append(eList,Cf2);
91
92 seqM := [ MonomialCoefficient(eList[j], aList[i]) : i in [1..20],
```

```
    j in [1..14]];
93
94  M1 := Matrix(Qz,14,20,seqM);
95
96  N := Nullspace(M1);
97
98  v := N.1;
99
100
101
102 Q3<X,Y,Z> := PolynomialRing(Qz,3);
103
104 xyzList := [X^i*Y^j*Z^k : i in [0..3], j in [0..3], k in [0..3] |
        i + j + k eq 3];
105
106 // polyList := [v[i]*xyzList[i] : i in [1..10]];
107 Cvpoly := &+[v[i]*xyzList[i] : i in [1..10]];
108
109 P2<u,v,t> := ProjectiveSpace(Qz,2);
110
111 Cv := Curve(P2,Cvpoly);
112
113 p := Cv![Qz!0,1,0];
114
115 F := Cvpoly; // F corresponds to Eq (3) from Duif.
116
117 lu1 := Derivative(F,X);
118 lv1 := Derivative(F,Y);
119 lt1 := Derivative(F,Z);
120
121
122 // l is the tangent line at the point $P = (P_x, P_y, P_z)$
123 // in this case the point p := (0,1,0)
124 l := Evaluate(lu1,[0,1,0])*(u - p[1]) + Evaluate(lv1, [0,1,0])*(v
        - p[2]) + Evaluate(lt1, [0,1,0])*(t - p[3]);
125
126
127
128 // We solved l for u interms of t
129
130 U := -(1/958410922935*(-777665536*z^9 + 3887508480*z^8 -
        14587372800*z^7 + 109267056000*z^6 + 1296196608*z^5 +
        18666430464*z^4 - 107850712320*z^3 + 241106371200*z^2 -
        4255194121856*z + 1555200000)*t)/(1/63894061529*(-1214846400*z
        ^9 + 4558554000*z^8 - 34145955000*z^7 + 324000000*z^6 +
        2186416320*z^5 + 33703347600*z^4 - 75345741000*z^3 +
        1330720245000*z^2 - 3402245760*z + 2187184320));
131
132
133
134
```

```
F1 := Evaluate(F, [U, v, t]);
//"IsFlex(Cv,p) returns ", IsFlex(Cv,p);


V := -(1/512286525*(-6314416*z^9 - 7285776*z^8 - 9107892*z^7 +
    4320*z^6 +
         18910848*z^5 + 230476056*z^4 + 265931784*z^3 + 286894278*z
            ^2 +
         25153984*z - 45852288))*t;


F2 := Evaluate(F, [U,V,t]);

U1 := Evaluate(U, [0,0,1]);
V1 := Evaluate(V, [0,0,1]);

Q := Cv![U1,V1,1];

l2 := Evaluate(lu1,[U1,V1,1])*(u - Q[1]) + Evaluate(lv1,[U1,V1,1])
    *(v - Q[2]) + Evaluate(lt1,[U1,V1,1])*(t - Q[3]);


// We solved l2 for u in terms of t and v.
U2 := (- 1/50625*(6400*z^9 + 11904*z^8 + 23040*z^7 + 21600*z^6 -
    19200*z^5 - 246912*z^4 - 464256*z^3 - 790560*z^2 - 868000*z +
    29184)*v - 1/145798602053653125*(15568016150333696*z^9 +
    41649850612160832*z^8 + 393261986764800*z^7 + 589519774614528*
    z^6 - 45817641211778304*z^5 - 632067029684635584*z^4 -
    1375593321557825856*z^3 - 147466527846819 84*z^2 -
    86152541879682560*z - 7692438763894272)*t)
    /(1/3239968934525625*(-24028807035392*z^9 - 65540554650624*z^8
     - 122847720762240*z^7 - 184493203778880*z^6 -
    1309425192515424*z^5 + 986287441559808*z^4 + 2531428121757312*
    z^3 + 4791527625490560*z^2 + 8671112355027488*z +
    53865896442060192));


F3 := Evaluate(F, [U2,v,t]);

// From the Factorizaiton of F3;
V2 := -(1/27471366193975278745708428846024022859466045 *
    (24472679885435659727546281853095229980833 2*z^9 +
    98618953269625392226131335947498494307104*z^8 -
    62671305540591408189678273357100001785260*z^7 +
    18308400236281599297594959523995662406922 36*z^6 -
    72426578151856403652871966285419772876350 6*z^5 -
    84020685056902189659111220974352408924525 68*z^4 -
    34214663692117907890144177549209502988351 52*z^3 -
    48963349353436644490668704470387076657643 78*z^2 -
    72444881979072531975787844295341631380871962*z +
    20944910918583154648862493238058371314380 58)*t);
```

```
162
163
164 U21 := Evaluate(U2, [0,V2,t]);
165
166 F4 := Evaluate(F, [U21,V2,t]);
167
168 R := Cv![Evaluate(U21,[0,0,1]), Evaluate(V2, [0,0,1]), 1];
169
170 M := Matrix([[p[1], Q[1], R[1]],[p[2], Q[2], R[2]], [p[3], Q[3], R
        [3]]]);
171 // M is the matrix $M_{\gamma}$ [Duif, 5]
172
173 Determinant(M);
174
175 inM := M^(-1); // inM is the matrix $M_{\delta}$ [Duif,5]
176
177 x := p[1]*u + Q[1]*v + R[1]*t;
178 y := p[2]*u + Q[2]*v + R[2]*t;
179 z := p[3]*u + Q[3]*v + R[3]*t;
180
181
182 F5 := Evaluate(F, [x,y,z]);
183
184 mm := MonomialCoefficient(F5, u*v^2);
185 pp := MonomialCoefficient(F5, u^2*t);
186 qq := MonomialCoefficient(F5, u*v*t);
187 ss := MonomialCoefficient(F5, u*t^2);
188 tt := MonomialCoefficient(F5, v*t^2);
189
190 c2 := ss/pp;
191 c1 := qq/pp;
192 c0 := mm/pp;
193 c3 := tt/pp;
194
195 a1 := c1/c0;
196 a3 := -c3/c0^2;
197 a2 := -c2/c0;
198
199
200 E := EllipticCurve([a1,a2,a3,0,0]);
201 //WE := WeierstrassModel(E);
202 //MinE := MinimalModel(E); // returns a simpler model along with a
        map.
203
204
205 /*************************************************************
206 THE FOLLOWING IS THE IMPLEMENTATION OF THE NOTES FROM 20140112
207 *************************************************************/
208
209 C1 := Curve(P2, F5); // Corresponds to (17) in Duif
210
```

```
211 // (u,v,t) := (U,V,W) in notes
212 phi := map< C1 -> P2 | [u*t, u*v, t^2 ] >;
213
214 ///*  //The following block was used before C2 had been computed
215 print "\n\n***Computing C2 := Image(phi). ETA < 2 min.***\n\n";
216 //File := Open("Image_phi.txt","r")
217
218 time(Image(phi)); // Takes about 100 seconds to compute.
219 C2 := Image(phi); // Corresponds to (19) in Duif
220                   // Note that Magma takes care of dividing
                         through
221                   // by $v$, pp in this case, as in equation (18).
222 //*/
223
224 phi2 := map< C2 -> P2 | [u,v,-mm*t/pp] >; C3 := Image(phi2);
225
226 C0 := Curve(ProjectiveSpace(Qz,3),[Cf1,Cf2]); // The genus 4 curve
227
228
229 phi0 := map< C0 -> Cv | [e2,e3,e4] >;
230 phi1 := map< Cv -> C1 | [inM[1][1]*u + inM[1][2]*v + inM[1][3]*t,
       inM[2][1]*u + inM[2][2]*v + inM[2][3]*t, inM[3][1]*u + inM
       [3][2]*v + inM[3][3]*t]    >;
231 phi2 := map< C1 -> C2 | [u*t, u*v, t^2 ]>;
232 phi3 := map< C2 -> C3 | [u,v, -mm*t/pp ]>;
233
234 PHI := phi0*phi1*phi2*phi3; // Gives the composition phi0(phi1(
       phi2(phi3(x)))
235
236 // S.D.G.
```

Curriculum Vitae

Education:

- M.A. in Mathematics,

  Wake Forest University, 2014,

  Thesis title: *Trinomials Defining Quintic Number Fields.*

  Advisor: Dr. Jeremy Rouse

- B.S. in Mathematics,

  Oral Roberts University, 2012.

Presentations:

- *Trinomials Defining Quintic Number Fields:* Algebra, Combinatorics, and Number Theory Seminar, April 30, 2014, University of North Carolina at Greensboro.

- *Trinomials Defining Quintic Number Fields:* Fourteenth Annual Graduate Student and Postdoctoral Research Day, March 28, 2014, Wake Forest University, Winston Salem, NC

Research:

- Research assistant, Wake Forest University, Spring 2014.

  Advisor: Dr. Jennifer Erway

- Summer Thesis Research, Wake Forest University, Summer 2013.

  Advisor: Dr. Jeremy Rouse